МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ И.Г.Игнатова
«24» марта 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Технологии защиты информации от утечки по техническим каналам»

Направление подготовки – 10.04.01 «Информационная безопасность»
Направленность (профиль) – «Аудит информационной безопасности»

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций**:**

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1. ТЗИУТК. Способен обосновывать требования к подсистеме защиты объекта информатизации от утечки информации по техническим каналам	**Знания:** технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ), возможности специальных технических средств по перехвату информации, обрабатываемой СВТ; технические каналы утечки акустической речевой информации, возможности средств акустической речевой разведки по перехвату разговоров из выделенных помещений; принципы построения и основные характеристики средств защиты объектов информатизации от утечки информации по техническим каналам; принципы построения и основные характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам; организация защиты объектов информатизации от утечки информации по техническим каналам. **Умения:** проводить анализ потенциальных технических каналов утечки информации на объектах информатизации, рассчитывать опасные зоны R2 и r1; проводить анализ потенциальных технических каналов утечки речевой информации в выделенных помещениях, рассчитывать словесную разборчивость речи; обосновывать требования к под-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		системе защиты объекта информатизации от утечки информации по техническим каналам. **Опыт практической деятельности:** обоснования требования к подсистеме защиты объекта информатизации от утечки информации по техническим каналам.
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2. ТЗИУТК. Способен разрабатывать технические решения по защите объекта информатизации от утечки информации по техническим каналам	**Знания:** технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ), возможности специальных технических средств по перехвату информации, обрабатываемой СВТ; технические каналы утечки акустической речевой информации, возможности средств акустической речевой разведки по перехвату разговоров из выделенных помещений; принципы построения и основные характеристики средств защиты информации от утечки по техническим каналам; принципы построения и основные характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам; организацию защиты объектов информатизации от утечки информации по техническим каналам. **Умения:** устанавливать, настраивать и исследовать характеристики средств защиты объектов информатизации от утечки информации по техническим каналам; устанавливать, настраивать и ис-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		следовать характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам, основные характеристики этих средств; разрабатывать технические решения по защите объекта информатизации от утечки информации по техническим каналам. **Опыт практической деятельности:** настройки и исследования характеристики средств защиты информации от утечки по техническим каналам; разработки технические решений по защите объекта информатизации от утечки информации по техническим каналам

В результате изучения дисциплины студент должен:

Знать:

цели и задачи защиты информации от утечки по техническим каналам;

технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ), возможности специальных технических средств по перехвату информации, обрабатываемой СВТ;

технические каналы утечки акустической речевой информации, возможности средств акустической речевой разведки по перехвату разговоров из выделенных помещений;

принципы построения и основные характеристики средств защиты объектов информатизации от утечки информации по техническим каналам;

принципы построения и основные характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам;

организацию защиты объектов информатизации от утечки информации по техническим каналам.

Уметь:

проводить анализ потенциальных технических каналов утечки информации на объектах информатизации, рассчитывать опасные зоны R2 и r1;

проводить анализ потенциальных технических каналов утечки речевой информации в выделенных помещениях, рассчитывать словесную разборчивость речи;

устанавливать, настраивать и исследовать характеристики средств защиты объектов информатизации от утечки информации по техническим каналам;

устанавливать, настраивать и исследовать характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам;

обосновывать требования к подсистеме защиты объекта информатизации от утечки информации по техническим каналам;

разрабатывать технические решения по защите объекта информатизации от утечки информации по техническим каналам.

Иметь опыт практической деятельности:

настройки и исследования характеристики средств защиты информации от утечки по техническим каналам;

обоснования требования к подсистеме защиты объекта информатизации от утечки информации по техническим каналам;

разработки технические решений по защите объекта информатизации от утечки информации по техническим каналам.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Технологии защиты информации от утечки по техническим каналам» входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 1-м курсе в 1-м семестре.

Изучение дисциплины базируется на знаниях и умениях, полученных при освоении основной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность при изучении следующих дисциплин: «Физика», «Теория вероятностей и математическая статистика», «Информатика», «Теория информации», «Электротехника», «Электроника и схемотехника», «Аппаратные средства вычислительной техники», «Основы радиотехники», «Сети и системы передачи информации», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Защита информации от утечки по техническим каналам».

Знания и умения, полученные в результате изучения дисциплины, используются в дисциплинах «Контроль эффективности защищенности информации от утечки по техническим каналам», «Защищенные информационные системы», производственной практике и при подготовке ВКР.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа, часы					Самостоятельная работа, часы	Вид промежуточной аттестации
				ВСЕГО	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации		
1	1	8	288	120	32	64	-	24	132	Экз. (36)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации		
1. Технические каналы утечки информации	14	32	-	8	36	Компьютерный тест КТ-1. Зачет по Лр 1 - 8
2. Технологии защиты информации от утечки по техническим каналам	14	20	-	8	28	Компьютерный тест КТ-2. Зачет по Лр 9 – 13
3. Организация защиты информации по техническим каналам.	4	12	-	8	68	Компьютерный тест КТ 3. Зачет по Лр 14 – 16. Сдача ДЗ № 1 и 2

4.1. Лекционные занятия

Номер модуля дисциплины	**Номер лекции**	**Объем занятий, часы**	**Краткое содержание**
1	1.	2	**Вводная лекция. Цели и задачи защиты информации от утечки информации по техническим каналам.** Термины и определения в области защиты информации от утечки по техническим каналам: объект информатизации, выделенное помещение, ОТСС, ВТСС, посторонние проводники, контролируемая зона, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, технический канал утечки информации. Цели и задачи защиты информации от утечки информации по техническим каналам. Содержание и порядок изучения дисциплины.

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			Тема 1 «Технические каналы утечки информации, обрабатываемой СВТ»
	2.	2	**Электромагнитные и электрические технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ)** Классификация технических каналов утечки информации, обрабатываемой СВТ. Причины возникновения побочных электромагнитных излучений (ПЭМИ) СВТ. Опасная зона R2. Схема технического канала утечки информации, возникающего за счет ПЭМИ СВТ. Причины возникновения электрических технических каналов утечки информации, обрабатываемой СВТ. Случайные антенны. Причины возникновения наводок информативных сигналов в случайных антеннах. Опасная зона r1. Схема технического канала утечки информации, возникающего за счет наводок ПЭМИ СВТ в случайных антеннах. Причины возникновения наводок информативных сигналов в линиях электропитания и цепях заземления СВТ. Схемы технических каналов утечки информации, возникающих за счет наводок ПЭМИ СВТ в линиях электропитания и цепях заземления СВТ. Средства разведки ПЭМИН
	3.	2	**Специально создаваемые технические каналы утечки информации, обрабатываемой СВТ** Схема технического канала утечки информации, создаваемого методом «высокочастотного облучения». Средства перехвата информации путем «высокочастотного облучения» СВТ. Схема технического канала утечки информации, создаваемого путем внедрения в СВТ электронных устройств перехвата информации. Электронные устройства перехвата информации, внедряемых в СВТ.
			Тема 2 «Технические каналы утечки акустической речевой информации»
	4.	2	**Характеристики речи. Классификация технических каналов утечки акустической речевой информации.** Акустические сигналы. Линейные и энергетические характеристики акустического поля. Характеристики речи (семантические, фонетические, физические). Спектр и типовые уровни речевого сигнала. Разборчивость речи. Методы оценки разборчивости речи.
	5.	2	**Прямые акустические каналы утечки речевой информации**. Способы перехвата речевой информации из выделенных помещений по прямому акустическому каналу. Схемы перехвата информации по прямым акустическим каналам утечки информации. Средства акустической

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			разведки с датчиками микрофонного типа: цифровые диктофоны, электронные устройства перехвата речевой информации, направленные микрофоны.
	6.	2	**Акустовибрационные и акустооптический каналы утечки речевой информации.** Способы перехвата речевой информации из выделенных помещений по акустовибрационным каналам. Схемы перехвата речевой информации по акустовибрационным каналам. Электронные стетоскопы. Радиостетоскопы. Способы перехвата речевой информации из выделенных помещений по акустооптическому каналу. Схема перехвата речевой информации по акустооптическому каналу. Лазерные акустические системы разведки.
	7.	2	**Акустоэлектрические и акустоэлектромагнитные каналы утечки речевой информации.** Причины возникновения акустоэлектрические каналов утечки речевой информации. Акустоэлектрические преобразователи генераторного типа. Акустоэлектрические преобразователи модуляторного типа. Способы перехвата речевой информации из выделенных помещений по акустоэлектрическим каналам. Схема пассивного акустоэлектрического канала утечки речевой информации. Схема активного акустоэлектрического канала утечки речевой информации. Причины возникновения акустоэлектромагнитных каналов утечки речевой информации. Способы перехвата речевой информации из выделенных помещений по акустоэлектрическим каналам. Схема пассивного акустоэлектромагнитного канала утечки речевой информации. Схема активного акустоэлектромагнитного канала утечки речевой информации.
2			**Тема 3 «Технологии защиты объектов информатизации от утечки информации по техническим каналам»**
	8.	2	**Экранирование и заземление технических средств.** Классификация способов и средств защиты объектов информатизации от утечки информации по техническим каналам. Экранирование технических средств их соединительных линий. Экранирующие материалы. Экранированные помещения (экранированные камеры). Защищенные ПЭВМ. Заземление технических средств. Требования к заземлению ОТСС. Схемы заземления ОТСС. Методы и средства измерения сопротивления заземления ОТСС.
	9.	2	**Системы пространственного электромагнитного зашумления**

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			Требования к системе пространственного электромагнитного зашумления. Принципы построения систем пространственного электромагнитного зашумления и широкополосных генераторов шума. Основные характеристики сертифицированных систем пространственного электромагнитного зашумления (САЗ типа А). Требования по установке систем пространственного электромагнитного. Особенности зашумления инженерных коммуникаций.
	10.	2	**Способы и средства защиты объектов информатизации от утечки информации по цепям электропитания и заземления** Требования к системе электропитания ОТСС. Требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания СВТ. Принципы построения, основные характеристики и требования по установке сертифицированных помехоподавляющих фильтров. Принципы построения систем линейного электромагнитного зашумления и их основные характеристики (САЗ типа Б). Требования по установке систем линейного электромагнитного зашумления.
			Тема 4 «Технологии защиты выделенных помещений от утечки речевой информации по техническим каналам»
	11.	2	**Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам** Пассивные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Активные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Звуко- и виброизоляция выделенных помещений, глушители шума. Звукопоглощающие материалы. Специальные защищенные помещения.
	12.	2	**Системы и средства виброакустической маскировки** Требования к системе виброакустической маскировки. Принципы построения низкочастотных генераторов шума. Принципы построения акустических излучателей и виброизлучателей. Основные характеристики сертифицированных систем виброакустической маскировки типа А. Основные характеристики сертифицированных систем виброакустической маскировки типа Б. Особенности установки акустических излучателей и виброизлучателей в выделенных помещениях. Специальная аппаратура для ведения конфиденциальных переговоров.
	13.	2	**Средства защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам** Пассивные способы защиты ВТСС от утечки речевой информации по аку-

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			стоэлектрическим каналам (ограничение сигналов малой амплитуды, фильтрация высокочастотных сигналов навязывания, отключение акусто-электрических преобразователей опасных сигналов). Активные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам. Принципы построения и основные характеристики средств защиты ВТСС, основанных на использовании ограничителей малой амплитуды и фильтров нижних частот. Принципы построения основные характеристики средств защиты ВТСС, основанных на отключении акустоэлектрических преобразователей. Принципы построения основные характеристики средств защиты ВТСС, основанных на использовании низкочастотных генераторов шума.
	14.	2	**Специальные технические средства подавления электронных устройств перехвата речевой информации** Принципы построения и основные характеристики подавителей диктофонов. Принципы построения и основные характеристики широкополосных генераторы шума. Принципы построения и основные характеристики блокираторов средств сотовой связи.
3			**Тема 5 «Организация защиты информации от утечки по техническим каналам на объектах информатизации»**
	15.	2	**Организация защиты информации от утечки по техническим каналам на объектах информатизации** Порядок организации защиты информации от утечки по техническим каналам. Предпроектное специальное обследование объекта информатизации.
	16.	2	**Проектирование подсистем защиты объектов информатизации от утечки информации по техническим каналам** Обоснование требований к подсистеме защиты информации от утечки по техническим каналам (СЗИУТК). Содержание технического задания на создание (СЗИУТК). Разработка технические решений по защите объекта информатизации от утечки. Содержание технического проекта СЗИУТК.

4.2. Практические занятия

Не предусмотрены

4.3.

Практическая подготовка при проведении лабораторных работ

Номер модуля дисциплины	Номер лабораторного занятия	Объем занятий, часы	Краткое содержание
1.			**Тема 1 «Технические каналы утечки информации, обрабатываемой СВТ»**
	1.	4	**Исследование спектров сигналов** Исследование спектров гармонических сигналов. Исследование спектров сигналов с амплитудной и частотной модуляцией. Исследование спектров импульсных сигналов.
	2.	4	**Исследование основных характеристик случайных приемных антенн** Измерение спектральной чувствительности случайных антенн. Измерение спектральных калибровочных характеристик случайных аентенн
	3.	4	**Исследование побочных электромагнитных излучений (ПЭМИ) ПЭВМ** Исследование ПЭМИ видеосистемы монитора ПЭВМ.
	4.	4	**Исследование ПЭМИ ПЭВМ:** Исследование ПЭМИ клавиатуры ПЭВМ. Исследование ПЭМИ съемных носителей ПЭВМ.
	5.	4	**Оценка возможностей по перехвату ПЭМИН СВТ:** Расчет опасной зоны *R*2. Расчет опасной зоны *r*1.
			Тема 2 «Технические каналы утечки акустической (речевой) информации»
	6.	4	**Исследование акустических и акустовибрационых каналов утечки речевой информации** Исследование спектров и слышимости речевых сигналов. Исследование вибрационных сигналов, возбуждаемых в ограждающих конструкциях при ведении разговоров в помещении. Измерение звукоизоляции помещения (двери в помещение).
	7.	4	**Оценка возможностей по перехвату речевой информации из выделенного помещения средствами акустической разведки** Расчет разборчивости речи при непреднамеренном прослушивании разговоров, ведущихся выделенном помещении. Расчет разборчивости речи при перехвате речевой информации средствами акустической разведки (направленными микрофонами). Расчет разборчивости речи при перехвате речевой информации средствами акустической разведки с датчиками контактного типа (электронными стетоскопами).

Номер модуля дисциплины	Номер лабораторного занятия	Объем занятий, часы	Краткое содержание
	8.	4	**Исследование подверженности ВТСС акустоэлектрическим преобразованиям** Исследование чувствительности акустоэлектрических преобразователей. Исследование подверженности акустоэлектрических преобразователей «высокочастотному навязыванию». Исследование подверженности радиоприемных устройств акустоэлектромагнитным преобразованиям.
2.			**Тема 3 «Технологии защиты объектов информатизации от утечки информации по техническим каналам»**
	9.	4	**Исследование основных характеристик систем пространственного и линейного электромагнитного зашумления** Исследование спектров помеховых сигналов систем пространственного электромагнитного зашумления (Гном-3, ГШ-1000У, ЛГШ-503, Соната-Р2). Исследование спектров помеховых сигналов, создаваемых в инженерных коммуникациях системой линейного электромагнитного зашумления (ГШ-1000У). Исследование спектров помеховых сигналов, создаваемых в сети 220 В системой линейного электромагнитного зашумления (SP-44).
	10.	4	**Исследование характеристик помехоподавляющих фильтров типа «ФП»** Расчет и измерение резонансной частоты и частоты среза помехоподавляющих фильтров типа «ФП». Измерение затухания помехоподавляющих фильтров типа «ФП» в полосе подавления. Измерение падения напряжения на шинах фильтра для переменного тока, частотой 50 Гц
			Тема 4 «Технологии защиты выделенных помещений от утечки речевой информации по техническим каналам»
	11.	4	**Исследование характеристик системы виброакустической защиты типа Б** Исследование характеристик акустического шумового сигнала, излучаемого генератором - акустическим излучателем. Исследование характеристик вибрационных шумовых сигналов, возбуждаемых в стене, инженерной коммуникации, оконном стекле генераторами-виброизлучателями при различных режимах их работы.
	12.	4	**Исследование характеристик средств защиты ВТСС от утечки информации по техническим каналам** Исследование характеристик пассивных средств защиты телефонных аппаратов от утечки информации по техническим каналам (Гранит-8, МП-8, Барьер-М). Исследование характеристик активных средств защиты телефонных аппаратов от утечки информации по техническим каналам (МП-1А). Исследование характеристик пассивных средств защиты громкоговорителей систем оповещения от утечки информации по техническим каналам (МП-5).

Номер модуля дисциплины	Номер лабораторного занятия	Объем занятий, часы	Краткое содержание
	13.	4	**Исследование характеристик специальных средств радиоподавления** Исследование характеристик средств радиоподавления телефонов сотовой связи, использующих для радиоподавления заградительные по частоте помехи. Исследование характеристик средств радиподавления телефонов сотовой связи, использующих для подавления имитационные, прицельные по частоте помехи. Исследование характеристик средств радиоподавления средств беспроводного доступа.
3			**Тема 5 «Организация защиты информации по техническим каналам»**
	14.	4	**Предпроектное специальное обследование объекта информатизации** Предпроектное специальное обследование объекта информатизации Предпроектное специальное обследование выделенного помещения
	15.	4	**Обоснование требований к подсистеме защиты объекта информатизации от утечки информации по техническим каналам (СЗИУТК)** Обоснование требований к СЗИУТК объекта информатизации. Обоснование требований к СЗИУТК выделенного помещения.
	16.	4	**Разработка технических решений по защите объекта информатизации от утечки информации по техническим каналам** Разработки технические решений по защите объекта информатизации от утечки информации по техническим каналам. Обоснование состава СЗИУТК объекта информатизации Разработки технические решений по защите выделенного помещения от утечки информации по техническим каналам. Обоснование состава СЗИУТК выделенного помещения.

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	4	**Подготовка к лабораторной работе № 1** Изучение материалов лекции №№ 1-3 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 1
	4	**Подготовка к лабораторной работе № 2** Изучение материалов лекции №№ 1-3 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 2
	4	**Подготовка к лабораторной работе № 3** Изучение материалов лекции №№ 1- 3 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 3
	4	**Подготовка к лабораторной работе № 4** Изучение материалов лекции №№ 1- 3 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 4
	4	**Подготовка к лабораторной работе № 5** Изучение материалов лекции №№ 1- 3 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 5
	4	**Подготовка к лабораторной работе № 6** Изучение материалов лекции №№ 4 - 7 рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 6
	4	**Подготовка к лабораторной работе № 7** Изучение материалов лекции №№ 4 - 7 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 7
	4	**Подготовка к лабораторной работе № 8** Изучение материалов лекции №№ 4 - 7 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 8
	4	**Подготовка к компьютерному тесту КТ-1** Изучение материалов лекции №№ 1 - 7 и рекомендованной литературы.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
2	4	**Подготовка к лабораторной работе № 9** Изучение материалов лекции №№ 8 -10 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 9
	4	**Подготовка к лабораторной работе № 10** Изучение материалов лекции №№ 8 -10 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 10
	4	**Подготовка к лабораторной работе № 11** Изучение материалов лекции № 11 -14 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 11
	4	**Подготовка к лабораторной работе № 12** Изучение материалов лекции № 11 -14 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 12
	4	**Подготовка к лабораторной работе № 13** Изучение материалов лекции № 11 -14 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 13
	8	**Подготовка к компьютерному тесту КТ-2** Изучение материалов лекции №№ 8 - 14 и рекомендованной литературы.
3	4	**Подготовка к лабораторной работе № 14** Изучение материалов лекции № 15 -16 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 14
	4	**Подготовка к лабораторной работе № 15** Изучение материалов лекции № 15 -16 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 15
	4	**Подготовка к лабораторной работе № 16** Изучение материалов лекции № 15 -16 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 16
	4	**Подготовка к компьютерному тесту КТ-3** Изучение материалов лекции №№ 15 - 16 и рекомендованной литературы.
	28	**Выполнение практико-ориентированного домашнего задания № 1**
	24	**Выполнение практико- ориентированного домашнего задания № 2**

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрены

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС, http://orioks.miet.ru/):

Модуль 1. Технические каналы утечки информации:

Тексты лекций № 1 – 6. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 1 – 3. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. Способы и средства защиты информации от утечки по техническим каналам

Тексты лекций № 7 – 14. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 4 – 6. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 3. Методы и средства контроля защищенности информации от утечки по техническим каналам

Тексты лекций № 15 – 21. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 7 – 9. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 4. Организация защиты информации по техническим каналам.

Тексты лекций № 22 – 24. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 10 – 12. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по выполнению практико-ориентированных заданий № 1 и 2. ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Зайцев А.П. Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2018. - 444 с. - URL: https://e.lanbook.com/book/111057 (дата обращения: 15.03.2021). - ISBN 978-5-9912-0233-6. - Текст : электронный.

2. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 . - Текст : электронный.

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы

1. Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наво-

док на вспомогательные технические средства и системы и их коммуникации, Гостехкомиссия России, 2002, дсп.

2. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации, Гостехкомиссия России, 2002, дсп.

3. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва, 2002, дсп.

4. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах», Гостехкомиссия России, Москва, 2002, дсп.

5. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

6. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации

7. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения

8. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Одобрены решением коллегии Гостехкомиссии России от 2 марта 2001 г. № 7.2, дсп.

9. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Периодические издания

1. ЗАЩИТА ИНФОРМАЦИИ. INSIDE : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 15.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный : непосредственный.

2. Безопасность информационных технологий : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: https://bit.mephi.ru/index.php/bit/index (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

3. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 15.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

4. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011 - 2018. - URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021). – Текст: электронный.
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.
3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение, которое основано на интеграции технологий традиционного и электронного обучения, замещении части традиционных учебных форм занятий формами и видами взаимодействия в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС http://orioks.miet.ru.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: ОРИОКС «Домашние задания», электронная почта преподавателя.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы (http://orioks.miet.ru).

Тестирование проводится в ОРИОКС (MOODLe).

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	**Оснащенность учебных аудиторий и помещений для самостоятельной работы**	**Перечень программного обеспечения**
Учебная аудитория	Мультимедийное оборудование: компьютер с программным обеспечением, возможностью подключения к сети Интернет и обеспечением доступа в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (микрофон, звуковые колонки), вебкамера с микрофоном).	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome/Explorer).

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	Учебная доска.	
Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью»	1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	1. Операционная система Microsoft Win Pro 7 – 28 шт. 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL – 28 шт. 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal – 28 шт. 4. Корпоративная информационно - технологическая платформа ОРИОКС – 28 шт.
Учебная аудитории № 3225Б: Лаборатория «Технической защиты информации»	1) Программно-технический комплекс (лабораторная установка) для исследования побочных электромагнитных излучений (ПЭМИ) СВТ (ЛУ 01) 2) Программно-технический комплекс (лабораторная установка) для исследования реального затухания ПЭМИ СВТ и их наводок (ЛУ 02). 3) Программно-технический комплекс (лабораторная установка) для исследования систем пространственного и линейного	1) ПО Microsoft WinPro 8.1 x64 Russian 1pk DSP OEL DVD 2) Права на программу для ЭВМ Microsoft Office Home & Business 2013 - 1 PC Russian 3) Неисключительное право на использование программы для ЭВМ Kaspersky Total Security 4) Лиц. На ПО Multisim 9 Academic Edituon Single seal

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	электромагнитного зашумления (ЛУ 03). 4) Программно-технический комплекс (лабораторная установка) для исследования характеристик помехоподавляющих фильтров (ЛУ 04). 5) Программно-технический комплекс (лабораторная установка) для исследования прямых акустических, акустовибрационных каналов утечки информации и систем виброакустической маскировки (ЛУ 05). 6) Программно-технический комплекс (лабораторная установка) для исследования акустоэлектрических каналов утечки информации и средств защиты вспомогательных технических средств (ВТСС) (ЛУ 06). 7) Программно-технический комплекс (лабораторная установка) для исследования специальных средств подавления электронных устройств перехвата информации (ЛУ 07). 8) Программно-технический комплекс (лабораторная установка) для исследования методов выявления электронных устройств перехвата информации, с использованием	

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	программно-аппаратных комплексов контроля (ЛУ 08). 9) Программно-технический комплекс (лабораторная установка) для исследования методов выявления электронных устройств перехвата информации с использованием средств контроля индикаторного типа (ЛУ 09). 10) Программно-технический комплекс (лабораторная установка) для исследования принципов построения и функционирования системы контроля и управления доступом, системы охранно-пожарной сигнализации и систем охранного видеонаблюдения (ЛУ 10). 11) Автоматизированное рабочее место преподавателя (АРМ-П).	
Помещение для самостоятельной работы обучающихся: Учебная аудитории № 3226	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС: 1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 – 28 шт. 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL – 28 шт. 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal– 28 шт. 4. Корпоративная информационно - технологическая платформа ОРИОКС – 28

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	– 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	шт.

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-1. ТЗИУТК. Способен обосновывать требования к подсистеме защиты объекта информатизации от утечки информации по техническим каналам.

ФОС по подкомпетенции ОПК-2. ТЗИУТК. Способен разрабатывать технические решения по защите объекта информатизации от утечки информации по техническим каналам

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/**.**

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

11.1. Особенности организации процесса обучения

В целях практической подготовки в дисциплине предусмотрены лабораторные работы и выполнение практико-ориентированных домашних заданий.

Каждая лабораторная работа и каждое домашнее задание направлены на формирование отдельных умений, необходимых для формирования общепрофессиональных и профессиональных компетенции.

Лабораторные работы и домашние задания выполняются каждым студентом индивидуально. По результатам выполнения каждой лабораторной работы и домашнего задания студент оформляет и представляет отчет. При защите отчетов по лабораторным работам и домашних заданий преподаватель разбирает типовые ошибки и указывает их причины.

11.2. Методические указания студентам по подготовке к лабораторным работам

Выполнение студентами лабораторных работ направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины;

- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;

- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;

- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Ведущей дидактической целью лабораторных работ является формирование практических умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности.

Наряду с ведущей дидактической целью в ходе выполнения заданий у студентов формируются практические умения и навыки обращения с различными приборами, установками, лабораторным оборудованием, аппаратурой, которые могут составлять часть профессиональной практической подготовки, а также исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты).

Лабораторная работа как вид учебного занятия проводиться в специально оборудованных учебных лабораториях. Продолжительность - не менее двух академических часов. Необходимыми структурными элементами лабораторной работы, помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

По каждой лабораторной работе разработаны и утверждены методические указания по их проведению.

Лабораторные работы носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория, основные характеристики), оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Формы организации студентов на лабораторных работах: индивидуальная, при которой каждый студент выполняет индивидуальное задание.

Для проведения лабораторных работ преподавателями разрабатываются методические рекомендации по их выполнению, которые рассматриваются и утверждаются на заседании кафедры. Методические рекомендации разрабатываются по каждой лабораторной работе, предусмотренными рабочей программой учебной дисциплины: в соответствии с количеством часов, требованиями к знаниям и умениям, темой практических занятий и лабораторных работ, установленными рабочей программой учебной дисциплины по соответствующим разделам (темам).

Методические рекомендации по выполнению лабораторных работ включают в себя:

- пояснительную записку;
- наименование раздела (темы);
- объем учебного времени, отведенный на лабораторную работу;
- наименование темы лабораторной работы;

- цель лабораторной работы (в т.ч. требования к знаниям и умениям студентов, которые должны быть реализованы);
- перечень необходимых средств обучения (оборудование, материалы и др.);
- требования по теоретической готовности студентов к выполнению лабораторных работ (требования к знаниям, перечень дидактических единиц);
- содержание заданий;
- рекомендации (инструкции) по выполнению заданий;
- требования к результатам работы, в т.ч. к оформлению;
- критерии оценки и формы контроля;
- список рекомендуемой литературы;
- приложения.

При подготовке к лабораторной работы студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к лабораторной работе;
- ознакомиться с методическими рекомендации по выполнению лабораторной работы;
- прочитать конспект лекций и соответствующие главы учебника (учебного пособия), дополнить запись лекций выписками из него;
- прочитать дополнительную литературу, рекомендованную преподавателем. Наиболее интересные мысли следует выписать;
- сформулировать и записать развернутые ответы на вопросы для подготовки к лабораторной работе;
- изучить схемы лабораторных установок (стендов), порядок работы на аппаратуре и технике, правила и меры безопасности;
- подготовить отчеты для заполнения.

На лабораторной работе студент должен выполнить задание в соответствии с методическими указаниями.

Особое внимание уделить усвоению порядка проведения измерений с использованием контрольно-измерительного оборудования, составу лабораторных установок (стендов).

Отчет о лабораторной работе должен быть оформлен в соответствии методическими указаниями и ГОСТами.

При защите отчета о лабораторной работе убедительно четко и аргументировано изложить содержание проведенных исследований и выводы по полученным результатам.

По завершению занятия студент должен уяснить недостатки, указанные преподавателем при необходимости записать их содержание.

Студенты, по каким-либо причинам, отсутствовавшие на занятии, в свободное время должны самостоятельно изучить учебный материал и провести лабораторные исследования, после чего отчитаться в проделанной работе перед преподавателем.

Студенты на лабораторной работе обязаны соблюдать меры безопасности при работе на аппаратуре (оборудовании). Перед началом занятий, каждый студент должен пройти инструктаж по соблюдению мер безопасности на рабочем месте и уяснить места расположения средств пожаротушения и обесточивания аппаратуры (оборудования).

11.3. Методические указания студентам по подготовке практико-ориентированных домашних заданий

Задачи выполнения практико-ориентированных домашних заданий:

обучение студентов самостоятельному применению полученных знаний для решения конкретных практических задач защиты информации от утечки по техническим каналам;

развитие навыков подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по организации, способам и средствам защиты информации на объектах информатизации;

овладение методами анализа потенциальных технических каналов утечки информации на объектах информатизации и в выделенных помещениях;

привитие навыков проведения аналитического обоснования необходимости создания подсистемы защиты информации от утечки по техническим каналам на объектах информатизации учреждения (предприятия);

привитие навыков разработки предложений в техническое задание на создание подсистемы защиты объекта информатизации организации от утечки информации по техническим каналам.

Домашнее задание № 1

Тема домашнего задания № 1 «Обоснование требований к подсистеме защиты объекта информатизации от утечки информации по техническим каналам».

Защищаемый объект информатизации – помещение, предназначенное для ведения конфиденциальных переговоров, в котором установлено автоматизированное рабочее место для обработки конфиденциальной информации на базе ПЭВМ.

Для выполнения задания студентам выделяются реально существующие объекты информатизации предприятий (учреждений).

Объем домашнего задания составляет 8 – 10 страниц машинописного текста пояснительной записки и графических материалов, выполненных на стандартных листах формата А4.

Графическая часть домашнего задания выполняется в ACAD (формат А4).

Пояснительная записка оформляется в редакторе Word, шрифт Times New Roman размер – 12-14 интервал – полуторный (30 строк по 60 печатных знаков в каждой строке, считая пробелы). Размеры полей следующие: левое – 30 мм, правое — не менее 10 мм, верхнее - не менее 20 мм, нижнее — не менее 20 мм. Отступ красной строки 1,25 см.

Структура отчета по домашнему заданию должна отвечать традиционным требованиям, предъявляемым к учебно-квалификационным работам и включать: титульный лист; содержание (оглавление); введение; основную часть; заключение; список литературы.

В основной части задания:

определяется назначение защищаемого объекта информатизации (далее по тексту – защищаемого объекта);

проводится описание защищаемого помещения (входа в помещение, пола, потолка, стен, окон, системы вентиляции и кондиционирования);

определяются технические средства, входящие в состав автоматизированного рабочего места для обработки конфиденциальной информации (далее по тексту – ОТСС), установленные на объекте информатизации и непосредственно участвующие в обработке конфиденциальной информации, составляется их перечень;

определяются вспомогательные технические средства и системы (ВТСС) установленные на объекте информатизации, составляется их перечень;

составляется схема расположения мебели, ОТСС и ВТСС в защищаемом помещении;

проводится анализ местоположения защищаемого объекта на местности и определяет-

ся граница его контролируемой зоны;

описывается система электропитания и заземления защищаемого объекта;

определяются месторасположение трансформаторной подстанции и заземлителя относительно границы контролируемой зоны объекта;

устанавливаются инженерные коммуникации и посторонние проводники, выходящие за пределы контролируемой зоны объекта;

устанавливаются соединительные линии ВТСС, выходящие за пределы контролируемой зоны объекта;

определяется наличие физической охраны здания, в котором расположено предприятие (учреждение);

определяется наличие системы охранной сигнализации, охранного телевидения, системы контроля и управления доступом в служебные и технические помещения предприятия (учреждения);

определяется возможность неконтролируемого доступа посторонних лиц к ограждающим конструкциям и окнам выделенного помещения;

описывается порядок доступа сотрудников и посторонних лиц на предприятие (в учреждение);

описывается порядок доступа сотрудников предприятия (учреждение), а также посторонних лиц на объект информатизации в служебное и неслужебное время;

определяются помещения, смежные с защищаемым объектом информатизации, устанавливается их назначение и принадлежность;

определяется возможность доступа посторонних лиц в смежные с защищаемым объектом информатизации помещения, а также к инженерным коммуникациям, проходящим через объект информатизации;

описываются и анализируются организационные мероприятия по технической защите информации, реализуемые на предприятии (в учреждении);

проводится анализ технических средств защиты объекта информатизации от утечки информации по техническим каналам;

проводится анализ технических средств защиты выделенного помещения от утечки речевой информации по техническим каналам;

разрабатывается модель противника (злоумышленника);

проводится анализ возможностей заинтересованных субъектов по перехвату информации, обрабатываемой ПЭВМ, по каналу утечки информации, возникающему за счет побочных электромагнитных излучений (ПЭМИ) ПЭВМ и каналам утечки информации, возникающим за счет наводок ПЭМИ ПЭВМ на токопроводящие коммуникации, линии электропитания и цепи заземления;

проводится анализ возможностей непреднамеренного прослушивания конфиденциальных разговоров, ведущихся в выделенном помещении, посторонними лицами;

проводится анализ возможностей заинтересованных субъектов по перехвату конфиденциальных разговоров, ведущихся в выделенном помещении:

с использованием лазерных акустических систем разведки (ЛАСР) и направленных микрофонов;

электронных стетоскопов и радиостетоскопов;

аппаратуры «высокочастотного навязывания» и средств, подключаемых к соединительным линиям ВТСС;

электронных устройств перехвата речевой информации, возможно внедренных в выделенное помещение;

составляется перечень потенциальных технических каналов утечки информации, обрабатываемой ОСТТ с указанием возможных средства перехвата информации (стационарных, мобильных и портативных) и мест их возможной установки;

составляется перечень потенциальных технических каналов утечки речевой информации из выделенных помещений (стационарных, мобильных и портативных) и мест их возможной установки;

обосновываются требования к подсистеме защиты объекта информатизации от утечки информации по техническим каналам.

Заключение содержит в сжатой форме теоретические выводы, полученные в результате выполнения задания. Заключение должно показать, насколько материал работы может быть использован в практике конкретной организации (предприятия).

Список использованной литературы включает источники и литературу, использованные студентом в ходе подготовки и написания домашнего задания.

Таблицы, схемы, рисунки, графики большого формата, фрагменты которых используются в основном тексте, могут быть вынесены в приложения к пояснительной записке.

Домашнее задание № 2

Тема домашнего задания «Разработка технических решений по защите объекта информатизации от утечки информации по техническим каналам».

Защищаемый объект информатизации – помещение, предназначенное для ведения конфиденциальных переговоров, в котором установлено автоматизированное рабочее место для обработки конфиденциальной информации на базе ПЭВМ.

Для выполнения задания студентам выделяются реально существующие объекты информатизации предприятий (учреждений).

Объем домашнего задания составляет 8 – 10 страниц машинописного текста пояснительной записки и графических материалов, выполненных на стандартных листах формата А4.

Графическая часть домашнего задания выполняется в ACAD (формат А4).

Пояснительная записка оформляется в редакторе Word, шрифт Times New Roman размер – 12-14 интервал – полуторный (30 строк по 60 печатных знаков в каждой строке, считая пробелы). Размеры полей следующие: левое – 30 мм, правое — не менее 10 мм, верхнее - не менее 20 мм, нижнее — не менее 20 мм. Отступ красной строки 1,25 см.

Структура отчета по домашнему заданию должна отвечать традиционным требованиям, предъявляемым к учебно-квалификационным работам и включать: титульный лист; содержание (оглавление); введение; основную часть; заключение; список литературы.

В основной части отчета:

проводится анализ пассивных и активных технических средств защиты информации, обрабатываемой ОТСС, по каналу утечки информации, возникающему за счет побочных электромагнитных излучений ОТСС (для сравнения характеристики анализируемых средств защиты сводятся в таблицы);

проводится анализ пассивных и активных технических средств защиты информации, обрабатываемой ОТСС, по каналу утечки информации, возникающему за счет наводок побочных электромагнитных излучений ОТСС на токопроводящие коммуникации, линии электропитания и цепи заземления (для сравнения характеристики анализируемых средств защи-

ты сводятся в таблицы);

проводится сравнительная оценка (по показателю эффективность – стоимость) технических средств защиты информации от утечки по техническим каналам, предполагаемых для установки на объекте информатизации;

определяется рациональный состав подсистемы защиты объекта информатизации от утечки информации по техническим каналам, составляется перечень предполагаемых к использованию технических средств защиты (в перечне указывается для закрытия каких технических каналов информации предполагается использовать техническое средство защиты);

разрабатываются технические решения по защите объекта информатизации от утечки информации по техническим каналам;

обосновываются требования, предъявляемые к техническим средствам защиты выделенного помещения от утечки речевой информации по техническим каналам;

проводится анализ систем виброакустической маскировки (для сравнения характеристики анализируемых систем сводятся в таблицы);

проводится анализ способов и средств защиты ВТСС от утечки информации по акустоэлектрическим каналам (для сравнения характеристики анализируемых средств защиты сводятся в таблицы);

разрабатываются технические решения по защите выделенного помещения от утечки информации по техническим каналам.

Заключение содержит в сжатой форме теоретические выводы, полученные в результате выполнения задания. Заключение должно показать, насколько материал работы может быть использован в практике конкретной организации (предприятия).

Список использованной литературы включает источники и литературу, использованные студентом в ходе подготовки и написания домашнего задания.

Таблицы, схемы, рисунки, графики большого формата, фрагменты которых используются в основном тексте, могут быть вынесены в приложения к пояснительной записке.

11.4. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительно-бальная система.

Под накопительно-бальной системой понимается система количественной, балльно - рейтинговой оценки качества освоения учебной дисциплины студентом $R_{нак}$ по суммарному результату текущего $R_{тек}$ и итогового контроля $R_{итог}$, с учетом посещаемости студентом занятий, его активности на занятиях и качества выполнения им текущих заданий $R_{пр}$.

Выполнение контрольных мероприятий текущего контроля (сдача компьютерных тестов, защита отчетов по лабораторным работам, защита отчетов по выполнению домашних заданий), посещаемость занятий и активность на занятиях, результаты итогового контроля (сдача экзамена) оцениваются баллами, общая сумма которых составляет 100 баллов (максимальное значение нормативного рейтинга учебной дисциплины – $R_{нор}$).

Примерная структура и график контрольных мероприятий приведены в таблице 11.1.

Структура и график контрольных мероприятий

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
7	Лабораторная работа № 1	4	2
7	Лабораторная работа № 2	4	2
8	Лабораторная работа № 3	4	2
9	Лабораторная работа № 4	4	2
9	Лабораторная работа № 5	4	2
10	Лабораторная работа № 6	4	2
11	Лабораторная работа № 7	4	2
11	Лабораторная работа № 8	4	2
11	Компьютерный тест (КТ-1)	2	1
12	Лабораторная работа № 9	4	2
13	Лабораторная работа № 10	4	2
13	Лабораторная работа № 11	4	2
14	Лабораторная работа № 12	4	2
15	Лабораторная работа № 13	4	2
15	Лабораторная работа № 14	4	2
15	Компьютерный тест (КТ-2)	2	1
17	Компьютерный тест (КТ-3)	2	1
18	Домашнее задание № 1	4	2
19	Домашнее задание № 2	4	2
	Итого за текущий контроль	***70***	***35***
	Итоговый контроль	***30***	***15***
	Накопленный рейтинг	**100**	**50**

В экзаменационную ведомость и зачетную книжку вносится не экзаменационная оценка по дисциплине, а ***итоговая 5-балльная оценка*** за семестр, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля учебной дисциплины.

Итоговая оценка студенту по дисциплине за семестр по 5-ти балльной шкале выставляется на основе накопленной им общей суммы баллов $R_{нак}$ по итогам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	**Оценка**
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Положительная оценка («отлично», «хорошо», «удовлетворительно») заносится в экзаменационную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в экзаменационную ведомость.

РАЗРАБОТЧИК

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор _____ А.А.Хорев

Рабочая программа дисциплины «Технологии защиты информации от утечки по техническим каналам» по направлению подготовки – 10.04.01 «Информационная безопасность», направленность (профиль) «Аудит информационной безопасности» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры 17 марта 2021 года, протокол № 3.

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор _____ А.А.Хорев

Лист согласования

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества
Начальник АНОК _____/ И.М.Никулина /

Рабочая программа согласована с библиотекой МИЭТ
Директор библиотеки _____/ Т.П.Филиппова /