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
«Контроль защищенности 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**:**

Компетенция ПК-1 «Способен проводить аттестацию автоматизированных систем, средств обработки информации на соответствие требованиям безопасности информации» сформулирована на основе профессионального стандарта «Специалист по технической защите информации», утверждённый приказом Минтруда России от 01.11.2016 № 599н. Регистрационный № 844.

Обобщенная трудовая функция G/7. Проведение аттестации объектов на соответствие требованиям по защите информации.

Трудовая функция G/01.7. Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ПК-1. Способен проводить аттестацию автоматизированных систем, средств обработки информации на соответствие требованиям безопасности информации	ПК-1. КЗИУТК Способен проводить аттестацию автоматизированных систем, средств обработки информации на соответствие требованиям безопасности информации.	**Знания** нормативные документы ФСТЭК России по контролю эффективности защиты информации от утечки по техническим каналам, организации аттестации объектов информатизации; методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам; методики аттестационных испытаний объектов СВТ по оценке защищенности информации от утечки по техническим каналам; организацию аттестации объектов информатизации по требованиям безопасности информации. **Умения:** разрабатывать программы и методики аттестационных испытаний объектов информатизации по требования безопасности информации; проводить контроль выполнения норм защищенности СВТ от утечки информации по техническим каналам; рассчитывать показатели защищенности СВТ от утечки информации по техническим каналам;

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		оформлять протоколы и заключения по результатам аттестационных испытаний объектов информатизации по требованиям безопасности информации. **Опыт практической деятельности:** разработки программы и методики аттестационных испытаний объектов информатизации по требования безопасности информации; проведения аттестационных испытаний объектов информатизации по оценке защищенности информации от утечки по техническим каналам; оформления протоколов и заключения по результатам аттестационных испытаний объектов информатизации по требованиям безопасности информации.

Компетенция ПК-2 «Способен проводить аттестацию выделенных (защищаемых) помещений на соответствие требованиям безопасности информации» сформулирована на основе профессионального стандарта «Специалист по технической защите информации», утверждённый приказом Минтруда России от 01.11.2016 № 599н. Регистрационный № 844.

Обобщенная трудовая функция G/7. Проведение аттестации объектов на соответствие требованиям по защите информации.

Трудовая функция G/02.7. Проведение аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ПК-2. Способен проводить аттестацию выделенных (защищаемых) помещений на соответствие требованиям безопасности информации	ПК-2.КЗИУТК Способен проводить аттестацию выделенных (защищаемых) помещений на соответствие требованиям безопасности информации.	**Знания:** нормативные документы ФСТЭК России по контролю эффективности защиты информации от утечки по техническим каналам, организации аттестации объектов информатизации; методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам; методики аттестационных испытаний выделенных помещений по оценке защищен-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		ности информации от утечки по техническим каналам; организацию аттестации выделенных помещений по требованиям безопасности информации. **Умения:** разрабатывать программы и методики аттестационных испытаний выделенных помещений по требования безопасности информации; проводить контроль выполнения норм защищенности речевой информации от утечки по техническим каналам; рассчитывать показатели защищенности речевой информации от утечки по техническим каналам; проводить специальную техническую проверку выделенного помещения с целью выявления электронных устройств перехвата речевой информации; оформлять протоколы и заключения по результатам аттестационных испытаний объектов информатизации (выделенных помещений) по требованиям безопасности информации. **Иметь практический опыт:** разработки программы и методики аттестационных испытаний объектов информатизации по требования безопасности информации; проведения аттестационных испытаний выделенных помещений на соответствие требованиям безопасности информации; оформления протоколов и заключения по результатам аттестационных испытаний выделенных помещений по требованиям безопасности информации.

В результате изучения дисциплины студент должен:

Знать:

нормативные документы ФСТЭК России по контролю эффективности защиты информации от утечки по техническим каналам, организации аттестации объектов информати-

зации;

методы и средства контроля эффективности защиты СВТ от утечки информации по техническим каналам;

методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам;

методы и средства выявления электронных устройств перехвата информации;

методики аттестационных испытаний объектов СВТ и выделенных помещений по оценке защищенности информации от утечки по техническим каналам;

организацию аттестации объектов информатизации и выделенных помещений по требованиям безопасности информации.

Уметь:

разрабатывать программы и методики аттестационных испытаний объектов информатизации по требования безопасности информации;

проводить контроль выполнения норм защищенности СВТ от утечки информации по техническим каналам;

рассчитывать показатели защищенности СВТ от утечки информации по техническим каналам;

проводить контроль выполнения норм защищенности речевой информации от утечки по техническим каналам;

рассчитывать показатели защищенности речевой информации от утечки по техническим каналам;

проводить специальную техническую проверку выделенного помещения с целью выявления электронных устройств перехвата речевой информации;

оформлять протоколы и заключения по результатам аттестационных испытаний объектов информатизации (выделенных помещений) по требованиям безопасности информации.

Иметь практический опыт:

разработки программы и методики аттестационных испытаний объектов информатизации по требования безопасности информации;

проведения аттестационных испытаний объектов информатизации по оценке защищенности информации от утечки по техническим каналам;

проведения аттестационных испытаний выделенных помещений на соответствие требованиям безопасности информации;

оформления протоколов и заключения по результатам аттестационных испытаний объектов информатизации по требованиям безопасности информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Контроль защищенности информации от утечки по техническим каналам» входит в часть, формируемую участниками образовательных отношщений Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 1-м курсе во 2-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», а также при изучении дисциплины «Технологии защиты информации от утечки по техническим каналам», изучаемой в 1-м семестре магистратуры.

Знания и умения, полученные в результате изучения дисциплины, используются в дисциплине «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*	Практическая подготовка при выполнении курсовой работы	Вид промежуточной аттестации
				ВСЕГО	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации			
1	2	5	180	84	24	40	-	20	60	22	Экз. (36), КР

* Часы на самостоятельную работы, включая часы на практическую подготовку при выполнении курсовой работы

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы*	Практическая подготовка при выполнении курсовой работы	Формы текущего контроля
	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации			
1. «Методы и средства контроля эффективности защиты информации, обрабатываемой СВТ».	4	12	-	5	11	-	Компьютерный тест КТ-1. Зачет по Лр 1-3
2. «Методы и средства контроля эффективности защиты речевой информации».	4	12	-	5	11	-	Компьютерный тест КТ-2. Зачет по Лр 4-6

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы*	Практическая подготовка при выполнении курсовой работы	Формы текущего контроля
	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации			
3. «Методы и средства выявления электронных устройств перехвата речевой информации».	8	8	-	5	8	-	Компьютерный тест КТ-3. Зачет по Лр 7-8
4. «Организация аттестации объектов информатизации по требованиям безопасности информации».	8	8	-	5	30	22	Компьютерный тест КТ-4. Зачет по Лр 9-10. Сдача КР

* Часы на самостоятельную работы, включая часы на практическую подготовку при выполнении курсовой работы

4.1. Лекционные занятия

Номер модуля дисциплины	**Номер лекции**	**Объем занятий, часы**	**Краткое содержание**
1	1.	2	**Методы и средства контроля эффективности защиты информации, обрабатываемой СВТ:** Показатели эффективности защиты информации, обрабатываемой СВТ, от утечки по техническим каналам. Методы контроля эффективности защиты информации, обрабатываемой СВТ. Требования к средствам измерения ПЭМИН СВТ и условиям проведения измерений.
	2.	2	**Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН:** Порядок проведения аттестационных испытаний СВТ при контроли эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИ. Порядок проведения аттестационных испытаний СВТ при контроле эффективности защиты СВТ от утечки информации, возникающей за счет наводок информативных сиг-

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			налов на токопроводящие коммуникации.
2	3.	2	**Методы и средства контроля выполнения норм защищенности речевой информации от утечки по техническим каналам:** Показатели защищенности речевой информации от утечки речевой информации по техническим каналам. Методы контроля эффективности защиты ВП от утечки речевой информации по техническим каналам. Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по прямым акустическим, акустовибрационным и акустооптическому каналам. Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по акустоэлектрическим каналам.
	4.	2	**Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по техническим каналам:** Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по прямым акустическим каналам. Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по акустовибрационным и акустооптическому каналам. Порядок проведения контроля ВТСС на подверженность акустоэлектрическим преобразованиям. Порядок проведения контроля ВТСС на подверженность «высокочастотному навязыванию».
3	5.	2	**Классификация методов поиска электронных устройств перехвата информации:** Демаскирующие признаки электронных устройств перехвата информации. Классификация методов и средств поиска электронных устройств перехвата информации. Порядок специальной проверки ВП на наличие возможно внедренных закладочных устройств.
	6.	2	**Методы и средства поиска электронных устройств перехвата информации:** Методы и средства выявления скрытых систем видеонаблюдения. Методы выявления закладочных устройств с использованием ИЭМП.

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			Методы выявления закладочных устройств с использованием нелинейных локаторов и рентгено-телевизионных комплексов.
	7.	2	**Методы выявления закладочных устройств с использованием сканирующих приемников:** Методы выявления закладочных устройств с использованием сканирующих приемников и интерсепторов. Сканирующие приемники (основные характеристики). Интерсепторы.
	8.	2	**Методы выявления закладочных устройств с использованием программно-аппаратных комплексов:** Методы выявления закладочных устройств с использованием ПАКРК. Программно-аппаратные комплексы радиоконтроля (основные характеристики). Методы и средства выявления закладочных устройств, подключаемым к проводным коммуникациям. Программно-аппаратные комплексы анализа проводных коммуникаций (основные характеристики).
4	9.	2	**Организация аттестации объектов информатизации:** Порядок организации аттестации ОИ (ВП) требованиям по безопасности информации. Подготовка к проведению аттестации ОИ (ВП). Программа и методика аттестационных испытаний ОИ (ВП)
	10.	2	**Порядок проведения аттестационных испытаний:** Порядок проведения аттестационных испытаний ОИ. Порядок проведения аттестационных испытаний ВП
	11.	2	**Специальное обследование ОИ (ВП)** Специальное обследование ОИ. Специальное обследование ВП.
	12.	2	**Оформление результатов аттестационных испытаний:** Протоколы оценки защищенности ОИ (ВП). Заключение по результатам аттестации ОИ (ВП). Аттестат соответствия ОИ (ВП).

4.2. Практические занятия

Не предусмотрены

4.3. Лабораторные работы
(практическая подготовка при проведении лабораторных работ)

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
1	1.	4	**Контроль выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИН**: Измерение ПЭМИ СВТ. Измерение наводок ПЭМИ СВТ в случайных антеннах. Измерение уровня шумов в случайных антеннах, создаваемых системами пространственного и линейного электромагнитного зашумления.
	2.	4	**Контроль выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИН**: Измерение реального затухания ПЭМИ. Измерение реального затухания наводок ПЭМИ СВТ в линиях электропитания и в токопроводящих коммуникациях. Измерение уровня электромагнитных шумов системы пространственного электромагнитного зашумления.
	3.	4	**Оценка выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИН:** Оценка выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИ. Оценка выполнения норм защищенности СВТ от утечки информации, возникающей за счет наводок ПЭМИ в линиях электропитания и в токопроводящих коммуникациях. Составление протокола оценки защищенности СВТ от утечки информации по каналам ПЭМИН.
2	4.	4	**Контроль выполнения норм защищенности речевой информации от утечки по прямым акустическим и акустовибрационным каналам:** Измерение звукоизоляции ограждающей конструкции. Измерение реального затухания акустических сигналов. Измерение уровня акустических шумов. Измерение виброизоляции ограждающей конструкции. Измерение уровня вибрационных шумов. Измерение реального затухания вибрационных сигналов. Измерение уровня вибрационных шумов, создаваемых системой виброакустической защиты, на зашумляемых поверхностях
	5.	4	**Оценка выполнения норм защищенности речевой информации от утечки по прямым акустическим, акустовибрационным и акустооптическому каналам:** Оценка выполнения норм защищенности речевой информации от утечки по прямым акустическим каналам. Оценка выполнения

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			норм защищенности речевой информации от утечки по акустовибрационным и акустооптическому каналам. Составление протокола оценки эффективности защиты акустической речевой информации от утечки информации по техническим каналам.
	6.	4	**Контроль выполнения норм защищенности речевой информации от утечки по акустоэлектрическим и акустоэлектромагнитным каналам:** Контроль вспомогательных технических средств (ВТСС) на подверженность акустоэлектрическим преобразованиям. Контроль вспомогательных технических средств (ВТСС) на подверженность акустоэлектромагнитным преобразованиям. Контроль ВТСС на подверженность «высокочастотному навязыванию» Составление протокола оценки эффективности защиты акустической речевой информации от утечки информации по техническим каналам.
3	7.	4	**Выявление закладных устройств с использованием средств поиска индикаторного типа:** Поиск закладных устройств с использованием ИЭМП. Поиск скрытых видеокамер с использованием оптико-электронных средств. Поиск закладных устройств с использованием нелинейных локаторов. Поиск закладных устройств с использованием сканирующих радиоприемников и интерсепторов.
	8.	4	**Выявление закладных устройств с использованием программно-аппаратных комплексов** Выявление закладных устройств, подключаемых к проводным коммуникациям (телефонным линиям, линиям электросети и т.д.) с использованием проводных анализаторов Поиск закладных устройств с использованием программно-аппаратных комплексов радиоконтроля.
4	9.	4	Разработка программы и методики аттестационных испытаний объекта информатизации на соответствие требованиям по безопасности информации.
	10.	4	**Оформление результатов аттестационных испытаний** Разработка протокола оценки защищенности СВТ от утечки информации по каналам ПЭМИН. Разработка протокола оценки выполнения норм противодействия акустической речевой разведке в ВП

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			Разработка заключения по результатам аттестации ОИ (ВП). Разработка аттестата соответствия ОИ (ВП).

4.4. Самостоятельная работа студентов

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

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
	2	**Подготовка к компьютерному тесту КТ-2** Изучение материалов лекции №№ 3 - 4 и рекомендованной литературы.
3	3	**Подготовка к лабораторной работе № 7** Изучение материалов лекции №№ 5 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 7
	3	**Подготовка к лабораторной работе № 8** Изучение материалов лекции №№ 5 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 8
	2	**Подготовка к компьютерному тесту КТ-3** Изучение материалов лекции №№ 5 - 8 и рекомендованной литературы.
4	3	**Подготовка к лабораторной работе № 9** Изучение материалов лекции №№ 9 -12 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 9
	3	**Подготовка к лабораторной работе № 10** Изучение материалов лекции №№ 9 -12 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 10
	2	**Подготовка к компьютерному тесту КТ-4** Изучение материалов лекции №№ 9 - 12 и рекомендованной литературы.
	22	**Выполнение курсовой работы**

4.5. Примерная тематика курсовых работ (проектов)

Тема курсовой работы «Аттестация объекта информатизации по требованиям безопасности информации».

Аттестуемые объекты (по выбору студента):

– объект информатизации, в котором установлено автоматизированное рабочее место для обработки конфиденциальной информации на базе ПЭВМ;

– помещение, предназначенное для ведения конфиденциальных переговоров.

Для аттестации студентам выделяются реальные объекты информатизации предприятий (учреждений).

Аттестационные испытания объектов информатизации студентами проводятся в ходе производственной практики.

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. Методы и средства контроля эффективности защиты информации, обрабатываемой СВТ:

Тексты лекций № 1 – 2. ОРИОКС// URL: http://orioks.miet.ru/

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

Модуль 2. Методы и средства контроля эффективности защиты речевой информации

Тексты лекций № 3 – 4. ОРИОКС// URL: http://orioks.miet.ru/

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

Модуль 3. Методы и средства выявления электронных устройств перехвата речевой информации:

Тексты лекций № 3 – 8. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 7 – 8. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 4. Организация аттестации объектов информатизации по требованиям безопасности информации.

Тексты лекций № 9 – 12. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 9 – 10. ОРИОКС// URL: http://orioks.miet.ru/

Руководство по выполнению курсовой работы ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Технические средства и методы защиты информации: учебник для вузов/ А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков/Под ред. А.П. Зайцева, А.А. Шелупанова. - 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.

2. Хорев, А.А. Техническая защита информации: учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А. А. Хорев. - М. : НПЦ "Аналитика", 2008. - 436 с. - ISBN 978-59901488-1-9.

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 наводок 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 конфи-

денциальной 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 Information technologies. Basic terms and definitions in scope of technical protection of information, Национальный стандарт РФ: Введ. 01.01.2006.- М.: Стандартинформ, 2018.

7. Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения: Technical information protection. Terms and definitions Национальный стандарт РФ: Введ. 01.06.2006.- М.: Стандартинформ, 2006.

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: с изм. на 02 июля 2021 г.- «Об информации, информационных технологиях и о защите информации»; Текст: электронный // Техэксперт : [сайт]. – URL: https://docs.cntd.ru/document/901990051 - (дата обращения 15.03.2021).-Текст электронный .

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: 15.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

5.

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 микрофо-	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome/Explorer).

	ном). 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 электромагнитного зашум-	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

	ления (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 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 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	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 шт.

	– 27 шт.	

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ПК-1. КЗИУТК. «Способен проводить аттестацию автоматизированных систем, средств обработки информации на соответствие требованиям безопасности информации».

ФОС по подкомпетенции ПК-2. КЗИУТК. «Способен проводить аттестацию выделенных (защищаемых) помещений на соответствие требованиям безопасности информации».

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 курсовой работы.

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

Лабораторные работы выполняются студентами в группе по 3-4 человека. По результатам выполнения каждой лабораторной работы каждый студент оформляет и представляет отчет. При защите отчетов по лабораторным работам преподаватель разбирает типовые ошибки и указывает их причины.

Курсовая работа (КР) направлена на формирование профессиональных компетенции. КР выполняются студентами в группе по 3-4 человека. По результатам выполнения КР каждый студент оформляет и представляет отчет. При защите отчетов по КР 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: групповая, при которой студенты выполняют одно 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 курсовой работы

Тема курсовой работы «Аттестация объекта информатизации по требованиям безопасности информации».

Задачи выполнения курсовой работы:

обучение студентов самостоятельному применению полученных знаний для решения конкретных практических задач аттестации объектов информатизации;

развитие навыков подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по организации и проведению аттестации объектов информатизации;

овладение методами контроля эффективности защиты информации от утечки по техническим каналам;

получение навыков разработки программы и методики аттестационных испытаний объектов информатизации;

получение опыта проведения аттестационных испытаний объектов информатизации;

получения навыков расчета показателей защищенности СВТ от утечки информации по техническим каналам;

получения навыков расчета показателей защищенности речевой информации от утеч-

ки по техническим каналам;

получения навыков оформления протоколов и заключения по результатам аттестационных испытаний объектов информатизации по требованиям безопасности информации.

Аттестуемые объекты (по выбору студента):

– объект информатизации, в котором установлено автоматизированное рабочее место для обработки конфиденциальной информации на базе ПЭВМ;

– помещение, предназначенное для ведения конфиденциальных переговоров.

Для аттестации студентам выделяются реальные объекты информатизации предприятий (учреждений). Аттестационные испытания студентами проводятся в ходе производственной практики.

Аттестационные испытания студентами проводятся в ходе производственной практики.

При проведении аттестационных испытаний студенты проводят:

Для объекта информатизации (ОИ):

1. Анализ полноты исходных данных, проверка их соответствия фактическим условиям размещения, монтажа и эксплуатации технических средств ОИ.
2. Исследование технологического процесса обработки и хранения информации,
3. Проверку состояния организации работ и выполнения требований по защите информации:
   A. Проверку достаточности представленных документов и соответствия их содержания установленным требованиям.
   B. Проверку правильности категорирования технических средств.
   C. Проверку уровня подготовки специалистов и распределения ответственности пользователей ОИ.
   D. Экспертизу протоколов специальных исследований технических средств, предписаний на эксплуатацию технических средств.
   E. Проверку выполнения требований к помещениям, в которых производится обработка информации.
4. Проверку ОТСС на соответствие требованиям по защите информации от утечки по техническим каналам за счет ПЭМИН:
   A. Проверку выполнения требований по защите информации от утечки за счет побочных электромагнитных излучений средств вычислительной техники;
   B. Проверку соответствия фактических размеров КЗ представленным документам.
   C. Проверку соответствия размеров КЗ требованиям предписаний на эксплуатацию ОТСС и других документов, определяющих требования к размеру зоны R2.
   D. Проверку наличия сертификатов на средства защиты информации, работоспособности средств защиты информации и выполнения правил их эксплуатации.
   E. Аппаратурные испытания эффективности защиты информации от утечки за счет побочных электромагнитных излучений ОТСС.
5. Проверку выполнения требований по защите информации от утечки за счет наводок информативных сигналов на цепи электропитания и заземления ПЭВМ:
   A. Проверку выполнения требований к электропитанию технических средств, монтажу питающих кабелей, фильтрации сигналов в цепях питания.

B. Проверку выполнения требований к заземлению технических средств, правилам монтажа заземляющих конструкций, величине сопротивления заземлителя и регламентному контролю его значений.
C. Проверку наличия сертификатов на средства защиты информации, работоспособности средств защиты информации и выполнения правил их эксплуатации.
D. Аппаратурные испытания эффективности защиты информации от утечки по цепям заземления и электропитания технических средств.

6. Проверку выполнения требований по защите информации от утечки за счет наводок информативных сигналов на ВТСС и их кабельные коммуникации, имеющие выход за границу КЗ:
A. Проверку взаимного размещения ОТСС и ВТСС на соответствие требованиям предписаний на эксплуатацию технических средств и других документов, определяющих размеры зон r1 и r1'.
B. Проверку работоспособности средств защиты и выполнения правил их монтажа и эксплуатации.
C. Аппаратурные испытания защиты информации от утечки за счет наводок на ВТСС и их кабельные коммуникации.
7. Проверку выполнения требований по защите ОТСС от утечки информации за счет возможно внедренных в них специальных электронных устройств перехвата информации **(**Проверяется наличие актов или заключений о специальной проверке ОТСС, входящих в состав ПЭВМ, наличие специальных голографических марок на проверенных средствах и их соответствие указанным номерам в документах о специальной проверке).

Для выделенного помещения (ВП):

1. Анализ полноты исходных данных, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации технических средств, установленных в ВП;
2. Проверку состояния организации работ и выполнения требований по защите информации, оценка правильности категорирования ВП, оценка полноты и уровня разработки организационно-распорядительной, проектной и эксплуатационной документации, оценка уровня подготовки специалистов, обеспечивающих защиту информации в ВП и распределения ответственности должностных лиц, эксплуатирующих ВП, за выполнение требований безопасности информации;
3. Проверку выполнения требований по защите ВП от утечки акустической речевой информации по акустическому и виброакустическому каналам:
A. Проверку соответствия расположения и конструкции ВП требованиям по безопасности информации от утечки по акустическому каналу.
B. Проверку соответствия расположения и конструкции ВП требованиям по безопасности информации от утечки по виброакустическому каналу.
C. Проверку работоспособности средств защиты информации и выполнения правил их эксплуатации.
D. Аппаратурные испытания защищенности (эффективности защиты) информации от утечки по акустическому каналу.
E. Аппаратурные испытания защищенности (эффективности защиты) информации от утечки по виброакустическому каналу.

4. Проверку ВП на соответствие требованиям по защите информации от утечки акустической речевой информации по проводным линиям и цепям ОТСС и ВТСС за счет акусто-электрических преобразований и паразитной генерации.
5. Проверку выполнения требований по защите ВП от утечки информации за счет возможно внедренных специальных электронных устройств перехвата информации.

После проведения аттестационных испытаний студенты оформляют:

При аттестации ОИ:

1. Протокол оценки защищенности ОИ от утечки информации по каналам ПЭМИН.
2. Заключение по результатам аттестационных испытаний ОИ по требованиям безопасности информации.

При аттестации ВП:

1. Протокол оценки защищенности речевой информации от утечки по прямым и акустовибрационным каналам.
2. Заключение по результатам аттестационных испытаний ВП по требованиям безопасности информации.

Курсовая работа выполняется на основе глубокого изучения основной и дополнительной литературы по дисциплине (учебники, учебные пособия, монографии, журналы и другие периодические издания, сайты в INTERNET). При выполнении курсовой работы рекомендуется широко использовать внутренние документы организаций, а также привлекать различного рода официальную, справочную, инструктивную, методическую, нормативную и другую документацию.

Структура курсовой работы должна отвечать традиционным требованиям, предъявляемым к научным работам и включать следующие части (структурные элементы):

Титульный лист.

Задание на КР.

Реферат.

Содержание.

Перечень условных обозначений и сокращений.

Введение.

Основная часть (основные разделы работы, предусмотренные заданием).

Заключение.

Список использованных источников.

Приложения.

Объем пояснительно записки составляет 50 – 70 страниц машинописного текста с приложениями, выполненных на стандартных листах формата А4.

Титульный лист является первым листом в пояснительной записке.

Реферат – это сокращенное изложение содержания и существа КР с основными сведениями о выполненных разработках и полученных результатах.

Реферат имеет следующую структуру:

− перечень количественных сведений о КР;

− перечень ключевых слов;

− текст реферата.

Перечень количественных сведений о КР должен включать количество: ___ с., ___

рис., ___ табл., __ источник, ___ прил.)..

Перечень ключевых слов должен включать от 5 до 15 слов или словосочетаний из текста КР, которые в наибольшей мере характеризуют содержание и обеспечивают возможность информационного поиска. Ключевые слова приводятся в именительном падеже и печатаются строчными буквами в строку через запятые.

Текст реферата в общем случае должен отражать сведения:

− об объекте аттестации;

− о цели аттестации;

− об использованных методах и средствах, использованных при аттестационных испытаниях;

− о результатах аттестации.

Если КР не содержит сведений по какой-либо из перечисленных структурных частей реферата, то в тексте реферата она опускается, при этом последовательность изложения сохраняется.

Объем реферата определяется содержанием КР, количеством сведений и их научной и практической ценностью. Средний объем реферата составляет 1500 − 2000 знаков.

Перечень условных обозначений и сокращений. Принятые в работе малораспространенные условные обозначения, сокращения, символы, единицы и специфические термины необходимо представлять в виде отдельного списка. Если сокращения, условные обозначения, символы, единицы и термины повторяются в работе менее трех раз, отдельный список не составляют, а расшифровку дают непосредственно в тексте при первом упоминании.

Содержание пояснительной записки включает введение, наименования всех разделов, подразделов и пунктов (если последние имеют наименования), заключение, список использованных источников и наименование приложений с указанием номеров страниц, с которых начинаются эти элементы пояснительной записки.

Введение должно содержать:

− общие сведения о целях, задачах и организации аттестации объектов информатизации;

− постановку задачи исследования с указанием цели, используемых методов и средств;

− исходные данные по аттестуемому объекту;

− планируемые результаты.

Объем введения 3 − 5 страниц.

Основная часть. Основная часть должна включать:

При аттестации ОИ:

Программу и методики аттестационных испытаний ОИ.

Протокол оценки защищенности ОИ от утечки информации по каналам ПЭМИН.

Заключение по результатам аттестационных испытаний ОИ по требованиям безопасности информации.

При аттестации ВП:

Программу и методики аттестационных испытаний ОИ.

Протокол оценки защищенности речевой информации от утечки по прямым и акустовибрационным каналам.

Протокол контроля подверженности ВТСС акустоэлектрическим преобразованиям.

Заключение по результатам аттестационных испытаний ВП по требованиям безопас-

ности информации.

Заключение должно содержать:

− краткие выводы по результатам выполнений работы;

− оценку полноты решений поставленных задач.

Типовой объем заключения составляет 1-2 страницы.

Список использованных источников должен содержать сведения обо всех источниках, использованных при написании КР. В список следует включать только те наименования, с которыми автор КР ознакомился лично. На все источники, приведенные в списке, должны быть ссылки в тексте. На источники, содержащие общие сведения по теме ВКР, ссылки делаются обычно во введении.

Источники в списке нумеруются в порядке появления ссылок в тексте.

При оформлении библиографического описания источников в списке необходимо руководствоваться ГОСТ 7.1–2003.

Приложения. В приложения выносится протоколы измерений, планы и план-схемы объекта информатизации, схемы электропитания, заземления объекта, схемы инженерных коммуникаций, линий связи и т.д.

Все приложения нумеруются и располагаются в конце пояснительной записки в порядке ссылок на них. Каждое приложение начинается с новой страницы и имеет содержательный заголовок. При необходимости текст приложения может быть разбит на разделы, подразделы, пункты и подпункты, которые следует нумеровать в пределах каждого приложения в соответствии с требованиями для основной части записки.

Курсовая работа должна быть написана студентом самостоятельно, грамотно, по логически построенному плану. Прямое переписывание в работе текста из учебной и научной литературы не допускается.

11.3. 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), 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 – $R_{нор}$).

Структура и график контрольных мероприятий приведены в таблице 11.1 и 11.2.

Таблица 11.1

Структура и график контрольных мероприятий дисциплины

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
7	Лабораторная работа № 1	4	2
8	Лабораторная работа № 2	4	2

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
9	Лабораторная работа № 3	4	2
9	Компьютерный тест (КТ-1)	4	2
10	Лабораторная работа № 4	4	2
11	Лабораторная работа № 5	4	2
12	Лабораторная работа № 6	4	2
12	Компьютерный тест (КТ-2)	4	2
13	Лабораторная работа № 7	4	2
14	Лабораторная работа № 8	4	2
11	Компьютерный тест (КТ-3)	4	2
15	Лабораторная работа № 9	4	2
16	Лабораторная работа № 10	4	2
16	Компьютерный тест (КТ-4)	4	2
16	Посещаемость, активность	4	2
	Итого за текущий контроль	***60***	***30***
	Итоговый контроль	***40***	***20***
	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

Таблица 11.1

Структура и график контрольных курсовой работы

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
8	Контроль № 1	10	5
12	Контроль № 2	10	5
16	Контроль № 3	10	5
17	Итоговый просмотр (оценка качества кур-	50	25

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
	совой работы)		
	Итого за текущий контроль	***80***	***40***
18	***Итоговый контроль*** *(защита курсовой работы)*	***20***	***10***
	Накопленный рейтинг	**100**	**50**

За курсовую работу в зачетную ведомость и зачетную книжку вносится ***итоговая 5-балльная оценка***, рассчитанная на основе накопленных рейтинговых баллов по результатам 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 зачетную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в зачетную ведомость.

РАЗРАБОТЧИК

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

Рабочая программа дисциплины «Контроль защищенности информации от утечки по техническим каналам» по направлению подготовки 10.04.01 «Информационная безопасность», направленности (профилю) «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 /