МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» ____02_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Защита информации от утечки по техническим каналам»

Направление подготовки
10.04.01 Информационная безопасность

Образовательная программа (профиль)
Системы управления информационной безопасностью

Квалификация (степень) выпускника
Магистр

Форма обучения
Очная

Москва, 2023 г.

Разработчик:

Доцент кафедры «Информационная безопасность», к.э.н., доцент по кафедре «Информационная безопасность»

/ Ю.Н. Рагозин /

Согласовано:

И.о. заведующего кафедрой «Информационная безопасность»,

А.Ю. Гневшев

Руководитель образовательной программы
Доцент. к.т.н.

/С.А. Кесель/

Содержание

1. Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Защита информации от утечки по техническим каналам» следует отнести:

- теоретическую и практическую подготовленность магистра к формированию требований по защите информации от утечки по техническим каналам в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости

К **основным задачам** освоения дисциплины следует отнести:

- изучение и усвоение директивных и нормативно-методических документов Федеральной службы технического и экспортного контроля (ФСТЭК) по направлению защиты информации от утечки по техническим каналам;
- практическое ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, автоматизированными системами и с техническими каналами утечки акустической (речевой) информации;
- изучение способов и средств защиты информации от утечки по техническим каналам;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации защиты информации от утечки по техническим каналам на объектах информатизации.

Обучение по дисциплине направлено на формирование у обучающихся следующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК-3	**Способен** проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	**Знать**: - отечественные и международные стандарты информационной безопасности; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - основные методы и средства, в отношении которых отсутствует необходимость присвоения им категорий значимости категорий значимости обеспечения безопасности операционных систем; - основные методы и средства обеспечения сетевой безопасности; основные методы и средства обеспечения безопасности в системах управления базами данных. **Уметь**: - обосновывать принципы организации технического, программного и информационного

		обеспечения информационной безопасности объекта защиты; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности. **Владеть**: - навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; - навыками настройки подсистем защиты основных операционных систем
ПК-7	**Способен** проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	**Знать:** - методы экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. **Уметь:** - проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. **Владеть**: - навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации от утечки по техническим каналам» относится к числу профессиональных учебных элективных дисциплин №2 (Б1.2.ЭД.2.2) основной образовательной программы магистратуры.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП специалитета по направлению подготовки 10.05.03 (Информационная безопасность автоматизированных систем): «Математический анализ», «Теория вероятностей», «Электроника и схемотехника», «Физические основы информационной безопасности», «Основы информационной безопасности».

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **4** зачетных единиц, т.е. **144** академических часов (лабораторные занятия – 72 часа, самостоятельная работа – 72 часа), форма контроля – **экзамен** в 3 семестре.

3.1. Виды учебной работы и трудоемкость (по формам обучения)

Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	3	1-18
	В том числе:			
1.1	Лекции	-	-	1-18
1.2	Семинарские/практические занятия	-	-	-
1.3	Лабораторные занятия	**72**	3	1-18
2	**Самостоятельная работа**	**72**	3	1-18
3	**Промежуточная аттестация**		3	
	Экзамен		3	По расписанию
	Итого:	**144**		

3.2. Тематический план изучения дисциплины (по формам обучения)

Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Тема 1. ФСТЭК-регулятор технической защиты информации в государственной системе защиты информации в Российской Федерации	13		-	4	-	9
2	Тема 2. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	21		-	12	-	9
3	Тема 3. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	19		-	10	-	9
4	Тема 4. Технические каналы утечки акустической (речевой) информации	19		-	10	-	9
5	Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам	19		-	10	-	9
6	Тема 6. Методы и средства контроля эффективности защиты автоматизированных систем от утечки информации по каналам ПЭМИН и защищаемых (выделенных) помещений от утечки речевой информации по техническим каналам.	21		-	12	-	9
7	Тема 7. Методы и средства выявления электронных устройств негласного получения информации	17		-	8	-	9
8	Тема 8. Организация технической защиты информации	15		-	6	-	9
Итого		**144**			**72**		**72**

3.3. Содержание дисциплины

Темы лекций дисциплины и для самостоятельного изучения:

Тема 1. ФСТЭК-регулятор технической защиты информации в государственной системе защиты информации в Российской Федерации

Нормативно-методические и директивные документы ФСТЭК по технической защите информации.

Термины и определения в области технической защиты информации: объект информатизации, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

Тема 2. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации, создаваемый путем внедрения в СВТ электронных устройств негласного получения информации.

Тема 3. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Классификация способов и средств защиты объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке). Защищённые средства вычислительной техники.

Тема 4. Технические каналы утечки акустической (речевой) информации

Характеристики речевого сигнала. Общая характеристика и классификация технических каналов утечки акустической информации. Прямые акустические каналы утечки речевой информации. Акустовибрационные каналы утечки речевой информации. Акустооптический (оптикоэлектронный, лазерный) канал утечки речевой информации.

Акустоэлектрические каналы утечки речевой информации. Акустоэлектромагнитные каналы утечки речевой информации. Средства акустической разведки и их технические характеристики

Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке). Способы и средства защиты вспомогательных технических средств и систем. Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

Тема 6. Методы и средства контроля эффективности защиты автоматизированных систем от утечки информации по каналам ПЭМИН и защищаемых (выделенных) помещений от утечки речевой информации по техническим каналам

Отношение сигнал-помеха, как нормативный показатель защищенности информации при обработке в автоматизированных системах. Определение зон **R2** и **r1.** Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Методика оценки возможностей средств акустической разведки по перехвату речевой информации. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Тема 7. Методы и средства выявления электронных устройств негласного получения информации

Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.

Тема 8. Организация технической защиты информации

Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации.

Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты. Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию.

Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации. Порядок документального оформления результатов аттестационных испытаний и соответствия объекта информатизации требованиям по безопасности информации.

3.4. Тематика семинарских/практических и лабораторных занятий

Проведение семинарских и практических занятий по данной дисциплине учебным планом не предусмотрено.

Тематика лабораторных работ:

Лабораторная работа №1

Выявление каналов утечки информации за счет акустоэлектрических преобразований в ВТСС

Лабораторная работа № 2

Определение требуемого радиуса контролируемой зоны Rкз для защиты конфиденциальной информации от утечки по каналу побочных электромагнитных излучений

Лабораторная работа №3

Оценка защищенности ОТСС от наводок ПЭМИ на линии и коммуникации, выходящие за пределы контролируемой зоны

Лабораторная работа № 4

Инструментально-расчетное определение коэффициентов звукоизоляции и виброизоляции ограждающих конструкций защищаемых помещений на базе многофункционального поискового прибора ST-031 «Пиранья»

Лабораторная работа №5

Поиск и анализ сигналов ПЭМИ от ОТСС на базе программно-аппаратного комплекса «Навигатор-П-3Г»

Лабораторная работа №6

Обнаружение и локализация закладных устройств негласного съема информации измерителем спектра вторичных полей «NR-μ»

Лабораторная работа №7

Контроль эффективности защиты речевой информации от утечки по прямому акустическому и акустовибрационному каналам программно-аппаратным комплексом ПАК «Спрут-мини»

Лабораторная работа №8

Система акустической и виброакустической защиты информации «СОНАТА-АВ»

Лабораторная работа №9

Анализатор проводных линий «Отклик-2». Генератор шума по сети 220В SEL SP 41/С

3.5. Тематика курсовых проектов

Курсовое проектирование по дисциплине «Защита информации от утечки по техническим каналам» рабочим планом не запланировано.

4. Учебно-методическое и информационное обеспечение

4.1. Нормативные документы и ГОСТы

1. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК. 2008 г. https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g
2. Методический документ "Меры защиты информации в государственных информационных системах" (утв. ФСТЭК РФ 11 февраля 2014 г.) **https://it-security.admin-smolensk.ru/zakonodatelstvo/normativnye-dokumenty-fstek-rossii/metodicheskij-dokument-mery-zaschity-informacii-v-gosudarstvennyh-informacionnyh-sistemah-/**
3. ГОСТ Р 59712–2022 "Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты".
4. ГОСТ 7.1–84. Библиографическое описание документа. Общие требования и правила составления. – М., 1985.

4.2. Основная литература

1. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации: учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург: Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337

2. Рагозин Ю.Н. Инженерно-техническая защита информации: учебное пособие - ИЦ «Интермедия» Санкт-Петербург, 2018 – 168 с. (библиотечный фонд Мосполитеха -50 экз.)

3. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург: Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст: электронный// Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009

4. Технические средства защиты объектов. Часть 1. Основные понятия. Принципы построения средств инженерно-технической защиты объектов / Б. Г. Ануфриев, О. В. Трубиенко, В. В. Филатов, А. А. Худяков. – М.: МИРЭА - Российский технологический университет, 2020. –

144 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://reader.lanbook.com/book/256700

4.3. Дополнительная литература

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. том 1 Технические каналы утечки информации – М.: НПЦ «Аналитика», 2010 – 436 с.

2. Торокин А.А. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в обл. информ. Безопасности – М.: Гелиос АРВ, 2005 -960 с.

3. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки: учебное пособие – М.: Российск. гос. гуманитарный ун-т, 2002 – 399 с.

4.4. Электронные образовательные ресурсы

1. Рагозин Ю.Н. ЭОР - Курс: «Техническая защита информации». СДО «Мосполитеха», 2022 г., https://online.mospolytech.ru/
2. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань https://mospolytech.ru/obuchauschimsya/biblioteka/

4.5. Современные профессиональные базы данных и информационные справочные системы

1. Банк данных угроз безопасности информации ФСТЭК России https://bdu.fstec.ru/

5. Материально-техническое обеспечение

Для проведения лабораторных работ необходимы:

- анализатор спектра с демодуляторами с полосой частот 9КГц-3ГГц;
- интерфейс анализатора спектра с компьютером (GPIB, USB);
- набор электрических и магнитных антенн (полоса частот 9КГц-3ГГц);
- эквивалент сети;
- генераторы пространственного и линейного электромагнитного зашумления;
- генераторы акустического и виброакустического зашумления;
- программно-аппаратный комплекс «СПРУТ-мини»;
- многофункциональный поисковый прибор SN-031 «Пиранья»;
- измеритель спектра вторичных полей (детектор нелинейных переходов) «NR- μ»;
- генератор виброакустического шума "Соната АВ";
- генератор шума по сети 220В SEL SP 41/C;
- программно-аппаратного комплекса «Навигатор-П-3Г»

Для проведения презентаций по тематике лабораторных работ помещения должны быть оборудованы современными электронными досками.

При проведении лабораторных работ с использованием специального программного обеспечения рекомендуется применение аттестованных тестовых программ из единой базы тестов ФСТЭК.

6. Методические рекомендации

6.1. Методические рекомендации для преподавателя по организации обучения

При подготовке к лабораторным работам следует предварительно проработать теоретический материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить для лабораторной работы необходимую контрольно-измерительную аппаратуру и специальные программно-аппаратные комплексы контроля эффективности защиты информации от утечки по техническим каналам.

При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать правильность выполнения лабораторных работ на всех этапах в соответствии с используемым инструментально-расчетным методом.

6.2. Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи с учебным планом. Основой теоретической подготовки студентов являются лекции, методические и теоретические материалы, предоставляемые преподавателем перед каждой лабораторной работой, а также **самостоятельная работа студентов** в соответствии с тематическим планом.

В процессе самостоятельной работы студенты самостоятельно изучают темы учебной программы. закрепляют и углубляют знания, полученные во время лабораторных занятий, готовятся к экзамену.

Лабораторные занятия проводятся по наиболее важным темам дисциплины. Особое внимание обращается на развитие умений и навыков работы с программно-аппаратными комплексами, которые используются в профессиональной деятельности специалистов по информационной безопасности.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Лабораторные работы проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков работы с программно-аппаратными комплексами, предназначенными для профессиональной деятельности будущего специалиста по информационной безопасности автоматизированных систем.

Лабораторные работы предполагают также проведение творческих дискуссий, активный обмен мнениями по рассматриваемым вопросам, заслушивание и обсуждение докладов (презентаций) по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия

требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме лабораторной работы и дать перечень литературы по теме. При проведении лабораторных работ преподаватель выполняет, в основном, функции ведущего - следит за регламентом времени, помогает уточнить формулировки, помогает с развертыванием и включением в работу программно-аппаратных комплексов, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа по дисциплине предполагает выполнение студентами домашних заданий (подготовка презентаций по темам дисциплины). Домашние задания содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, посещение различных выставок и конференций по проблемным вопросам технической защиты информации, использование справочной литературы и др.

При выдаче заданий (тем презентаций) для самостоятельной работы используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умение студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

7. Фонд оценочных средств

7.1. Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2. Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: - отечественные и международные стандарты информационной безопасности; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - основные методы и средства, в отношении которых отсутствует необходимость присвоения им категорий значимости обеспечения безопасности операционных систем; - основные методы и средства	Обучающийся демонстрирует **полное отсутствие** или недостаточное знание: -отечественных и международных стандарты информационной безопасности; - основных принципов организации технического, программного и информационного обеспечения защищенных информационных систем; -основных методов и средств, в отношении которых отсутствует необходимость присвоения им категорий значимости обеспечения сетевой безопасности;	Обучающийся демонстрирует **частичное знание** -отечественных и международных стандарты информационной безопасности; - основных принципов организации технического, программного и информационного обеспечения защищенных информационных систем; -основных методов и средств, в отношении которых отсутствует необходимость присвоения им категорий значимости обеспечения сетевой безопасности; -основных методов и средств	Обучающийся демонстрирует **полное знание:** -отечественных и международных стандарты информационной безопасности; - основных принципов организации технического, программного и информационного обеспечения защищенных информационных систем; -основных методов и средств, в отношении которых отсутствует необходимость присвоения им категорий значимости обеспечения сетевой безопасности;	Обучающийся демонстрирует **полное знание**: --отечественных и международных стандарты информационной безопасности; - основных принципов организации технического, программного и информационного обеспечения защищенных информационных систем; -основных методов и средств, в отношении которых отсутствует необходимость присвоения им категорий

обеспечения сетевой безопасности; - основные методы и средства обеспечения безопасности в системах управления базами данных.	-основных методы и средства обеспечения безопасности в системах управления базами данных операционных систем.	обеспечения безопасности в системах управления базами данных операционных систем. Испытывает затруднения при оперировании терминами и понятиями	Допускаются незначительные ошибки, неточности	значимости обеспечения сетевой безопасности. Допускаются незначительные неточности
уметь: - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности.	Обучающийся **не умеет** или в недостаточной степени умеет: -обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности.	Обучающийся демонстрирует **частичное умение:** - в обосновании принципов организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; - в осуществлении выбора функциональной структуры системы обеспечения информационной безопасности. Допускаются значительные ошибки,	Обучающийся демонстрирует **полное умение:** - в обосновании принципов организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; - в осуществлении выбора функциональной структуры системы обеспечения информационной безопасности. Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует **полное умение**: - в обосновании принципов организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; - в осуществлении выбора функциональной структуры системы обеспечения информационной безопасности. Допускаются незначительные неточности
владеть: - навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; -навыками настройки подсистем защиты	Обучающийся **не владеет:** - навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; - навыками настройки подсистем защиты	Обучающийся демонстрирует **частичное владение**: -навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты;	Обучающийся демонстрирует **полное владение**: -навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты. Допускаются	Обучающийся демонстрирует **полное владение**: -навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения

основных операционных систем	основных операционных систем	- навыками настройки подсистем защиты	незначительные ошибки, неточности	информационной безопасности объектов защиты. Допускаются незначительные неточности
ПК-7 Способен проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента				
знать: - методы экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	Обучающийся демонстрирует полное незнание методов экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	Обучающийся демонстрирует частичное знание методов экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	Обучающийся демонстрирует полное знание методов экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное знание методов экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. Допускаются незначительные неточности

уметь: - проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	Обучающийся демонстрирует полное неумение проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	Обучающийся демонстрирует частичное умение проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	Обучающийся демонстрирует полное умение проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. Допускаются незначительные ошибки неточности	Обучающийся демонстрирует полное умение проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. Допускаются незначительные неточности
владеть: - навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	Обучающийся **не владеет:** - навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	Обучающийся демонстрирует **частичное владение:** - навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	Обучающийся демонстрирует **полное владение**: - навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. Допускаются незначительные ошибки неточности	Обучающийся демонстрирует **полное владение**: - навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. Допускаются незначительные неточности

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3. Оценочные средства

7.3.1. Текущий контроль

Текущий контроль успеваемости студентов осуществляется в процессе проведения лабораторных работ и в процессе защиты (презентаций) докладов, подготовленных в рамках самостоятельной работы по выбранным и согласованным темам.

Примерные темы презентаций (докладов)

№ п/п	**Тема доклада (презентации)**
1.	Организация и порядок проведения аттестации объекта информатизации по требованиям безопасности информации
2.	Обеспечение информационной безопасности в системах электронного документооборота органов государственной власти
3.	Нормативно-методические документы ФСТЭК в области технической защиты информации.
4.	Автоматизированная система формирования защищенной консолидированной финансовой отчетности
5.	Графовый метод исследования защищенности объектов информатизации
6.	Информационное противоборство как крайнее проявление конфликта в информационном пространстве
7.	Обеспечение информационной безопасности платежных систем
8.	Математическая модель оптимизации состава комплекса средств защиты информации современных автоматизированных систем обработки данных по критерию «стоимость-риск»
9.	Методы и средства защиты информации в кредитно-финансовой сфере России
10.	Оптимизация состава комплекса средств защиты информации в системах передачи и обработки информации
11.	Особенности определения периодичности контроля состояния технической защиты информации на типовых объектах контроля
12.	Современный подход к обеспечению информационной безопасности систем связи
13.	Стандарты защиты информации для российских платежных систем
14.	Обоснование требований к системе защиты информации на объекте защиты
15.	Сравнительный анализ отечественных и зарубежных алгоритмов защиты информации от несанкционированного доступа при разработке сложных высокотехнологичных систем
16.	Методы обеспечения безопасности сетевых каналов передачи данных
17.	Программно-аппаратные комплексы для проведения специальных исследований СВТ на ПЭМИН.
18.	Программно-аппаратные комплексы для проведения акустических и виброакустических измерений.
19.	Защита конфиденциальной информации от утечки по каналу ПЭМИН
20.	Программно-аппаратные комплексы для оценки защищенности вспомогательных технических средств и систем от акустоэлектрических преобразований.
21.	Программно-аппаратные комплексы радиомониторинга.

22.	Современные методы и средства контроля и управления доступом к объектам информатизации
23.	Программно-аппаратные комплексы для выявления акустоэлектромагнитных (акустопараметрических) каналов утечки информации.
24.	Информационная безопасность в бизнесе
25.	Методы и средства защиты речевой конфиденциальной информации
26.	Цифровые анализаторы спектра и векторные анализаторы сигналов.
27.	Программно-аппаратные комплексы для исследования проводных линий.
28.	Защита акустической речевой информации с использованием импульсных помех
29.	Оптимальная стратегия защиты от перехвата сигналов цифровых радиотелеметрических систем передачи данных
30.	Методы защиты линий связи телекоммуникационных систем от преднамеренных помех

Вопросы теста по дисциплине

№ п/п	Вопросы теста по дисциплине	Прав. ответ
1.	**Основные технические средства и системы (ОТСС) – это** **A** - Технические средства и системы, непосредственно участвующие в обработке информации ограниченного доступа. B -Технические средства и системы обработки открытой информации. C- Технические средства и системы обработки информации. D - Средства вычислительной техники и автоматизированные системы обработки информации. E - Технические средства и системы, установленные на объекте информатизации.	A
2.	**Вспомогательные технические средства и системы (ВТСС) – это** A - Технические средства и системы, участвующие в обработке информации ограниченного доступа. B - Технические средства и системы обработки открытой информации. C - Технические средства и системы обработки информации. D - Технические средства и системы, установленные на объекте информатизации. **E** - Технические средства и системы, установленные на объектах информатизации или в выделенных (защищаемых) помещениях,	E

	непосредственно не участвующие в обработке (приеме, передачи, записи, хранения и т.д.) информации ограниченного доступа.	
3.	**Основные задачи защиты информации от утечки по техническим каналам:** A - Предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств обработки информации. **B** - Предотвращение утечки речевой информации по техническим каналам из выделенных (защищаемых) помещений. C - Выявление электронных устройств перехвата информации, внедренных в технические средства и выделенные (защищаемые) помещения. D - Исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации. E - Предотвращение хищения носителей информации и несанкционированного снятия копий с носителей информации.	B
4.	**4. Что означает принцип экономичности защиты информации?** A – минимизация затрат на защиту информации **B – затраты на защиту информации не должны превышать возможный ущерб от реализации угроз** C – численность службы защиты информации не должна превышать 7 чел. D –комплексное использование различных способов и средств защиты информации	B
5.	**5. Что означает принцип рациональности защиты информации?** A – использование только сертифицированных средств защиты B – системный подход к технической защите информации **C – минимизацию ресурсов на обеспечение необходимого уровня безопасности информации** D –все вместе	C
6.	**Утечка информации по техническому каналу:** A - Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками. **B** - Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. C - Неконтролируемое распространение защищаемой информации в результате ее разглашения.	B

	D - Неконтролируемое распространение защищаемой информации в результате получения защищаемой информации иностранными разведками. E - Получение возможности ознакомления с информацией с использованием программных и (или) технических средств.	
7.	**Чем отличаются ОТСС от ВТСС?** A – потребляемой мощностью **B – наличием принятых мер по защите информации** C – не могут использоваться для обработки открытой информации D –большей скоростью обработки информации	B
8.	**По способу формирования электрического сигнала активные акустоэлектрические преобразователи могут быть** A – индуктивными, электродинамическими и пьезоэлектрическими B – емкостными, электродинамическими и электромагнитными **C - электродинамическими, электромагнитными и пьезоэлектрическими** D –индуктивными, емкостными и резистивными	C
9.	**Информативный сигнал:** A - Физические поля, возникающие при обработке информации техническими средствами. B - Побочные электромагнитные колебания, возникающие при работе СВТ. C - Паразитные электромагнитные излучения технических средств обработки информации. D - Информация, переданная или полученная пользователем информационно-телекоммуникационной сети. **E** - Сигнал, по параметрам которого может быть определена защищаемая информация.	E
10.	**Чувствительность вторичных электрических часов как акустоэлектрических преобразователей** A – 30 - 45 мВ/Па B – 4 - 6 мВ/Па **C – 0,1 – 0,5 мВ/Па** D – 0,001 – 0,2 мВ/Па	C
11.	**Чувствительность абонентских громкоговорителей как акустоэлектрических преобразователей** **A – 30 - 45 мВ/Па** B – 4 - 6 мВ/Па C – 0,1 – 0,5 мВ/Па	A

	D – 0,001 – 0,2 мВ/Па	
12.	**Чувствительность трансформаторов и дросселей как акусто-электрических преобразователей** A – 30 - 45 мВ/Па B – 4 - 6 мВ/Па C – 0,1 – 0,5 мВ/Па **D – 0,001 – 0,2 мВ/Па**	D
13.	**Виды паразитных связей** A – положительная, отрицательная и дифференциальная **B – емкостная, индуктивная и гальваническая** C – емкостная, индуктивная и пьезоэлектрическая D –магнитометрическая, высокочастотная и низкочастотная	B
14.	**Сигналы по форме бывают** **A - аналоговые и дискретные** B – импульсные и цифровые C – электрические и электромагнитные D –акустические и магнитные	A
15.	**Освещенность поверхности Земли звездным светом составляет** A – 1 лк B – 0.01 лк **C – 0,001 лк** D – 0,0001 лк	C
16.	**Диапазон освещенности поверхности Земли лунным светом при средней прозрачности атмосферы составляет** **A - 0,03-0,25 лк** B – 0,25-5 лк C- 5-10 лк	A
17.	**Диапазон освещенности земной поверхности Солнцем в дневное время составляет** A –10 в 2 степени лк **B – 10 в 5 степени лк** C - 10 в 6 степени лк	B
18.	**К случайной распределенной антенне относятся:** **A** - Соединительные линии ВТСС, посторонние проводники, линии электропитания и цепи заземления, выходящие за пределы контролируемой зоны. **B** - Трубы парового отопления, выходящие за пределы контролируемой зоны.	A B C

	C - Телефонный провод городской АТС. D - Датчики охранной и пожарной сигнализации локальной системы охранно-пожарной сигнализации, все элементы которой, включая приборы приемно-контрольные, располагаются в пределах контролируемой зоны. E - Телефонный аппарат городской АТС.	
19.	**При увеличении угловых размеров объекта наблюдения в два раза время обнаружения сокращается** A – в два раза B – в 4 раза C – в 6 раз **D – в 8 раз**	D
20.	**При увеличении угла поля обзора в два раза время обнаружения объекта увеличивается** A – в два раза **B – в 4 раза** C – в 6 раз D – в 8раз	B
21.	**Диапазон длин волн в видимом диапазоне составляет** A – 0,3-0,7 мкм **B – 0,4-0,76 мкм** C – 0,46 - 0,86 мкм D – 0.46 - 0,7 мкм	B
22.	**При какой освещенности человек перестает различать цвета?** A – 0,01 лк **B – 0.1 лк** C – 1 лк D – 10 лк	B
23.	**Разведка по виду носителя технического средства разведки классифицируется** **A – космическая, морская, наземная, воздушная** B – космическая, воздушная, морская, сухопутная C – космическая, воздушная, морская, агентурная	
24.	**В структуру системы технической разведки входят** A – объекты разведки, органы добывания и органы сбора и обработки B – потребители информации, органы планирования и управления, органы добывания	C

	С - органы планирования и управления, органы добывания и органы сбора и обработки	
25.	**Когда возникает паразитная гальваническая связь?** А – в результате воздействия магнитного поля В - в результате воздействия электрического поля **С – через общее активное сопротивление** D – все ответы верны	С
26.	**Чем отличается технический канал утечки информации от канала связи?** А – средой распространения сигнала **В – типом получателя информации** С – видом помехи в канале D - все ответы верны	В
27.	**Акустическое давление измеряется в** А) кг/м^2. **Б) Па.** В) Вт/м^2. Г) Н/м^2. Д) мм ртутного столба.	Па
28.	**К естественным ТКУИ, обрабатываемой ОТСС, относятся**: **А** -Электромагнитные технические каналы утечки информации. **В** - Электрические технические каналы утечки информации. С - Технические каналы утечки информации, создаваемые путем «высокочастотного облучения» ОТСС. D - Технические каналы утечки информации, создаваемые путем внедрение в ОТСС электронных устройств перехвата информации (закладных устройств).	А В
29.	**Условное (нормированное) значение нулевого уровня акустического давления (порог слухового восприятия) составляет** А) 0,2 Па. В) 0,02 Па. С) 0,002 Па. D) 0,0002 Па. **Е) 0,00002 Па.**	Е
30.	**Относительный уровень речевого сигнала рассчитывается по формуле** А) $L = 10\lg\left[\frac{L_c}{L_n}\right]$. **В)** $L = 20\lg\left[\frac{L_c}{L_n}\right]$ С) $L = 20\lg L_c$. D $L = 20\lg\left[L_c \cdot L_n\right]$. Е) $L = 10\lg L_c$.	В

31.	**В октавной полосе частот нижняя граничная частота $f_н$ и верхняя граничная частота $f_в$ связаны зависимостью:** **A)** $f_в = 2 \cdot f_н$. B) $f_в = 3 \cdot f_н$. C) $f_в = 10 \cdot f_н$. D) $f_в = 1/3 \cdot f_н$	A
32.	**Количество октавных полос речевого сигнала равно:** A - 3. B - 5. **C - 7**. D - 8. E - 10.	C
33.	**Среднегеометрические частоты октавных полос речевого сигнала равны:** A - 100, 300, 500, 1000, 3000, 4000, 8000 Гц. B - 20, 200, 500, 1000, 3000, 5000, 10000 Гц. C - 100, 250, 500, 1000, 2000, 3000, 4000 Гц. **D - 125, 250, 500, 1000, 2000, 4000, 8000 Гц.** E - 300, 500, 1000, 3000, 5000, 8000, 10000 Гц.	D
34.	**Какие способы перехвата речевой информации требуют проникновения в выделенное помещение?** **A - перехват акустических колебаний, возникающих при ведении разговоров, закладными устройствами с датчиками микрофонного типа** B –перехват вибрационных колебаний, возникающих при ведении разговоров в ограждающих конструкциях и инженерных коммуникациях, закладными устройствами с датчиками контактного типа. C - перехват вибрационных колебаний, возникающих при ведении разговоров в ограждающих конструкциях и инженерных коммуникациях, электронными стетоскопами. D -перехват информативных электрических сигналов, возникающих вследствие акустоэлектрических преобразований акустических сигналов элементами ВТСС, техническими средствами, построенными на базе низкочастотных усилителей, подключаемыми к соединительным линиям ВТСС. E) Перехват акустической (речевой) информации методом «высокочастотного облучения» ВТСС, имеющих в своем составе акустоэлектрические преобразователи.	**A**
35.	**При какой полосе частот качество записанного разговора будет** лучше A - 300 – 3400 Гц B - 300 – 10000 Гц **C - 100 – 10000 Гц** D - 100 – 6500 Гц	C

36.	**Причины, вызывающие появление опасных сигналов в цепях электропитания** A – наведение в цепях ЭДС полями НЧ и ВЧ побочных излучений ОТСС B – модуляция тока электропитания токами радиоэлектронного средства C – попадание опасного сигнала в цепи электропитания через паразитные связи элементов схемы и блоков питания **D – все ответы верны**	D
37.	**От чего зависит эффективность электрического экранирования?** **A – от электропроводности экрана и сопротивления заземле**ния B – от толщины экрана и его магнитных свойств C – все ответы верны	A
38.	**К естественным ТКУИ, обрабатываемой ОТСС, относятся:** **A** -Электромагнитные технические каналы утечки информации. **B** - Электрические технические каналы утечки информации. C - Технические каналы утечки информации, создаваемые путем «высокочастотного облучения» ОТСС. D - Технические каналы утечки информации, создаваемые путем внедрение в ОТСС электронных устройств перехвата информации (закладных устройств).	A B
39.	**Эффективность электромагнитного экранирования измеряется** A – в децибелах B – в неперах **C – все ответы верны**	C
40.	**От чего зависит эффективность магнитного экранирования?** A – от электропроводности экрана и сопротивления заземления **B – от толщины экрана и его магнитных свойств** C – все ответы верны	B
41.	**При отражении лазерного луча от вибрирующей поверхности оконного стекла происходит его** **A – частотная, угловая и фазовая модуляция** B – частотная, амплитудная и фазовая модуляция C – амплитудная, широтно-импульсная и фазовая модуляция	A
42.	**Нормативное значение коэффициента звукоизоляции для обеспечения защиты речевой конфиденциальной информации для смежных помещений, не оборудованных системами звукоусиления, равно** A – 26 дБ	C

	B – 36 дБ **C – 46 дБ** D – 56 дБ	
43.	**Нормативное значение коэффициента звукоизоляции для обеспечения защиты речевой конфиденциальной информации для смежных помещений, оборудованных системами звукоусиления, равно** A – 46 дБ B – 50 дБ **C – 60 дБ** D – 65 дБ	C
44.	**Как влияет увеличение разрешения цифрового фотоаппарата на количество отснятых кадров** A - не влияет B – увеличивает **C – уменьшает**	C
45.	**Разрешение светочувствительного слоя цифрового фотоаппарата составляет** A – десятки пикселей B – сотни пикселей C – десятки тысяч пикселей **D – миллионы пикселей**	D
46.	**Разрешающая способность ПЗС определяется** A – размером диагонали матрицы **B – количеством ячеек, размещающихся в поле изображения** C – величиной напряжения питания D – габаритами объекта наблюдения	B
47.	**По назначению антенны бывают** A – передающие B – приемные C – приемопередающие **D – все утверждения верны**	D
48.	**Избирательность реального радиоприемника** **A – оценивается шириной полосы пропускания и коэффициентом прямоугольности АЧХ радиоприемника** B - оценивается шириной полосы пропускания и динамическим диапазоном радиоприемника C – оценивается динамическим диапазоном и коэффициентом прямоугольности АЧХ радиоприемника	A

49.	**К специально создаваемым техническим каналам утечки информации (ТКУИ), обрабатываемой техническими средствами (ОТСС), относятся:** A - Электромагнитные технические каналы утечки информации. B - Электрические технические каналы утечки информации. **C** - Технические каналы утечки информации, создаваемые путем «высокочастотного облучения» ОТСС. **D** - Технические каналы утечки информации, создаваемые путем внедрения в ОТСС электронных устройств перехвата информации (закладных устройств).	C D
50.	**Зоной R2 называется** **A – пространство вокруг ОТСС, на границе и за пределами которого напряженность электромагнитного поля не превышает допустимого (нормированного)значения** B - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного)значения C - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах не превышает допустимого (нормированного)значения	A
51.	**Зоной r1 называется** A – пространство вокруг ОТСС, на границе и за пределами которого напряженность электромагнитного поля не превышает допустимого (нормированного) значения **B - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного)значения** C - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах не превышает допустимого (нормированного)значения	B
52.	**Зоной r1* называется** A – пространство вокруг ОТСС, на границе и за пределами которого напряженность электромагнитного поля не превышает допустимого (нормированного)значения B - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного)значения **C - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в**	C

	распределенных антеннах не превышает допустимого (нормированного)значения	
53.	**Чувствительность контактных микрофонов (вибропреобразователей) составляет** A – 0,1 – 1,0 мкВ/Па B - 5 – 10 мкВ/Па C – 30 – 50 мкВ/Па **D – 50 – 100 мкВ/Па**	D
54.	**Чувствительность микрофонов акустической разведки составляет** A – 0,1 – 1,0 мкВ/Па B - 5 – 10 мкВ/Па **C – 30 – 60 мкВ/Па** D – 50 – 100 мкВ/Па	C
55.	**Какие разведки входят в разведсообщество США?** A – ЦРУ, СВР, РУМО **B – АНБ, ФБР, ЦРУ** C – АНБ, ФСБ, ЦРУ D – ЦРУ, СВР, РУМО, МИ-5	B
56.	**Какое другое название у измерителя спектра вторичных полей?** A – частотомер B – анализатор спектра **C – детектор нелинейных переходов** D – вторичный спектроанализатор	C
57.	**Назначение прибора ST-031 «Пиранья»** A – для уничтожения радиозакладок в цепях электропитания B – для создания акустических тест-сигналов C- для проверки эффективности электромагнитного экранирования **D – многофункциональный поисковый прибор**	D
58.	**Когда система защиты считается эффективной?** A – функционирует непрерывно B – перекрывает заданный диапазон частот **C – обеспечивает выполнение требований и норм по защите** D – имеет минимальную стоимость по критерию «эффективность-стоимость»	C
59.	**Точность локализации закладного устройства нелинейным локатором**	

	A – несколько сантиметров B – 10- 20 см C – 30 – 50 см	A
60.	**Мощность в импульсе нелинейного локатора может достигать** A – нескольких Вт B – нескольких десятков Вт **C – нескольких сот Вт** D – более 1000 Вт	C
61.	**Нормированное значение отношения сигнал/помеха для информации с грифом «сов. секретно» составляет** A – 0,1 **B – 0,2** C – 0,3 D – 0,5	B
62.	**Лицензирование деятельности в области технической защиты информации и сертификацию средств защиты осуществляет** A – ФСБ B – СВР **C – ФСТЭК** D – МО	C
63.	**Нормированное значение отношения сигнал/помеха для информации с грифом «особой важности» составляет** **A – 0,1** B – 0,2 C – 0,3 D – 0,5	A
64.	**Виды отражений в оптическом диапазоне** A – ортогональное, диффузное, зеркальное B – прямолинейное, зеркальное C – дисперсное, зеркальное, смешанное **D – зеркальное, диффузное, смешанное**	D
65.	**Пропускная способность канала связи** A – тем больше, чем меньше полоса пропускания частот и выше отношение сигнал/шум на входе приемника канала связи B - тем меньше, чем меньше полоса пропускания частот и выше отношение сигнал/шум на входе приемника канала связи **C - тем больше, чем больше полоса пропускания частот и выше отношение сигнал/шум на входе приемника канала связи** D - тем больше, чем меньше полоса пропускания частот и меньше отношение сигнал/шум на входе приемника канала связи	C

66.	**По соотношению спектра помех и полезных сигналов помехи подразделяются на** A – прицельные и пространственные B – заградительные и линейные **C – заградительные и прицельные** D – заградительные и пространственные	C
67.	**К разведывательным организациям гражданских ведомств США относятся** A – ЦРУ и управление разведки и исследований Госдепартамента **B – ФБР и разведывательные подразделения Министерства финансов** C – АНБ и разведывательные подразделения Министерства энергетики D – АНБ, РУМО, ФБР E – нет правильного ответа	B

7.3.2. Промежуточная аттестация

Промежуточная аттестация обучающихся в форме **экзамена** проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Типовые вопросы экзаменационных билетов:

1. Объект информатизации (определение). Основные технические средства и системы (ОТСС).
2. Вспомогательные технические средства и системы (ВТСС).
3. Технический канал утечки информации (определение). Схема технического канала утечки информации
4. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).
5. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.
6. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений.
7. Линейные и энергетические характеристики акустического поля. Основные характеристики речи и речевого сигнала. Разборчивость речи.
8. Классификация технических каналов утечки акустической (речевой) информации и способов перехвата речевой информации.
9. Средства акустической разведки: цифровые диктофоны, направленные микрофоны (классификация, характеристики, основные возможности, схема канала перехвата).
10. Дальность перехвата речевого сигнала средствами акустической разведки.

11. Схемы перехвата речевой информации по акустовибрационному каналу утечки речевой информации.

12. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.

13. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.

14. Экранирующие материалы, их основные характеристики.

15. Формула для расчета коэффициента экранирования для электрической и магнитной составляющей электромагнитного поля.

16. Экранированные помещения и экранированные камеры (классификация, состав, основные характеристики).

17. Основные требования к заземлению технических средств. Схемы заземлителей. Схемы заземления технических средств. Схемы измерения сопротивления заземления технических средств.

18. Основные требования к системе пространственного электромагнитного зашумления.

19. Схема установки системы пространственного зашумления на объекте информатизации.

20. Основные требования по установке системы пространственного зашумления на объекте информатизации.

21. Основные характеристики генераторов шума.

22. Основные требования к системе электропитания технических средств.

23. Способы защиты цепей электропитания технических средств от утечки информации, возникающей за счет наводок побочных электромагнитных излучений.

24. Основные требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания технических средств.

25. Основные характеристики фильтров нижних частот (ФНЧ). Схемы установки помехоподавляющих фильтров на объекте информатизации.

26. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.

27. Средства звуко- и виброизоляции выделенных помещений.

28. Звукоизолирующие кабины. Специальные защищенные помещения.

29. Порядок проведения контроля эффективности защиты ВТСС.

30. Состав и основные требования к аппаратуре контроля при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.

31. Схема измерительной установки при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.

32. Порядок проведения проверки ВТСС на подверженность акустоэлектрическим преобразованиям.

33. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.

34. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.

35. Сканирующие приемники (принцип работы, основные характеристики). Методы обнаружения, идентификации радиозакладок (РЗ) и определения их местоположения.

36. Порядок организации защиты информации на объектах информатизации.

37. Организация аттестации объекта информатизации по требованиям безопасности информации. Перечень документов, предоставляемых Заявителем для проведения аттестации объекта информатизации.

38. Порядок проведения аттестации объекта информатизации по требованиям безопасности информации.

39. Заключение по результатам аттестационной проверки объекта информатизации. Аттестат соответствия объекта информатизации.

40. Выявление каналов утечки информации за счет акустоэлектрических преобразований в ВТСС.

41. Определение требуемого радиуса контролируемой зоны Rкз для защиты конфиденциальной информации от утечки по каналу побочных электромагнитных излучений и наводок (зоны R2 и r1.

42. Оценка защищенности ОТСС от наводок ПЭМИ на линии и коммуникации, выходящие за пределы контролируемой зоны.

43. Инструментально-расчетное определение коэффициентов звукоизоляции и виброизоляции ограждающих конструкций защищаемых помещений на базе многофункционального поискового прибора ST-031 «Пиранья».

44. Обнаружение и локализация закладных устройств негласного съема информации измерителем спектра вторичных полей «NR-μ».

45. Контроль эффективности защиты речевой информации от утечки по прямому акустическому и акустовибрационному каналам программно-аппаратным комплексом ПАК «Спрут-мини».

46. Система акустической и виброакустической защиты информации «СОНАТА-АВ».

47. Анализатор проводных линий «Отклик-2». Генератор шума по сети 220В SEL SP 41/C.

48. Поиск сигналов ПЭМИН от ОТСС на базе программно-аппаратного комплекса «Навигатор-П-3Г».

Пример билета

1.Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).

2. Схема измерительной установки при контроле ВТСС на подверженность акустоэлектрическим преобразованиям

3. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.