Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 04.09.2025 12:56:05
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

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

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"27" февраля 2025 г.

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

Направление подготовки 10.03.01
«Информационная безопасность»

Образовательная программа (профиль):
«Безопасность компьютерных систем»

Квалификация (степень) выпускника
Бакалавр

Год приема – 2025

Форма обучения
Очная

Москва, 2025 г.

Разработчик:

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



/ Ю.Н. Рагозин /

Согласовано:
Заведующий кафедрой «Информационная безопасность»  /И.В.Калуцкий/

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1. Цели, задачи и планируемые результаты обучения по дисциплине …… 4
2. Место дисциплины в структуре образовательной программы……..... 5
3. Структура и содержание дисциплины……. 5
3.1.Виды учебной работы и трудоемкость……5
3.2.Тематический план изучения дисциплины…… 6
3.3.Содержание дисциплины…… 7
3.4.Тематика семинарских/практических и лабораторных занятий……...9
3.5.Тематика курсовых проектов (курсовых работ) ……9
4. Учебно-методическое и информационное обеспечение…… 10
4.1. Нормативные документы и ГОСТы…… 10
4.2. Основная литература……. 10
4.3. Дополнительная литература……. 10
4.4. Электронные образовательные ресурсы……. 10
4.5. Современные профессиональные базы данных и информационные справочные системы…… 11
5. Материально-техническое обеспечение…… 11
6. Методические рекомендации……11
6.1. Методические рекомендации для преподавателя по организации обучения 11
6.2. Методические указания для обучающихся по освоению дисциплины……12
7. Фонд оценочных средств…… 13
7.1. Методы контроля и оценивания результатов обучения…… 13
7.2. Шкала и критерии оценивания результатов обучения…… 13
7.3 Оценочные средства……..... 16
7.3.1. Текущий контроль…… 16
7.3.2. Промежуточная аттестация……. 17

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 бакалавра к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации.

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

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- ознакомление с техническими каналами утечки акустической (речевой) информации;
- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

Обучение по дисциплине «Защита информации от утечки по техническим каналам» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**знать:** современные программные, программно-аппаратные (в том числе криптографические) и технические средства защиты информации **уметь:** выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК – 3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**знать:** виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации **уметь:** организовывать и сопровождать контроль эффективности технических средств защиты информации

	владеть: навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации от утечки по техническим каналам» относится к числу профессиональных учебных дисциплин обязательной части цикла Б1.1 (Б1.1.38) основной образовательной программы бакалавриата.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Математический анализ», «Теория вероятностей» и «Математическая статистика», «Электроника и схемотехника», «Основы информационной безопасности», «Физические основы информационной безопасности».

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, т.е. **144** академических часа (лекции – 8 часов, лабораторные занятия – 64 часа, самостоятельная работа – 72 часа), формы контроля – **экзамен и курсовой проект** в 7 семестре.

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

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	7	1-18
	В том числе:			
1.1	Лекции	8	7	1-2
1.2	Семинарские/практические занятия	-	-	-
1.3	Лабораторные занятия	64	7	3-18
2	**Самостоятельная работа**	**72**	7	1-18
3	**Промежуточная аттестация**		7	6-17
	Экзамен, курсовой проект		7	По расписанию
	Итого:	**144**		

3.2. Тематический план изучения дисциплины (по формам обучения)

3.2.1 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. Место технической защиты информации в государственной системе защиты информации в Российской Федерации	18	1	-	8	-	9
2	Тема 2. Технические каналы утечки акустической (речевой) информации	18	1	-	8	-	9
3	Тема 3. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	18	1	-	8	-	9
4	Тема 4. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	18	1	-	8	-	9
5	Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам	18	1	-	8	-	9
6	Тема 6. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	18	1	-	8	-	9
7	Тема 7. Методы и средства выявления электронных устройств негласного получения информации	18	1	-	8	-	9
8	Тема 8. Организация технической защиты информации	18	1	-	8	-	9

Итого	**144**	**8**	**-**	**64**	**-**	**72**

3.3. Содержание дисциплины

Темы лекций:

Тема 1. Место технической защиты информации в государственной системе защиты информации в Российской Федерации

Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации). Нормативные документы 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 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 3. 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 4. 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 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 выделенных помещений от утечки речевой информации по техническим каналам

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 R2 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

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

Лабораторная работа №6

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

Лабораторная работа №7

Система акустической и виброакустической защиты информации «СОНАТА-АВ»

Лабораторная работа №8

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

3.5. Тематика курсовых проектов

Курсовое проектирование выполняется в соответствии с методическими указаниями по курсовому проектированию, изложенными в Приложении к РПД.

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: учебное пособие - ИЦ «Интермедия» Санкт-Петербург, 2018 – 168 с.
2. Рагозин Ю.Н. Инженерно-техническая защита информации на объектах информатизации: учебное пособие - ИЦ «Интермедия» Санкт-Петербург, 2019 – 216 с.

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.: Российский 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 занятий лекционного типа в формате онлайн преподавателю необходим ноутбук с возможностью использования сервиса корпоративной платформы **Microsoft Teams.**

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);
- генератор виброакустического шума "Соната АВ";
- генератор шума по сети 220В SEL SP 41/С.

Для проведения презентаций по тематике дисциплины 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

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

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 занятия ***лекционного типа и самостоятельная работа студентов***.

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 занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на занятиях лекционного типа

и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков работы с программно-аппаратными комплексами, которые используются в профессиональной деятельности специалистов по информационной безопасности.

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 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;
- умения 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-1 **Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации**				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: современные программные, программно-аппаратные (в том числе криптографические) и технические средства защиты информации	Обучающийся демонстрирует полное отсутствие или недостаточное знание современных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Обучающийся демонстрирует знание основных современных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации, но допускает существенные ошибки, неточности.	Обучающийся демонстрирует полное знание современных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации, но допускает незначительные ошибки, неточности	Обучающийся демонстрирует полное знание современных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
уметь: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Обучающийся не умеет или в недостаточной степени умеет выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Обучающийся демонстрирует умение выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации, но допускает существенные ошибки, неточности.	Обучающийся демонстрирует полное умение выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации, но допускает незначительные ошибки, неточности	Обучающийся демонстрирует полное умение выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации
ПК – 3 **Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации**				

знать: виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации	Обучающийся не знает видов и методов контрольных проверок эффективности применяемых мер и средств защиты информации	Обучающийся знает виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации, но допускает существенные ошибки, неточности.	Обучающийся знает все виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации, но допускает незначительные ошибки, неточности	Обучающийся знает все виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации
уметь: организовывать и сопровождать контроль эффективности технических средств защиты информации	Обучающийся не умеет организовывать и сопровождать контроль эффективности технических средств защиты информации	Обучающийся имеет представление об организации и сопровождении контроля эффективности технических средств защиты информации, но допускает значительные неточности, ошибки	Обучающийся имеет представление об организации и сопровождении контроля эффективности технических средств защиты информации, но допускает незначительные неточности.	Обучающийся умеет организовать и сопровождать контроль эффективности технических средств защиты информации
владеть: навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения	Обучающийся не владеет навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения	Обучающийся не в полной мере владеет навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения	Обучающийся владеет навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения, но допускает незначительные неточности	Обучающийся полностью владеет навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения

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 выбранной и согласованной теме.

Примерные темы презентаций (докладов)

1. Безопасность данных на жестких дисках и твердотельных накопителях
2. Современные методы и средства контроля и управления доступом к объектам информатизации
3. Безопасность информации в облачных хранилищах
4. Методы обеспечения безопасности сетевых каналов передачи данных
5. Методы и средства защиты речевой конфиденциальной информации
6. Технические каналы утечки информации
7. Компьютерная преступность и виды преступной деятельности
8. Защита конфиденциальной информации от утечки по каналу ПЭМИН
9. Система обнаружения и предотвращения вторжений в корпоративную сеть
10. Компьютерная контркриминалистика: состояние и перспективы развития
11. Каналы и методы несанкционированного доступа к информации
12. Защита облачного сервиса
13. Информационная безопасность в бизнесе
14. Классификация иностранной технической разведки и ее возможности по получению сведений конфиденциального характера.
15. Сертификация средств защиты информации по требованиям безопасности информации

16. Типы микрофонных систем и их технические характеристики. Область применения электронных стетоскопов (радиостетоскопов), их конструктивные особенности.
17. Лазерные акустические систем разведки.
18. Цифровые анализаторы спектра и векторные анализаторы сигналов.
19. Измерительные цифровые приемники.
20. Измерительные антенны, токосъемники, пробники для проведения специальных исследований средств вычислительной техники.
21. Программно-аппаратные комплексы для проведения специальных исследований СВТ на ПЭМИН.
22. Портативные шумомеры и виброметры.
23. Аудиоанализаторы и область применения.
24. Программно-аппаратные комплексы для проведения акустических и виброакустических измерений.
25. Программно-аппаратные комплексы для выявления акустоэлектромагнитных (акустопараметрических) каналов утечки информации.
26. Программно-аппаратные комплексы для оценки защищенности вспомогательных технических средств и систем от акустоэлектрических преобразований.
27. Индикаторы электромагнитного поля.
28. Радиочастотомеры и сканирующие радиоприемники.
29. Специальные поисковые приемники ближней зоны и интерсепторы.
30. Программно-аппаратные комплексы радиомониторинга.
31. Анализаторы проводных линий.
32. Программно-аппаратные комплексы для исследования проводных линий.
33. Нелинейные радиолокаторы. Рентгенотелевизионные комплексы и портативные металлоискатели.
34. Нормативно-методические документы ФСТЭК в области технической защиты информации.

По согласованию с преподавателем тема презентации может быть предложена студентом самостоятельно.

№ п/п	Вопросы теста по дисциплине	Прав. ответ
1.	**Что представляет собой ресурс системы защиты информации?** A - количество специалистов по защите информации B - состав инженерно-технических сооружений C - выделенные денежные средства **D – все вместе**	D
2.	**2. Что надо определить перед выбором мер защиты информации?** A – квалификацию персонала **B – угрозы безопасности информации** C – систему пожарно-охранной сигнализации	B
3.	**3. Локальные показатели эффективности защиты информации** подразделяются на: A – тактические и стратегические B – оперативные и постоянные **C – функциональные и экономические** D –территориальные и пространственные	C
4.	**4. Что означает принцип экономичности защиты информации?** A – минимизация затрат на защиту информации	

	В – затраты на защиту информации не должны превышать возможный ущерб от реализации угроз С – 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.	**6. Зоны защиты объектов информатизации бывают:** **A - независимыми, пересекающимися и вложенными** B – автономными, многоярусными и многозвенными C - укрепленными, локальными и общими	A
7.	**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.	**Вопросы теста по дисциплине** **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.	**Чувствительность электродинамического микрофона лежит в пределах** A – 30 - 45 мВ/Па **B – 4 - 6 мВ/Па** C – 0,1 – 0,5 мВ/Па D – 0,001 – 0,2 мВ/Па	B
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	A

	C – 0,1 – 0,5 мВ/Па D – 0,001 – 0,2 мВ/Па	
12.	**Чувствительность трансформаторов и дросселей 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**	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	
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 – 1- 10 в 2 степени лк **B – 10-10 в 5 степени лк** C - 100 – 10 в 6 степени лк	B
18.	**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
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 - органы планирования и управления, органы добывания и органы сбора и обработки**	C
25.	**Когда возникает паразитная гальваническая связь?** A – в результате воздействия магнитного поля B - в результате воздействия электрического поля **C – через общее активное сопротивление** D – все ответы верны	C
26.	**Чем отличается технический канал утечки информации от канала связи?** A – средой распространения сигнала **B – типом получателя информации** C – видом помехи в канале D - все ответы верны	B

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.	**Скорость звука в воздухе при температуре воздуха 15^{0}С и давлении 101325 Па составляет** **А) 340 м/с.** В) 1200 м/с. С) 3000 км/ч. Г) 20 км/с. Д) 60 км/ч	А
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** A) $L = 10\lg\left[\frac{L_c}{L_n}\right]$. **B)** $L = 20\lg\left[\frac{L_c}{L_n}\right]$ C) $L = 20\lg L_c$. D $L = 20\lg[L_c\ L_n]$. E) $L = 10\lg L_c$.	В
31.	**В октавной полосе частот нижняя граничная частота $f_н$ и верхняя граничная частота $f_в$ связаны зависимостью:** **А)** $f_в = 2\ f_н$. B) $f_в = 3\ f_н$. C) $f_в = 10\ f_н$. D) $f_в = 1/3\ f_н$	А
32.	**Количество октавных полос речевого сигнала равно:** A - 3**.** B - 5**.** **C - 7**. D - 8. E - 10.	С
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?**	

	А - перехват акустических колебаний, возникающих при ведении разговоров, закладными устройствами с датчиками микрофонного типа В –перехват вибрационных колебаний, возникающих при ведении разговоров в ограждающих конструкциях и инженерных коммуникациях, закладными устройствами с датчиками контактного типа. С - 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. Е) Перехват акустической (речевой) информации методом «высокочастотного облучения» ВТСС, имеющих в своем составе акустоэлектрические преобразователи.	**А**
35.	**При какой полосе частот качество записанного разговора будет** лучше А - 300 – 3400 Гц В - 300 – 10000 Гц **С - 100 – 10000 Гц** D - 100 – 6500 Гц	С
36.	**Причины, вызывающие появление опасных сигналов в цепях электропитания** А – наведение в цепях ЭДС полями НЧ и ВЧ побочных излучений ОТСС В – модуляция тока электропитания токами радиоэлектронного средства С – 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?** **А – от электропроводности экрана и сопротивления заземления** В – от толщины экрана и его магнитных свойств С – все ответы верны	А
38.	**Геостационарная орбита ИСЗ находится на высоте** А – 2000 км В – 3580 км С – 24700 км **D – 35800 км**	D
39.	**Эффективность электромагнитного экранирования измеряется** А – в децибелах В – в неперах **С – все ответы верны**	С

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 B – 36 дБ **C – 46 дБ** D – 56 дБ	C
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** **А – оценивается шириной полосы пропускания и коэффициентом прямоугольности АЧХ радиоприемника** В - оценивается шириной полосы пропускания и динамическим диапазоном радиоприемника С – оценивается динамическим диапазоном и коэффициентом прямоугольности АЧХ радиоприемника	А
49.	**Для идентификации персонала применяются** А – атрибутные, биометрические и психофизические идентификаторы **В – атрибутные и биометрические идентификаторы** С – вещественные и логические	В
50.	**Зоной R2 называется** **А – пространство вокруг ОТСС, на границе и за пределами которого напряженность электромагнитного поля не превышает допустимого (нормированного)значения** В - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного)значения С - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах не превышает допустимого (нормированного)значения	А
51.	**Зоной r1 называется** А – пространство вокруг ОТСС, на границе и за пределами которого напряженность электромагнитного поля не превышает допустимого (нормированного) значения **В - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного)значения** С - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах не превышает допустимого (нормированного)значения	В
52.	**Зоной r1* называется** А – пространство вокруг ОТСС, на границе и за пределами которого напряженность электромагнитного поля не превышает допустимого (нормированного)значения В - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного)значения **С - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах не превышает допустимого (нормированного)значения**	С

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 R2 для защиты конфиденциальной информации от утечки по каналу побочных электромагнитных излучений.

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/С.

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

Пример билета

1. Классификация технических каналов утечки акустической (речевой) информации и способов перехвата речевой информации.

3. Порядок организации защиты информации на объектах информатизации

3. Определение требуемого радиуса контролируемой зоны R2 для защиты конфиденциальной информации от утечки по каналу побочных электромагнитных излучений.

ПРИЛОЖЕНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО КУРСОВОМУ ПРОЕКТИРОВАНИЮ
по дисциплине «Защита информации от утечки по техническим каналам»

1. **Цели и задачи курсового проектирования.**
2. **Руководство и контроль выполнения курсового проекта.**
3. **Типовая структура курсового проекта.**
4. **Оформление курсового проекта.**
5. **Защита курсового проекта.**
6. **Критерии оценки курсового проекта.**

1. Цели и задачи курсового проектирования

Курсовой проект (КП) выполняется на базе теоретических знаний и практических навыков, полученных студентом в процессе освоения учебной дисциплины «Защита информации от утечки по техническим каналам», и оформляется в соответствии с установленными требованиями.

Основными целями курсового проектирования являются:

- овладение методами анализа угроз безопасности информации и соответствующих им уязвимостей на конкретном объекте информатизации;

- овладение навыками практической самостоятельной работы при разработке курсовых проектов на создание систем защиты информации (СЗИ) предприятия (организации) от утечки по техническим каналам;

- развитие навыков самостоятельной работы с методическими материалами и литературой.

Целевой задачей КП является разработка аналитического обоснования создания СЗИ на конкретном объекте защиты (предприятии, организации).

Темы КП предлагаются выпускающей кафедрой «Информационная безопасность». Для обучающихся по специальности 10.05.03 - «Информационная безопасность автоматизированных систем» темы КП могут

предлагаться студентами исходя из целесообразности или необходимости совершенствования СЗИ на конкретных предприятиях, на которых они проходят производственную практику.

КП выполняется по выданному руководителем проекта заданию каждым студентом индивидуально. Срок выполнения курсового проекта устанавливается в соответствии с учебным планом. Для более четкой и эффективной организации работы разрабатывается план-график выполнения курсового проекта, который содержит названия основных этапов работы и рекомендуемые сроки их выполнения.

При курсовом проектировании студент должен проявлять большую самостоятельность: инициатива по предложению вариантов решения поставленных задач, а также по выбору окончательного решения должна принадлежать студенту. За принятые решения, а также за правильность всех расчетов и графического материала полностью отвечает автор работы.

2. Руководство и контроль выполнения курсового проекта

Руководителями КП могут быть преподаватели кафедры «Информационная безопасность», проводящие занятия по дисциплинам «Защита информации от утечки по техническим каналам» и «Комплексная система защиты информации на предприятии».

Основная задача руководителя состоит в организации самостоятельной работы студента.

Руководитель КП разрабатывает задание и календарный план-график его выполнения. Студент представляет руководителю на проверку выполненные разделы задания, по которым руководитель дает рекомендации по их улучшению.

Руководитель проводит систематические консультации с целью оказания помощи студентам в дни и часы, предусмотренные расписанием, предостерегает студентов от грубых ошибок в решении поставленных задач, осуществляет контроль за соблюдением графика выполнения КП, информирует об этом кафедру.

3. Типовая структура курсового проекта

Структура оформленного КП должна отвечать традиционным требованиям, предъявляемым к учебно-квалификационным работам, и включать следующие части:

- титульный лист;
- оглавление (содержание) – наименование всех глав и параграфов курсового проекта (с обязательным указанием страниц);
- введение, обосновывающее актуальность и значение защиты информации, а также цель курсового проекта;
- основную часть из трех глав (аналитическую, теоретическую и практическую), раскрывающую главное содержание курсового проекта. Каждая глава, как правило, подразделяется на несколько параграфов;
- заключение;
- библиографический список;
- приложение (при необходимости, объем не ограничивается).

Во **введении** обосновывается актуальность темы, её практическая значимость. Формулируется цель и конкретные задачи, связанные с вопросами проектирования. Также рекомендуется указать, на каких материалах базируется проект.

Объем введения должен быть не более двух страниц.

В **аналитической главе** приводятся исходные данные об объекте защиты:

- тип объекта, вид его деятельности и защищаемая информация;
- его дислокация, структура и поэтажные планы;
- технические характеристики ограждающих конструкций и перекрытий;
- состав и размещение основных технических средств и систем (ОТСС);
- состав и размещение вспомогательных технических средств и систем (ВТСС).

Составляется план инженерных коммуникаций здания (в масштабе) с указанием границы контролируемой зоны, места расположения трансформаторной подстанции, заземляющего устройства, трасс прокладки

инженерных коммуникаций и силовых кабелей с указанием мест установки распределительных устройств.

Анализируются угрозы безопасности информации с построением модели злоумышленника, выявляются уязвимости объекта защиты, через которые возможна реализация угроз (проводится анализ возможных технических каналов утечки информации с объекта защиты).

Аналитическая часть должна заканчиваться выводами по рассмотренным вопросам с обоснованием главных направлений проектных решений.

Пример возможного названия главы:

«Глава 1. Анализ угроз безопасности информации и построение модели злоумышленника на предприятии. Выявление уязвимостей объекта защиты и технических каналов утечки информации».

Объем аналитической части может составлять 10 – 15 страниц.

Теоретическая глава может быть посвящена теоретическим и методологическим основам технической защиты информации, в которой излагаются концептуальные основы противодействия техническим разведкам, рассматриваются технические каналы утечки информации по теме курсового проекта и соответствующие им нормативно-методические документы по защите информации.

Теоретическая часть должна заканчиваться выводами по рассмотренным вопросам с обоснованием решений по главным направлениям работы.

Пример возможного названия главы:

«Глава 2. Классификация технических каналов утечки акустической (речевой) конфиденциальной информации. Методы и нормы противодействия акустической речевой разведке».

Объем теоретической части проекта может составлять 10 – 15 страниц.

Проектная часть посвящается анализу и сравнению характеристик промышленно выпускаемых средств защиты информации с дальнейшим обоснованием их выбора (например, по показателю «эффективность-

стоимость») для нейтрализации выявленных уязвимостей объекта защиты. Проводится анализ организаций, имеющих лицензии на разработку технических проектов СЗИ объектов информатизации, и подрядных организаций-исполнителей других видов работ. Описывается разработанная система защиты информации и приводится предлагаемая план-схема размещения пассивных и активных средств защиты информации.

Пример возможного названия главы:

«Глава 3. Разработка системы защиты речевой конфиденциальной информации в кабинете Генерального конструктора ЗАО «ИМПУЛЬС» от утечки по техническим каналам»

(может совпадать с названием темы курсового проекта).

Объем практической части курсового проекта может составлять 15 - 20 страниц.

В **заключении** в сжатой форме делаются теоретические выводы по первой и третьей главам о предлагаемых решениях задач курсового проектирования, дается оценка (при возможности) их реализуемости в практике конкретной организации (предприятия).

Объем заключения составляет, как правило, 1 - 2 страницы.

В **библиографическом списке** перечисляются все источники информации, использованные студентом при написании курсового проекта, в том числе ссылки на материалы из сети INTERNET.

Список наименований должен содержать не менее 10 источников. Оформление списка должно выполняться по правилам, установленным государственным стандартом ГОСТ 7.1.84 «Библиографическое описание документа».

В **приложения** (таблицы, схемы, рисунки, графики большого формата, фрагменты которых используются в основном тексте) помещают материалы, которые носят вспомогательный, поясняющий характер. Материалы приложения должны иметь порядковые номера. Объем приложения не лимитируется.

4. Оформление курсового проекта

Рекомендуемый объем курсового проекта, обычно, составляет 40 - 50 страниц машинописного текста, выполненных через 1,5 интервала шрифтом Times New Roman с размером шрифта 14 (30 строк по 60 печатных знаков в каждой строке, считая пробелы).

Размеры полей должны быть следующими: левое – 30 мм, правое – не менее 10 мм, верхнее – не менее 20 мм, нижнее – не менее 20 мм. Отступ красной строки 1,25 см.

Курсовой проект выполняется на одной стороне листа. Число страниц приложения не входит в общий объем страниц курсового проекта.

Разделы (главы) должны иметь порядковые номера в пределах всего курсового проекта. Наименования разделов записываются в виде заголовков строчными буквами (кроме первой прописной). Переносы слов в заголовках не допускаются. Точку в конце заголовка не ставят.

Каждый раздел рекомендуется выполнять с нового листа. Не следует начинать подразделы в нижней части страницы, если после его заголовка не помещаются четыре-пять строк последующего текста.

Текст курсового проекта должен быть четким, последовательным и логичным, исключать всякие повторения и произвольные сокращения слов. Не допускается переписывание текста и копирование иллюстрированного материала из учебников и прочей учебной литературы. Если используются цитаты из литературных источников, то следует чужие слова взять в кавычки и сделать ссылку. Формулы и другие данные, необходимые для расчетов и заимствованные из литературных источников, должны быть оформлены в тексте курсового проекта с соответствующими ссылками.

Значения символов и числовых коэффициентов, входящих в формулу, должны быть расшифрованы сразу же после формулы. При этом символы (каждый отдельно) записывают с новой строки в той последовательности, в которой они приведены в формуле. Первая строка расшифровки должна начинаться со слова «где» без двоеточия после него.

Цифровой материал, как правило, оформляется в виде таблиц, которые должны иметь заголовок, выполняемый над таблицей посередине строчными буквами (кроме первой прописной). Заголовок должен быть кратким и полностью отражать содержание таблицы. Все таблицы, если их в проекте больше одной, нумеруются в пределах главы арабскими цифрами. При переносе таблицы на следующую страницу шапку таблицы следует повторить и над ней поместить слова «Продолжение табл.» с указанием номера. Шапку таблицы необходимо повторять на каждом листе. Заголовок не повторяется.

На все таблицы должны быть ссылки в тексте, при этом слово «Таблица» в тексте пишут полностью, если таблица не имеет номера, и сокращенно, если имеет номер, например: «В табл. 3.2…».

Иллюстративный материал, таблицы большого формата или текст вспомогательного характера следует помещать в приложениях к курсовому проекту на отдельных листах с указанием в правом верхнем углу первого листа слова «Приложение» прописными буквами. Все приложения должны иметь заголовок, который прописывается симметрично тексту прописными буквами.

На все приложения дается ссылка в основном тексте КП.

В тексте КП могут использоваться следующие сокращения:

- общепринятые аббревиатуры (РФ, ФСТЭК, ФСБ, вуз и т.п.);
- сложносокращенные слова, которые составляются из сочетаний усеченных и полных слов (электроприбор – электрический прибор), одних усеченных слов (модем – модулятор и демодулятор);
- условные общепринятые сокращения: в т.ч. (в том числе), пр. (прочий), напр. (например), мн.др. (многие другие), см. (смотри), т.е. (то есть), г. (год), гг. (годы), д.т.н. (доктор технических наук), и т.п. (и тому подобное), и т.д. (и так далее).

Когда в КП используются нестандартные аббревиатуры, сокращенно обозначающие какие-либо понятия из соответствующих областей знания, то после первого упоминания полного названия в скобках указывается аббревиатура, например: курсовой проект (КП), комплексная система защиты

информации (КСЗИ). В дальнейшем при упоминании этих понятий по тексту в основном употребляют их аббревиатуру.

5. Защита курсового проекта

Студент должен тщательно подготовиться к защите курсового проекта.

Законченный КП должен быть отредактирован, вычитан, подписан студентом и представлен руководителю.

После проверки КП руководитель решает вопрос о допуске студента к защите, делая об этом соответствующую запись на титульном листе курсового проекта. Защита КП осуществляется в форме собеседования.

По результатам защиты КП руководитель принимает решение об оценке проекта.

Студент, не защитивший КП, допускается к повторной защите не ранее, чем через неделю после первой защиты.

Студенты, вовремя не защитившие курсовые проекты по неуважительным причинам, к экзамену по данной дисциплине не допускаются**.** Для допуска к экзамену в назначенное время для пересдачи***, необходимо получить у преподавателя новую тему КП*** и успешно его защитить в установленные сроки до начала пересдачи экзаменов**.**

6. Критерии оценки курсового проекта

Оценка курсового проекта определяется исходя из двух критериев:

- качества КП;
- ответов на вопросы.

Качество КП оценивается руководителем по составляющим, приведенным в таблице.

Таблица

Оценка качества курсового проекта

№ п/п	Наименование критерия	Оценка качества курсового проекта			
		«отлично»	**«хорошо»**	**«удовлетворительно»**	**«неудовлетворительно»**
			Не более 20% вопросов	Более половины вопросов задания на	

1.	Содержание курсового проекта	Достаточно полно разработаны все вопросы задания на КП. Имеются обоснованные выводы по главам и в целом по проекту	задания на КП разработаны недостаточно полно. Обоснованные выводы по главам и в целом по КП в основном имеются	КП разработаны недостаточно полно. Обоснованные выводы по главам и в целом по КП имеются частично	Не разработан (исследован) хотя бы один вопрос задания на КП. Выводы по главам и в целом по КП отсутствуют
2.	Обоснованность и доказательность принятых решений	Все предложения (решения) математически, логически или экспериментально обоснованы (доказаны)	В основном предложения (решения) математически, логически или экспериментально обоснованы (доказаны)	Предложения (решения) математически, логически или экспериментально обоснованы (доказаны) частично	Отсутствует математическое, логическое или экспериментально обоснованное доказательство принятых решений и разработанных предложений
3.	Соответствие чертежей, рисунков и схем требованиям ГОСТ и ЕСКД	Полностью соответствует	В основном соответствует	Частично соответствует	Не соответствует
4.	Практическое значение выполненного проекта	Имеется	В основном имеется	Частично имеется	Отсутствует
5.	Грамотность изложения и качество оформления КП	Оформлен аккуратно. Имеются несущественные стилистические ошибки, исправления (не более одного исправления на лист)	Оформлен в основном аккуратно. Имеются несущественные стилистические и грамматические ошибки, исправления (не более трех исправлений на лист)	Оформлен небрежно. Имеются стилистические и грамматические ошибки, большое количество исправлений	Оформлен небрежно. Имеются грубые стилистические и грамматические ошибки,
6.	Самостоятельность выполнения (владение материалом), использование научной,	Полностью самостоятельно	В основном самостоятельно	Частично самостоятельно	КП выполнен не самостоятельно

	технической и справочной литературы				

Для выставления оценки **«отлично»** необходимо, чтобы оценка по трем пунктам (включая 1 и 2) была «отлично», а по остальным - не ниже «хорошо».

Для выставления оценки **«хорошо»** необходимо, чтобы оценка по трем пунктам (включая 1 и 2) была не ниже «хорошо», а по остальным - не ниже «удовлетворительно».

При получении хотя бы по одному из пунктов неудовлетворительной оценки общая оценка не может быть выше, чем **«удовлетворительно».**

Оценка **«неудовлетворительно»** выставляется при оценке «неудовлетворительно» по 1 и 2 или по трем и более пунктам критериев.

Ответ на вопрос оценивается на:

- «отлично» - если ответ правильный, уверенный, четкий и полный;

- «хорошо» - если ответ, в основном полный, правильный и уверенный, но допущены незначительные погрешности, исправленные после дополнительных вопросов;

- «удовлетворительно» - если ответ неполный, неуверенный, нечеткий, отдельные положения неправильные, но путем наводящих вопросов, в основном, достигается необходимая полнота ответов;

- «неудовлетворительно» - если ответ сумбурный, неправильный, содержит существенные, принципиальные ошибки, а студент не понимает сущности излагаемого вопроса или не дает на него ответ.

Общая оценка за ответы на вопросы слагается из оценок, полученных за отдельные ответы, и определяется следующим образом:

- «отлично» - если отсутствуют неудовлетворительные оценки и средний балл за все оценки – не менее 4,5;

- «хорошо» - если отсутствуют неудовлетворительные оценки и средний балл за все оценки – не менее 3,5;

- «удовлетворительно» - если более половины всех оценок не ниже «удовлетворительно»;

- «неудовлетворительно» - если не выполняются требования для получения «удовлетворительной» оценки.

Итоговая оценка курсового проекта определяется следующим образом:

- «отлично» - если по всем критериям выставлены оценки не ниже «хорошо», причем не менее, чем по двум (включая 1) критериям – «отлично»;

- «хорошо» - если по всем критериям выставлены оценки не ниже «удовлетворительно», причем не менее, чем по двум (включая 1) критериям не ниже «хорошо»;

- «удовлетворительно» - если по всем критериям выставлены оценки не ниже «удовлетворительно»;

- «неудовлетворительно» - если не выполняются требования для получения «удовлетворительной» оценки.