ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказом ректора
от «31» мая 2024 г. № 425-1

Б1.О.37 Защита информации от утечки по техническим каналам

рабочая программа дисциплины

Специальность/направление подготовки – 10.05.03 Информационная безопасность автоматизированных систем
Специализация/профиль – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – очная форма 5 лет, 6 месяцев
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 8
Часов по учебному плану (УП) – 288

Формы промежуточной аттестации
очная форма обучения:
зачет 7 семестр, экзамен 6 семестр, курсовой проект 6 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	6	7	**Итого**
Вид занятий	Часов по УП	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	51	68	**119**
– лекции	34	34	**68**
– практические (семинарские)		17	**17**
– лабораторные	17	17	**34**
Самостоятельная работа	93	40	**133**
Экзамен	36		**36**
Итого	180	108	**288**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем утвержденным Приказом Минобрнауки России от от 26.11.2020 № 1457.

Программу составил(и):
д.т.н., доцент, доцент, В.В. Ерохин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «21» мая 2024 г. № 11

Зав. кафедрой, к. э. н, доцент Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели дисциплины

1	развитие у обучающихся социально-личностных качеств: коммуникативности, организованности, ответственности, трудолюбия, целеустремленности
2	формирование профессиональных знаний, навыков и умений в области технической защиты информации

1.2 Задачи дисциплины

1	формирование профессиональных знаний, навыков и умений по установке, настройке, эксплуатации и поддержании в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований
2	участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем
3	получение навыков сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности
4	получение навыков сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования
5	участие в проведении экспериментов по заданной методике, обработка и анализ их результатов
6	участие в совершенствовании системы управления информационной безопасностью

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.
Цель достигается по мере решения в единстве следующих задач:
– формирование сознательного отношения к выбранной профессии;
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;
– формирование психологии профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Б1.О.34 Документоведение
2	Б1.О.36 Сети и системы передачи информации
3	Б1.О.47 Информационные технологии
4	Б1.О.51 Кибербезопасность

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б1.О.31 Безопасность сетей ЭВМ
2	Б1.О.39 Программно-аппаратные средства защиты информации
3	Б1.О.42 Открытые информационные системы
4	Б1.О.43 Криптографические протоколы и стандарты
5	Б1.О.45 Виртуальные частные сети
6	Б1.О.54 Методы и средства криптографической защиты информации
7	Б1.О.55 Защита объектов критической информационной инфраструктуры
8	Б1.О.60 Защита информации от несанкционированного доступа
9	Б1.О.62 Моделирование процессов и систем защиты информации
10	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
11	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-9 Способен	ОПК-9.1 Проводит анализ	Знать: основные источники и носители конфиденциальной

решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных	информации; текущее состояние и тенденции развития сетей и систем передачи информации; демаскирующие признаки объектов защиты; угрозы безопасности информации, возникающие за счет технических каналов утечки информации
		Уметь: проводить анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных; описывать (моделировать) объекты защиты
		Владеть: навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации; навыками настройки и эксплуатации средств технической защиты информации
	ОПК-9.3 Знает текущее состояние и тенденции развития сетей и систем передачи информации	Знать: принципы и основные средства добывания информации; возможности технических каналов утечки информации и методы их оценки; основные нормативные и методические документы по технической защите информации; технические средства защиты информации автоматизированных систем
		Уметь: выявлять и оценивать угрозы безопасности информации по техническим каналам утечки информации; устанавливать, настраивать и проверять работоспособность средств защиты информации
		Владеть: навыками составления отчетов по результатам исследований защищенности объекта информации; специальной терминологией
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Знать: методы и способы защиты информации, показатели эффективности защиты; средства криптографической и технической защиты информации для решения задач профессиональной деятельности
		Уметь: использовать средства криптографической защиты информации при решении задач профессиональной деятельности; определять рациональные меры защиты на объектах и оценивать их эффективность; контролировать эффективность мер технической защиты информации
		Владеть: методами проведения контроля безопасности информации от утечки по техническим каналам; навыками проведения инструментальных исследований

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Объекты информационной защиты.**						
1.1	Тема 1. Введение. Объекты информационной защиты.	6	2			4	ОПК-9.3 ОПК-10.1
1.2	Тема 2. Источники и носители конфиденциальной информации.	6	2			4	ОПК-9.3
1.3	Тема 3. Демаскирующие признаки объектов защиты и сигналов. Выдача тем курсовых проектов.	6	4		4	6	ОПК-9.3
2.0	**Раздел 2. Технические каналы утечки информации.**						
2.1	Тема 4. Структура, классификация и основные характеристики технических каналов утечки информации	6	2			4	ОПК-9.1 ОПК-9.3
2.2	Тема 5. Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.	6	4		4	4	ОПК-10.1
2.3	Тема 6. Технические каналы утечки речевой информации	6	2			4	ОПК-9.1 ОПК-9.3
2.4	Тема 7. Технические каналы утечки видовой информации	6	2			4	ОПК-9.1 ОПК-9.3
2.5	Тема 8. Каналы утечки информации при ее передаче по каналам связи. Проработка теоретической части	6	2		4	6	ОПК-9.3

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
	курсового проекта.						
3.0	**Раздел 3. Способы и средства добывания информации техническими средствами.**						
3.1	Тема 9. Классификация и возможности технической разведки	6	2			4	ОПК-9.3 ОПК-10.1
3.2	Тема 10. Технические средства доступа, перехвата и съема информации.	6	2		2	4	ОПК-9.1
3.3	Тема 11. Направленные микрофоны. Проводные системы, портативные диктофоны и электронные стетоскопы. Проработка практической части курсового проекта.	6	4		2	4	ОПК-9.1 ОПК-9.3
3.4	Тема 12. Классификация устройств съема информации с телефонной линии. Перехват сигналов сотовых телефонов	6	2			4	ОПК-10.1
3.5	Тема 13. Средства фотосъемки и видеонаблюдения. Защита курсовых проектов.	6	2		1	4	ОПК-9.1 ОПК-9.3
3.6	Тема 14. Принципы радиолокационного наблюдения	6	2			4	ОПК-9.1
	Форма промежуточной аттестации – экзамен	6	36				ОПК-9.1 ОПК-9.3 ОПК-10.1
4.0	**Раздел 4. Методы, способы и средства технической защиты информации.**						
4.1	Тема 15. Концепция инженерно-технической защиты информации	7	2			6	ОПК-9.1
4.2	Тема 16. Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения	7	2	2		6	ОПК-9.3
4.3	Тема 17. Классификация, виды и принцип действия средств обнаружения и локализации закладных устройств	7	4		4	6	ОПК-9.1
4.4	Тема 18. Многофункциональные комплекты и комплексы для выявления каналов утечки информации	7	4		4	6	ОПК-9.1
4.5	Тема 19. Обнаружение скрытых камер и закладных устройств с помощью нелинейного локатора	7	2	2	2	4	ОПК-9.1 ОПК-9.3 ОПК-10.1
4.6	Тема 20. Методы и средства защиты от утечки информации по акустоэлектрическому каналу	7	2	2	2	1	ОПК-9.1 ОПК-9.3
4.7	Тема 21. Подавление информативных сигналов в цепях заземления и электропитания	7	4		1	4	ОПК-9.3 ОПК-10.1
4.8	Тема 22. Экранирование и компенсация информативных полей	7	2	2		6	ОПК-9.1
4.9	Тема 23. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	7	4		4	4	ОПК-9.3
4.10	Тема 24. Сетевые пассивные полосно-заграждающие и полосно-пропускающие фильтры	7		2		6	ОПК-9.3
5.0	**Раздел 5. Организация деятельности по технической защите информации.**						
5.1	Тема 24. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации от утечки по техническим каналам.	7	2	3		6	ОПК-9.1
5.2	Тема 25. Технический контроль эффективности защиты информации	7	2	2			ОПК-9.1 ОПК-9.3
5.3	Тема 26. Общие положения по специальным проверкам, специальным обследованиям и специальным исследованиям. Заключение	7	4	2		6	ОПК-9.1 ОПК-9.3
	Форма промежуточной аттестации – зачет	7					ОПК-9.1 ОПК-9.3 ОПК-10.1
	Курсовой проект	6				12	ОПК-9.1 ОПК-9.3 ОПК-10.1

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
	Итого часов (без учёта часов на промежуточную аттестацию)		68	17	34	133	

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — URL: https://e.lanbook.com/book/130184 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Аникин, Д. В. Информационная безопасность и защита информации : учебное пособие / Д. В. Аникин. — Санкт-Петербург : ИЭО СПбУТУиЭ, 2011. — 269 с. — URL: http://e.lanbook.com/books/element.php?pl1_id=63950 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.3	Аршинский, Л. В. Техническая защита информации: практикум : практикум / Л. В. Аршинский, А. А. Бутин, Н. И. Глухов, П. Ю. Пушкни, В. В. Ерохин. — Иркутск : ИрГУПС, 2022. — 76 с. — URL: https://e.lanbook.com/book/342083 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.4	Исаева, М. Ф. Техническая защита информации : учебное пособие / М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2017. — 49 с. — URL: https://e.lanbook.com/book/101600 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Аршинский, Л. В. Техническая защита информации : практикум / Л. В. Аршинский, А. А. Бутин, Н. И. Глухов [и др.]. Иркутск : ИрГУПС, 2022. - 76с.	17
6.1.2.2	Горбачев, А. А. Техническая защита информации. Поисковые приборы : учебное пособие / А. А. Горбачев, С. И. Алешников. — Калининград : БФУ им. И.Канта, 2022. — 148 с. — URL: https://e.lanbook.com/book/310139 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.2.3	Раков, А. С. Техническая защита информации : учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева, А. О. Почепцов, В. О. Гуреев. — Самара : ПГУТИ, 2020. — 96 с. — URL: https://e.lanbook.com/book/255575 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн

6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Ерохин, В.В. Методические указания по изучению дисциплины Б1.О.37 Защита информации от утечки по техническим каналам по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Безопасность открытых информационных систем / В.В. Ерохин; ИрГУПС. – Иркутск: ИрГУПС, 2024. – 17 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47629_1529_2024_1_signed.pdf	Онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»	
6.2.1	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/
6.3 Программное обеспечение и информационные справочные системы	
6.3.1 Базовое программное обеспечение	
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License
6.3.2 Специализированное программное обеспечение	
6.3.2.1	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01
6.3.2.2	Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html
6.3.2.3	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/
6.3.2.4	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.
6.3.2.5	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01. прогр.средство защиты от НСД Secret Net4.0, клиент серв.безоп.Secret Net 4.0, сервер безопасности C Secret Net4.0
6.3.3 Информационные справочные системы	
6.3.3.1	Не предусмотрены
6.4 Правовые и нормативные документы	
6.4.1	Не предусмотрены

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	
1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор,экран, (ноутбук переносной)
3	Лаборатория Д-525 «Специальные средства и методы защиты информации».«Техническая защита информации» для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, Мультимедиапроектор (переносной), экран (переносной), компьютер Милливольтметр В3-38Б, Учебный стенд "Защита информации от утечки за счет электроакустических преобразований", Учебный стенд "Практика применения программно-аппаратного комплекса радиомониторинга RS-turbo", имитатор р/микрофона, программно-аппаратный комплекс "Легенда-05", Программно-аппаратный комплекс "Спрут-7", Учебный стенд "Защита информации от утечки за счет побочных электромагнитных излучений", Компьютер DEPO Neos 240SE/C2.67D/256/80G/FDD/LAN/KB/Mo , Учебный стенд "Защита информации от утечки по сети 220В", Учебный стенд "Некриптографические методы защиты информации в телефонных каналах связи", Генератор шума Октава-ВА., Генератор шума по сети Октава-Ш. , локатор нелинейный+ аккум.блок+зар.устр-во (Катран), поисковый прибор "Пиранья", Имитатор работы "Пиранья", виброизлучатель ВИ-45 00-000000000002011, виброизлучатель ВИ-45 00-000000000002012, Виброизлучатель СТД-М, микрофон направленный, микрофон с наушниками, аналоговый детектор поля, генератор ГЭШ 63, обнаружитель видеокамер средствами контроля и управления доступом в помещения, лабораторный стенд "Охранно-пожарная сигнализация"
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507;

	– помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного

	эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Защита информации от утечки по техническим каналам» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией Университета, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Защита информации от утечки по техническим каналам» участвует в формировании компетенций:

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
6 семестр				
1.0	**Раздел 1. Объекты информационной защиты**			
1.1	Текущий контроль	Тема 1. Введение. Объекты информационной защиты.	ОПК-9.3 ОПК-10.1	Собеседование (устно)
1.2	Текущий контроль	Тема 2. Источники и носители конфиденциальной информации.	ОПК-9.3	Собеседование (устно)
1.3	Текущий контроль	Тема 3. Демаскирующие признаки объектов защиты и сигналов. Выдача тем курсовых проектов.	ОПК-9.3	Лабораторная работа (письменно/устно)
2.0	**Раздел 2. Технические каналы утечки информации**			
2.1	Текущий контроль	Тема 4. Структура, классификация и основные характеристики технических каналов утечки информации	ОПК-9.1 ОПК-9.3	Собеседование (устно)
2.2	Текущий контроль	Тема 5. Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.	ОПК-10.1	Лабораторная работа (письменно/устно)
2.3	Текущий контроль	Тема 6. Технические каналы утечки речевой информации	ОПК-9.1 ОПК-9.3	Доклад (устно)
2.4	Текущий контроль	Тема 7. Технические каналы утечки видовой информации	ОПК-9.1 ОПК-9.3	Доклад (устно)
2.5	Текущий контроль	Тема 8. Каналы утечки информации при ее передаче по каналам связи. Проработка теоретической части курсового проекта.	ОПК-9.3	Лабораторная работа (письменно/устно)
3.0	**Раздел 3. Способы и средства добывания информации техническими средствами**			
3.1	Текущий контроль	Тема 9. Классификация и возможности технической разведки	ОПК-9.3 ОПК-10.1	Лабораторная работа (письменно/устно)
3.2	Текущий контроль	Тема 10. Технические средства доступа, перехвата и съема информации.	ОПК-9.1	Доклад (устно)
3.3	Текущий контроль	Тема 11. Направленные микрофоны. Проводные системы, портативные диктофоны и электронные стетоскопы. Проработка практической части курсового проекта.	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
3.4	Текущий	Тема 12. Классификация	ОПК-10.1	Лабораторная работа

	контроль	устройств съема информации с телефонной линии. Перехват сигналов сотовых телефонов		(письменно/устно)
3.5	Текущий контроль	Тема 13. Средства фотосъемки и видеонаблюдения. Защита курсовых проектов.	ОПК-9.1 ОПК-9.3	Лабораторная работа (письменно/устно)
3.6	Текущий контроль	Тема 14. Принципы радиолокационного наблюдения	ОПК-9.1	Собеседование (устно)
	Промежуточная аттестация	Раздел 1. Объекты информационной защиты. Раздел 2. Технические каналы утечки информации.	ОПК-9.1 ОПК-9.3 ОПК-10.1	Курсовой проект (письменно) Курсовой проект (устно)
	Промежуточная аттестация	Раздел 1. Объекты информационной защиты. Раздел 2. Технические каналы утечки информации. Раздел 3. Способы и средства добывания информации техническими средствами.	ОПК-9.1 ОПК-9.3 ОПК-10.1	Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)
7 семестр				
4.0	**Раздел 4. Методы, способы и средства технической защиты информации**			
4.1	Текущий контроль	Тема 15. Концепция инженерно-технической защиты информации	ОПК-9.1	Доклад (устно)
4.2	Текущий контроль	Тема 16. Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения	ОПК-9.3	Собеседование (устно)
4.3	Текущий контроль	Тема 17. Классификация, виды и принцип действия средств обнаружения и локализации закладных устройств	ОПК-9.1	Собеседование (устно)
4.4	Текущий контроль	Тема 18. Многофункциональные комплекты и комплексы для выявления каналов утечки информации	ОПК-9.1	Лабораторная работа (письменно/устно)
4.5	Текущий контроль	Тема 19. Обнаружение скрытых камер и закладных устройств с помощью нелинейного локатора	ОПК-9.1 ОПК-9.3 ОПК-10.1	Лабораторная работа (письменно/устно)
4.6	Текущий контроль	Тема 20. Методы и средства защиты от утечки информации по акустоэлектрическому каналу	ОПК-9.1 ОПК-9.3	Собеседование (устно)
4.7	Текущий контроль	Тема 21. Подавление информативных сигналов в цепях заземления и электропитания	ОПК-9.3 ОПК-10.1	Собеседование (устно)
4.8	Текущий контроль	Тема 22. Экранирование и компенсация информативных полей	ОПК-9.1	Лабораторная работа (письменно/устно)
4.9	Текущий контроль	Тема 23. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	ОПК-9.3	Лабораторная работа (письменно/устно)
4.10	Текущий контроль	Тема 24. Сетевые пассивные полосно-заграждающие и полосно-пропускающие фильтры	ОПК-9.3	Собеседование (устно)
5.0	**Раздел 5. Организация деятельности по технической защите информации**			
5.1	Текущий контроль	Тема 24. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации от утечки по техническим каналам.	ОПК-9.1	Собеседование (устно)
5.2	Текущий	Тема 25. Технический контроль	ОПК-9.1	Собеседование (устно)

	контроль	эффективности защиты информации	ОПК-9.3	
5.3	Текущий контроль	Тема 26. Общие положения по специальным проверкам, специальным обследованиям и специальным исследованиям. Заключение	ОПК-9.1 ОПК-9.3	Собеседование (устно)
	Промежуточная аттестация	Раздел 4. Методы, способы и средства технической защиты информации. Раздел 5. Организация деятельности по технической защите информации.	ОПК-9.1 ОПК-9.3 ОПК-10.1	Зачет (собеседование) Зачет - тестирование (компьютерные технологии)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов
3	Лабораторная работа	Средство, позволяющее оценить умение обучающегося письменно/устно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы.	Образец задания для выполнения лабораторной работы и примерный перечень

		Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	вопросов для ее защиты

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий к зачету
2	Тест – промежуточная аттестация в форме зачета	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
3	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (образец экзаменационного билета) к экзамену
4	Тест – промежуточная аттестация в форме экзамена	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
5	Курсовой проект	Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	Образец задания для выполнения курсового проекта и примерный перечень вопросов для его защиты

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета и экзамена. Шкала оценивания уровня освоения компетенций

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»		Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал	Базовый

		хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	
«удовлетворительно»		Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Тест – промежуточная аттестация в форме зачета и экзамена

Шкала оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»		Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования
«удовлетворительно»		Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«неудовлетворительно»	«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Курсовой проект

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсового проекта полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсового проекта логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсового проекта и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсового проекта обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсового проекта полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсового проекта логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсового проекта и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. При защите курсового проекта обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
«удовлетворительно»	Содержание курсового проекта частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений

	слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсового проекта. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. При защите курсового проекта обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсового проекта в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсового проекта. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. При защите курсового проекта обучающийся демонстрирует слабое понимание программного материала. Курсовой проект не представлена преподавателю. Обучающийся не явился на защиту курсового проекта

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Доклад

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»		Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»		Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность

		выполнения низкая
«неудовлетворительно»	«не зачтено»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль доклада не передана

Лабораторная работа

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»		Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»		Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	«не зачтено»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся, не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Типовые контрольные задания для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования
«Тема 1. Введение. Объекты информационной защиты»

1. 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.
2. Каналы утечки информации, обрабатываемой техническими средствами приема,

обработки, хранения и передачи информации.
3. Электромагнитные, электрические, параметрические и вибрационные каналы
4. Какие меры существуют по защите информации
5.Что входит в подготовительные мероприятия: что нужно сделать для настройки системы защиты?

Образец типового варианта вопросов для проведения собеседования
«Тема 2. Источники и носители конфиденциальной информации»

1. Что является источников угрозы потери информации
2. Какие угрозы конфиденциальной информации существуют
3. Носители конфиденциальной информации
4. Назовите принципы информационной безопасности
5. Что приводит к неправомерному овладению конфиденциальной информацией в информационных системах?

Образец типового варианта вопросов для проведения собеседования
«Тема 4. Структура, классификация и основные характеристики технических каналов утечки информации»

1. Объясните физическую сущность возникновения побочных электромагнитных излучений.
2. Какие причины приводят к возникновению электрических каналов утечки информации?
3. Назовите основные виды каналов утечки акустической информации.
4. Покажите, на каких физических процессах в помещениях и размещенных в них ОТСС и ВТСС построены основные виды утечки акустической информации из помещений.
5. Чем обусловлены каналы утечки речевой

Образец типового варианта вопросов для проведения собеседования
«Тема 14. Принципы радиолокационного наблюдения»

1. Приведите структуру комплекса средств перехвата радиосигналов.
2. Как реализуется метод «высокочастотного навязывания»?
3. На чем основана реализация лазерного канала утечки информации?
4. Как реализуется метод «высокочастотного облучения»?
5. Назовите основные виды каналов утечки информации, передаваемой по каналам связи.
6. Назовите способы получения видовой информации.

Образец типового варианта вопросов для проведения собеседования
«Тема 16. Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения»

1. Чем обусловлены каналы утечки речевой информации из объемов выделенных помещений?
1. Как создаются составные каналы утечки информации?
2. Контроль эффективности защиты речевой информации от утечки по прямому акустическому и акустовибрационному каналам программно-аппаратным комплексом ПАК «Спрут-мини».
3. Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке).
4. Способы и средства защиты вспомогательных технических средств и систем.
5. Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи)

Образец типового варианта вопросов для проведения собеседования
«Тема 17. Классификация, виды и принцип действия средств обнаружения и локализации закладных устройств»

1. Каким параметром определяется зона возможного перехвата информации?
2. Каковы основные акустические параметры речевых сигналов?
3. От чего зависит звукоизоляция основных строительных конструкций?
4. Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?
5. Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?
6. Обнаружение и локализация закладных устройств негласного съема информации измерителем спектра вторичных полей «NR-μ».

Образец типового варианта вопросов для проведения собеседования
«Тема 20. Методы и средства защиты от утечки информации по акустоэлектрическому каналу»

1. Чем обусловлены материально-вещественные каналы утечки информации?
2. Чем и как обусловлено комплексирование каналов утечки информации?
3. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений;
4. Порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи.
5. Методика оценки возможностей средств акустической разведки по перехвату речевой информации. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки

Образец типового варианта вопросов для проведения собеседования
«Тема 21. Подавление информативных сигналов в цепях заземления и электропитания»

1. Экранирующие материалы, их основные характеристики.
2. Формула для расчета коэффициента экранирования для электрической и магнитной составляющей электромагнитного поля.
3. Экранированные помещения и экранированные камеры (классификация, состав, основные характеристики).
4. Основные требования к заземлению технических средств. Схемы заземлителей.
5. Схемы заземления технических средств. Схемы измерения сопротивления заземления технических средств.
6. Основные требования к системе пространственного электромагнитного зашумления.
7. Схема установки системы пространственного зашумления на объекте информатизации.
8. Основные требования по установке системы пространственного зашумления на объекте информатизации.
9. Основные характеристики генераторов шума

Образец типового варианта вопросов для проведения собеседования
«Тема 24. Сетевые пассивные полосно-заграждающие и полосно-пропускающие фильтры»

1. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.
2. Средства звуко- и виброизоляции выделенных помещений.
3. Звукоизолирующие кабины. Специальные защищенные помещения.
4. Порядок проведения контроля эффективности защиты ВТСС.
5. Состав и основные требования к аппаратуре контроля при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.
6. Схема измерительной установки при контроле ВТСС на подверженность

акустоэлектрическим преобразованиям.

Образец типового варианта вопросов для проведения собеседования
«Тема 24. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации от утечки по техническим каналам»

1. Лицензирование деятельности по технической защите информации.
2. Сертификация технических средств защиты информации.
3. Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты.
4. Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию.
5. Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации.
6. Порядок документального оформления результатов аттестационных испытаний и соответствия объекта информатизации требованиям по безопасности информации.

Образец типового варианта вопросов для проведения собеседования
«Тема 25. Технический контроль эффективности защиты информации»
Средства акустической разведки: цифровые диктофоны, направленные микрофоны (классификация, характеристики, основные возможности, схема канала перехвата).

1. Дальность перехвата речевого сигнала средствами акустической разведки.
2. Схемы перехвата речевой информации по акустовибрационному каналу утечки речевой информации.
3. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.
4. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.

Образец типового варианта вопросов для проведения собеседования
«Тема 26. Общие положения по специальным проверкам, специальным обследованиям и специальным исследованиям. Заключение»

1. Акустический канал утечки информации, методы и средства защиты.
2. Виброакустический канал утечки информации, методы и средства защиты.
3. Акустоэлектрический и параметрический канал утечки информации, методы и средства защиты.
4. Оптико-электронный канал утечки информации, методы и средства защиты.

3.2 Типовые контрольные темы для написания докладов

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов тем для написания докладов.

Образец тем докладов
«Тема 6. Технические каналы утечки речевой информации»

1. Каналы утечки речевой информации.
2. Акустические каналы. Виброакустические каналы.
3. Акустоэлектрические каналы.
4. Оптико-электронные каналы.
5. Параметрические каналы

Образец тем докладов
«Тема 7. Технические каналы утечки видовой информации»

1. Технические каналы утечки информации, возникающей при работе вычислительной

техники за счет ПЭМИН.
2. Электрические и магнитные излучатели электромагнитного поля.
3. Электрические каналы утечки информации

Образец тем докладов

«Тема 10. Технические средства доступа, перехвата и съема информации»

1. Индикаторы электромагнитных излучений.
2. Радиочастотомеры.
3. Сканирующие приемники, селективные вольтметры, анализаторы спектра.
4. Автоматизированные поисковые комплексы
5. Характеристики нелинейных локаторов и селективных металлодетекторов.

Образец тем докладов

«Тема 15. Концепция инженерно-технической защиты информации»

1. Организационно-методические основы защиты информации.
2. Общие требования к защите информации.
3. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации
4. Организация защиты информации. Основные методы инженерно-технической защиты информации.

3.3 Типовые задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Тема 3. Демаскирующие признаки объектов защиты и сигналов. Выдача тем курсовых проектов»

Индивидуальное задание: подготовить реферат о технологиях и средствах противодействия наблюдению. Демаскирующие признаки объектов защиты и сигналов.

Вопросы:

1. Факторы, влияющие на эффективность поиска объектов наблюдения.
2. Способы маскировки объектов наблюдения.
3. Виды маскировочного окрашивания.
4. Различия в механизме маскировки защитного и деформирующего окрашивания.
5. Что представляют собой искусственные маски?
6. Чем засветка отличается от ослепления?
7. Специфика структурного скрытия объекта от радиолокационного наблюдения.
8. Особенности защиты от гидроакустического зашумления

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Тема 5. Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники»

Цель занятия: Изучить назначение, возможностей, функции и условия применимости технических средств уничтожения информации на магнитных носителях, регистрации информации в телефонных каналах

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для

их защиты

«Тема 8. Каналы утечки информации при ее передаче по каналам связи. Проработка теоретической части курсового проекта»

Целью лабораторной работы является освоение методики оценки защищенности основных технических средств и систем (ОТСС), предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации, от утечки информации за счет побочных электромагн Установление режима тестирования для исследуемого ОТСС в соответствии с требовании к тестовым режимам ра¬боты технических средств.

Определение инструментальным путем частотного спектра ПЭМИ исследуемого ОТСС, состоящего из набора спектральных составляющих f1, f2,…, fi,…, fk (где i - натуральные числа от 1 до k: k - число, соответствую-щее полному набору спектральных составляющих).

Определение направления максимального излучения по каждой спектральной составляющей fi ПЭМИ. Установку антенны измерителя напряженности поля (ИНП) на расстоянии R0 от исследуемого ОТСС (источника излучения). Исходя из требований минимального влияния суммарной погрешности (ошибки в выборе расстояния) на результат измерений, значение расстояния R0 от исследуемого ОТСС до места установки антенны

ИНП рекомендуется принять равным 1м Раздельное измерение в направлении минимального расстояния до границы контролируемой зоны (КЗ) объекта напряженности электромагнитного поля, возникающей за счет излучения информативного сигнала, по магнитной pHi (в диапазоне частот от 9 кГц до 30 МГц и электрической Ei (в диапазоне частот от 9 кГц до 1000 МГц) составляющим.

Частотный спектр ПЭМИ исследуемого ОТСС определяют по идентификационным признакам заданного (тестового) режима его работы. Для определения полного набора информативных составляющих сигналов ПЭМИ антенны ИНП устанавливают на минимальном расстоянии от исследуемого ОТСС. Анализ спектра производят в диапазоне частот от 9 кГц до 1000 МГц. По результатам анализа определяют f1, f2,…, fi,…, fk.

Направление максимального ПЭМИ для i-ой спектральной составляющей информативного сигнала определяют в горизонтальной плоскости путем поворота ОТСС на 360 градусов вокруг своей осиитных излучений (ПЭМИ).

Подготовка к проведению измерений

1. Устанавливают антенну ИНП на расстоянии 1м от ОТСС.

2. На ОТСС устанавливают тестовый режим работы.

3. Проводят подготовительные работы в соответствии с инструкцией по эксплуатации ИНП (присоединение измерительной антенны, выдержка во включенном состоянии, калибровка и т.д.).

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Тема 9. Классификация и возможности технической разведки»

1. Собрать измерительную установку согласно пунктам по подготовке к проведению работы. Измерительную антенну установить на расстоянии одного метра от проверяемого монитора.

2. На проверяемом компьютере запустить программу MonTest.exe (Monitor Test) и в окне программы (с описанием инструкции к программе) нажать на кнопку «Запустить тест». На экране монитора отобразятся черно-белые полоски в полноэкранном режиме. С помощью клавиатуры настроить минимальную ширину отображаемых полосок (1 пиксель).

3. Перемещаясь по диапазону сканируемых частот, найти на экране анализатора спектра пик сигнала, соответствующий демодулированному сигналу монитора.

4. Если сигнал на спектрограмме похож на ожидаемый демодулированный сигнал монитора, выключить отображаемые полоски (черный экран) с помощью клавиатуры. Если пик сигнала на экране анализатора спектра исчезнет, то это будет означать, что найден сигнал с частотой, на которой происходит излучение от работающего монитора.

5. С помощью кнопки MARKER анализатора спектра и плавного регулятора

установить маркер на пик обнаруженного сигнала и записать частоту сигнала – fi.

6. Записать уровень сигнала на этой частоте при работающей программе теста монитора (черно-белые полоски) – E0i;

7. Записать уровень сигнала на этой частоте при выключенной программе теста монитора (черный экран) – Eшi;

8. В процессе проверки может оказаться, что частота сигнала от монитора близка к рабочей частоте какого-либо телевизионного сигнала или радиосигнала. Вид демодулированного теле- (радио) сигнала близок к ожидаемому пику от монитора. Если при выключении программы теста монитора уровень сигнала уменьшится не менее чем на 3 дБ, то это будет означать, что сигнал от проверяемого монитора обнаружен.

9. Перемещаясь по диапазонам частот анализатора спектра, обнаружить нечетные гармоники (частоты, в 3, 5, 7 и т.д. раз больше основной частоты) сигнала монитора и повторить пункты 3-8. Записать результаты измерений для обнаруженных гармоник.

10. После завершения измерений для каждой из обнаруженных частот вычислить:

– уровень информативного сигнала от проверяемого оборудования Eci по формуле (5);

– длину волны λi по формуле (7);

– границу ближней и промежуточной зоны L1i по формуле (8);

– границу промежуточной и дальней зоны L2i по формуле (9);

– значение напряженности информативного сигнала на границе ближней и промежуточной зоны E1i по формуле (10);

– значение напряженности информативного сигнала на границе промежуточной и дальней зоны E2i по формуле (11).

Примечание: перед вычислением уровней информативного сигнала от проверяемого оборудования необходимо перевести измеренные данные из дБ в мкВ/м по формуле (3).

11. На основании полученных данных вычислить значения радиусов контролируемой зоны Ri для каждой из обнаруженных частот по формулам (13), (14) или (15) в зависимости от того, в какую из зон распространения электромагнитного поля (ближнюю, промежуточную или дальнюю) попадает значение Ri.

12. Обозначение зоны стоит вносить в последнюю строку в виде следующих сокращений: «бл» – в ближней зоне, «пр» – в промежуточной зоне, «дл» – в дальней зоне.

13. Выбрать наибольшее из полученных значений Ri в качестве минимально необходимого радиуса контролируемой зоны R.

14. Сделать вывод о защищенности технического средства от утечки информации по каналу ПЭМИ, сравнив полученное значение R с радиусом контролируемой зоны RКЗ по заданию преподавателя

Вопросы:

1. Каковы причины появления канала утечки информации за счет ПЭМИ?

2. Почему наибольшую опасность представляют сигналы, излучаемые монитором?

3. Какой тип модуляции у сигналов, излучаемых средствами ОТСС?

4. Вследствие чего происходит искажение формы демодулированных сигналов на выходе анализатора спектра PROTEK 3201 или селективного вольтметра SMV-8.5?

5. Какие дополнительные устройства применяются для выделения сигнала от отдельного персонального компьютера?

6. Пассивные и активные методы защиты.

7. Блок-схема широкополосного генератора радиошума.

8. Блок-схема «полосового» генератора радиошума.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Тема 11. Направленные микрофоны. Проводные системы, портативные диктофоны и электронные стетоскопы. Проработка практической части курсового проекта»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для

их защиты

«Тема 12. Классификация устройств съема информации с телефонной линии. Перехват сигналов сотовых телефонов»

При дальнейшем изложении используются следующие условные обозначения:

i – номер компоненты тест-сигнала;

$U_{(с+ш)i}$ – напряжение смеси обнаруженных компонент тест-сигнала и шума, дБ;

$U_{шi}$ – уровень шума в линии, дБ;

f – частота, МГц;

K – общее число спектральных составляющих в спектре информативного сигнала;

U_{ci} – напряжение сигнала в линии, дБ;

$П_i$ – показатель защищенности, дБ;

$К_{Пi}$ – коэффициент погонного затухания наведенных сигналов в исследуемой линии, дБ;

$U_{1\ измi}$ – напряжение специально созданного сигнала, измеренное на частоте f_i в исследуемой линии в непосредственной близости от ОТСС, мкВ;

$U_{2\ измi}$ – напряжение специально созданного сигнала, измеренное на частоте f_i в исследуемой линии на некотором удалении от ОТСС, мкВ;

R_i – максимальная длина пробега исследуемой линии, на которой возможно выделение информативного сигнала, м;

$R_{КЗ}$ – реальный пробег исследуемой линии до границы контролируемой зоны, м.

Суть методики заключается в оценке возможности выявления информативных сигналов от наводок ПЭМИ ОТСС в исследуемой цепи на границе контролируемой зоны (КЗ).

При этом критерием защищенности информации является, фактически, отношение сигнал/шум на границе КЗ, нормативное значение которого равно 1 для ОТСС, не имеющих видеоконтрольных устройств (ВКУ), и 0,3 для ОТСС, имеющих в своем составе ВКУ. Однако в силу того, что в большинстве реальных ситуаций возможность измерения уровней сигналов на границе КЗ отсутствует, методика несколько усложняется.

В общем случае методика оценки защищенности информации от утечки за счет наводок ПЭМИ ОТСС на цепи электропитания включает следующие экспериментально-расчетные процедуры.

1. Устанавливается режим тестирования на ОТСС и выявляются информативные частотные составляющие от наводок ПЭМИ (f_1, f_2,… f_n) в исследуемой цепи. При этом рекомендуется применять специальные тестовые программы, аттестованные ФСТЭК России. Анализ спектра ПЭМИ ОТСС проводят в диапазоне частот 0,01-250 МГц.

2. Измеряется уровень смеси «сигнал + шум» $U_{(с+ш)i}$ в линии на частотах выявленных компонент тест-сигнала.

3. Измеряется уровень шума $U_{шi}$ в линии на частотах выявленных компонент тест-сигнала.

4. Рассчитывается значения сигнала U_{ci} в линии:

$$U_{ci} = 20 \lg \sqrt{10^{U(с+ш)i/10} - 10^{Uшi/10}} \text{ (дБ)}. \quad (4)$$

5. Рассчитывается показатель защищенности в точке проведения измерений для каждой из частотных компонент (фактически, отношение сигнал/шум):

$$П_i = U_{ci} - U_{шi} \text{ (дБ)}. \quad (5)$$

6. Рассчитывается коэффициент погонного затухания $К_{Пi}$ наведенных сигналов в исследуемой линии для каждой из частотных компонент:

$$K_{Пi} = \frac{20 \lg(U_{1\ измi}/U_{2\ измi})}{L} \text{ (дБ/м)}, \quad (6)$$

где $U_{1\ измi}$ – напряжение специально созданного сигнала (при помощи генератора сигналов), измеренное на частоте f_i в точке А, мкВ (рис. 7.7); $U_{2\ измi}$ – напряжение специально созданного сигнала, измеренное на частоте f_i в точке Б, мкВ (рис. 7)

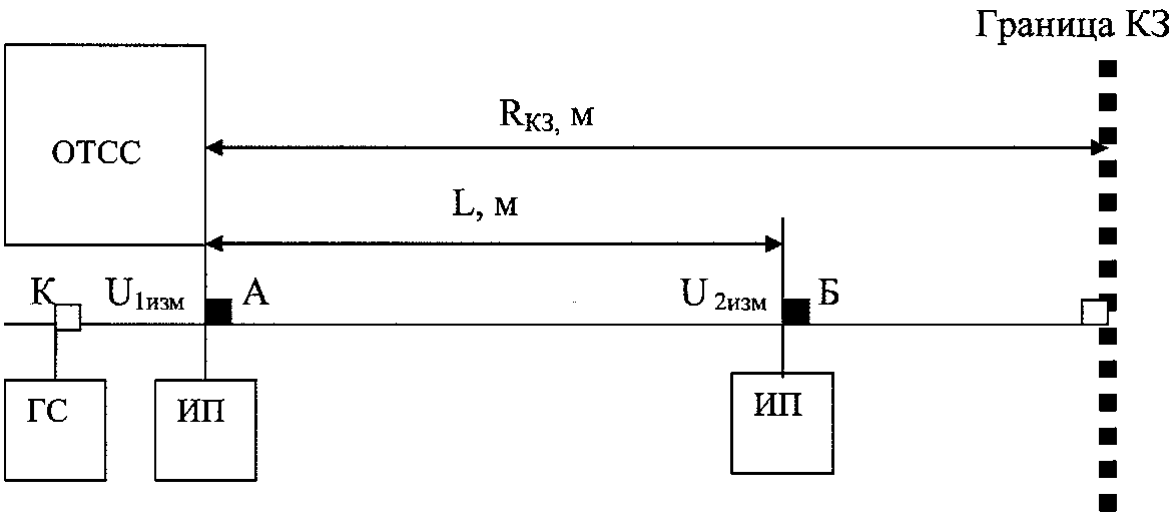

Рис. 7. Схема измерения коэффициента погонного затухания:
ОТСС – персональный компьютер; ГС – генератор сигналов; ИП – измерительный приемник

7. Рассчитывается максимальная длина пробега R_i исследуемой линии для каждой из частот, на которой возможно выделение информативного сигнала. Для ОТСС, имеющих в своем составе видеоконтрольные устройства, при нормированном значении отношения сигнал/шум, равном 0,3:

$$R_i = \frac{П_i + 10}{K_{Пi}} \text{ (м).} \quad (7)$$

Для ОТСС, не имеющих видеоконтрольных устройств, при нормированном значении отношения сигнал/шум, равном единице:

$$R_i = \frac{П_i}{K_{Пi}} \text{ (м).} \quad (8)$$

8. Выбирается максимальное из полученных значений R_i и сравнивается с пробегом линии до границы КЗ. Если пробег исследуемой линии до границы КЗ больше максимального из всех R_i, то делается вывод о защищенности информации обрабатываемой ОТСС от утечки за счет наводок в исследуемую линию. Если нет, то делается вывод о необходимости принятия дополнительных мер защиты.

Вопросы:

1. Технические каналы утечки информации по цепям электропитания и основные принципы их блокирования.
2. Эквивалентная схема цепи электропитания и ее основные характеристики.
3. Пассивные методы защиты информации от утечки по цепям электропитания; разновидности фильтров.
4. Требования, предъявляемые к сетевым фильтрам; характеристики серийно-выпускаемых фильтров.
5. Активные методы; принципы построения генераторов линейного зашумления.
6. Типовая структурная схема генераторов линейного зашумления.
7. Требования ФСТЭК России к генераторам шума по сети 220В; основные характеристики серийно-выпускаемых устройств.
8. Сетевые закладные устройства, их структурная схема и основные параметры.
9. Выявление закладных устройств. Принципы построения приемников-анализаторов.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Тема 18. Многофункциональные комплекты и комплексы для выявления каналов утечки информации»

Цель работы: освоить методику оценки защищенности помещения от утечки информации по акустическому и виброакустическому каналам и на ее основе произвести

расчет коэффициентов звуко- и виброизоляции защищаемого помещения.

Задание:

– получить теоретические знания о звуковых волнах и особенностях их распространения, методах звуко- и виброизоляции, генераторах акустического и виброакустического шума;

– изучить суть метода оценки коэффициентов звуко- и виброизоляции;

– ознакомиться с руководством оператора «Алгоритм-03» и собрать измерительную установку в контрольной точке по заданию преподавателя;

– произвести измерения, необходимые для расчетов;

– выполнить расчеты и сделать выводы;

– перечислить и проанализировать меры обеспечения защиты речевой информации

Вопросы:

1. Звук. Основные свойства звука
2. Основные характеристики звуковых волн.
3. Основные каналы утечки речевой информации.
4. Организационные меры по защите речевой информации.
5. Составление модели нарушителя.
6. Звукоизоляция. Звукопоглощение.
7. Основные методы звукоизоляции
8. Виброизоляция. Каналы утечки виброакустической информации.
9. Средства и методы защиты виброакустической информации.
10. Суть методики оценки коэффициентов звуко - и виброизоляции.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Тема 19. Обнаружение скрытых камер и закладных устройств с помощью нелинейного локатора»

При использовании нелинейного локатора необходимо, прежде всего, ознакомиться с инструкцией по эксплуатации, а также соблюдать правила техники безопасности. Ниже представлены общие положения по работе с локаторами.

Не следует направлять антенную систему в сторону глаз при расстоянии между антенным блоком и человеком менее одного метра.

Необходимо избегать длительного пребывания людей в зоне главного лепестка диаграммы направленности антенной системы.

Не рекомендуется направлять НЛ на пожарные или охранные датчики, да и вообще на работающие электронные средства, тем более возможные взрыватели, содержащие электронные схемы, поскольку возможно ложное срабатывание датчиков, пробивка электронных схем.

1.5. Состав лабораторного стенда

1. Нелинейный локатор «NR 900 EM».
2. Зарядное устройство.
3. Инструкция по эксплуатации НЛ.
4. Имитатор закладного устройства.
5. Измерительная установка.

1.6. Порядок выполнения работы

1. Ознакомиться с составом учебно-лабораторного стенда, правилами техники безопасности, изучить руководство по эксплуатации нелинейного локатора «NR 900 EM».

2. В соответствии с Приложением А собрать измерительную установку и проверить ее работоспособность. Перед включением собранную установку необходимо показать преподавателю.

3. Включить прибор. Провести оценку помеховой обстановки. Для этого с помощью кнопки АТТ− установить максимальную чувствительность приемников, при этом на экране ЖКИ (жидкокристаллического индикатора) в левой части 1-ой и 2-ой строки должны индицироваться символы 00. Направляя антенную систему в разные стороны и подключая

кнопкой OUT 2/3 головные телефоны к выходам приемников второй и третьей гармоник, убедиться в отсутствии помех на частотах приема при максимальной чувствительности приемников

4. Включить режим работы изделия «300» для чего вторично нажать кнопку ON/OFF пульта управления и индикации, при этом устанавливается максимальная выходная мощность передатчика, аттенюаторы приемников и головные телефоны находятся в положении, выбранном в п. 3.

5. Проверить работоспособность изделия с помощью штатного имитатора. Для этого расположить имитатор в свободном месте при отсутствии вблизи радиоэлектронной аппаратуры. Установить максимальный уровень зондирующего сигнала с помощью кнопки MAX/MIN (на экране ЖКИ в правой части 4-ой строки должен индицироваться символ Pmax) и максимальную чувствительность с помощью кнопок АТТ (на экране ЖКИ в левой части 1-ой и 2-ой строки должны индицироваться символы 00). С помощью кнопки OUT 2/3 переключить головные телефоны на выход приемника 2-ой гармоники. Направить антенную систему в сторону имитатора с расстояния 0,7-0,8 м. В головных телефонах должен прослушиваться тональный сигнал частоты 200 Гц средней громкости, а на экране ЖКИ в 1-ой и 2-ой строке должен индицироваться уровень принимаемого сигнала 2-ой и 3-ей гармоник соответственно. Удаление имитатора из зоны зондирования при неизменном положении антенной системы должно приводить к уменьшению и постепенному пропаданию сигнала-отклика.

6. Провести поиск имитатора закладного устройства в выделенном пространстве. Пространство для поиска назначается преподавателем. Определить точное местоположение имитатора закладного устройства.

Для определения точного местоположения средств съема информации необходимо:

– снизить уровень излучаемой мощности и чувствительность приемника;

– перемещая антенну около подозрительных зон, анализировать показания светового индикатора и частоту тонального сигнала в головных телефонах;

– определить направление прихода отраженного сигнала максимального уровня.

7. Используя показания уровней сигналов второй и третьей гармоник сигнала передатчика, провести идентификацию закладного устройства. Для этого необходимо следить за соотношением уровней сигналов-откликов второй и третьей гармоник на экране ЖКИ пульта управления и индикации. В случае существенного превышения уровня сигнала третьей гармоники над второй наиболее вероятно, что источником сигнала-отклика является коррозионная нелинейность.

8. Составить отчет о выполнении лабораторной работы.

Вопросы

1. Что называется вольтамперной характеристикой? ВАХ линейных и нелинейных элементов.
2. Отобразить на ВАХ нелинейного элемента в активном состоянии воздействие зондирующего сигнала.
3. Нелинейная локация. Определение и принцип.
4. Задачи нелинейной локации.
5. Основные классификационные признаки НЛ.
6. Какие характеристики антенны НЛ особенно важны?
7. Методы применения НЛ.
8. Поясните суть метода затухания.
9. Преимущества и недостатки импульсного НЛ по сравнению с НЛ непрерывного излучения?
10. Проведите сравнение НЛ «NR 900 EM» и «ЛОРНЕТ-24» по функциональным возможностям.
11. Правила безопасности при работе с нелинейным локатором.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Тема 22. Экранирование и компенсация информативных полей»

Цель работы: приобрести базовые навыки проведения мероприятий по обнаружению радиозакладных устройств в защищаемом помещении методом статистического анализа загрузки заданного радиодиапазона с помощью компьютерного комплекса радиоконтроля.

Задачи работы:

– изучить классификацию, принципы работы и демаскирующие признаки радиозакладных устройств;

– рассмотреть методы подавления сигналов радиозакладных устройств;

– ознакомиться с составом комплекса «RS digital Mobile 7G» и его функциональными возможностями;

– ознакомиться с принципами работы программно-аппаратного комплекса имитации сигналов закладных устройств «Аврова-Т» и с порядком формирования сигналов;

– сформировать различные сигналы закладных устройств с помощью программно-аппаратного комплекса «Аврова-Т» и продемонстрировать их обнаружение с помощью комплекса радиоконтроля «RS digital Mobile 7G»;

– провести анализ спектра радиосигнала и сделать вывод о принадлежности радиосигнала, выбранного преподавателем, к радиомикрофонной закладке.

Программно-аппаратный комплекс имитации сигналов закладочных устройств «Аврора-Т» обеспечивает формирование и излучение в эфир постоянно действующих радиосигналов с амплитудной, частотной и фазовой модуляцией, с возможностью изменения параметров модуляции. Параметры сигналов задаются и загружаются с помощью внешней ПЭВМ. Основной состав комплекса содержит основной блок имитатора, блок питания для подключения к сети переменного тока 220 В, внешнюю антенну, ПЭВМ типа ноутбук, кейс для укладки и переноски всего комплекта аппаратуры.

Имитатор «Аврора-Т» работает в диапазоне частот от 3 МГц до 3000 МГц с различными видами модуляции, в том числе:

– амплитудная модуляция;

– частотная модуляция;

– фазовая модуляция;

– GSM-сигнал;

– Bluetooth-сигнал;

– Wi-Fi-сигнал и др.

Данный комплекс обладает следующими возможностями:

– формирование и излучение в эфир радиосигналов с заданными оператором характеристиками;

– наличие библиотеки стандартных сигналов и возможность создания новых;

– применение для проверки реакции системы защиты информации, установленной на контролируемом объекте;

– применение в качестве тренажера при подготовке специалистов поиска сигналов подслушивающих устройств.

Вопросы:

1. Радиозакладные устройства это? Приведите их классификацию.

2. Расскажите принципы работы радиозакладного устройства. Из каких элементов оно состоит?

3. Перечислите демаскирующие признаки радиозакладных устройств.

4. Какие существуют способы подавления сигналов радиозакладок?

5. Перечислите методы обнаружения радиозакладок.

6. Какими возможностями обладает комплекс радиоконтроля «RS digital Mobile 7G»?

7. Как осуществляется поиск радиозакладных устройств с помощью данного комплекса?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Тема 23. Способы и средства предотвращения утечки информации через побочные

электромагнитные излучения и наводки»

Цель работы: освоить методику оценки защищенности помещения от утечки информации по каналам акустоэлектрических преобразований и проверить наличие микрофонного эффекта в основных и вспомогательных технических средствах.

Задачи работы:

– изучить акустоэлектрический канал утечки информации, физические эффекты, которые возникают в данном канале, а также элементы, которые являются источниками акустоэлектрических преобразований;

– ознакомиться с руководством оператора «СКМ-21.1» и собрать измерительную установку;

– провести инструментально-расчетную оценку защищенности от утечки речевой конфиденциальной информации по каналам акустоэлектрических преобразований в ВТСС;

– проанализировать полученные результаты и сделать выводы.

Для проведения измерений используются средства измерений и вспомогательное оборудование, на основе которых собираемся формирователь акустического тест-сигнала и анализатор низкочастотных сигналов. В нашем случае оборудование представляет собой:

1) цифровой шумомер Алгоритм-03 для калибровки АИ;

2) акустический излучатель Dialog W-203, для формирования тест-сигнала колонки;

3) анализатор маломощных электрических сигналов СКМ-21.1;

4) ноутбук с установленным программным обеспечением СКМ 21 ПО

5) режекторный фильтр, настроенный на частоты 50 и 150 Гц;

6) комплект соединительных проводов.

Вопросы:

1. Чем отличаются активные акустоэлектрические и преобразователи от пассивных преобразователей?

2. Какие угрозы создают случайные акустоэлектрические преобразователи?

3. Какие физические эффекты лежат в основе?

4. Какие устройства с акустоэлектрическим эффектом могут входить в состав некоторых ВТСС?

5. В каком случае проводную линию следует рассматривать как несимметричную?

6. Если акустоэлектрические преобразования обнаружены, то каким образом можно оценить их опасность?

7. Каким образом осуществляется перехват речевого сигнала в акустоэлектрическом канале?

3.4 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-9.3 ОПК-10.1	Тема 1. Введение. Объекты информационной защиты.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.3	Тема 2. Источники и носители конфиденциальной информации.	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт	1 – ОТЗ

		деятельности/ действие	1 –ЗТЗ
ОПК-9.3	Тема 3. Демаскирующие признаки объектов защиты и сигналов. Выдача тем курсовых проектов.	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 4. Структура, классификация и основные характеристики технических каналов утечки информации	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-10.1	Тема 5. Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 6. Технические каналы утечки речевой информации	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 7. Технические каналы утечки видовой информации	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.3	Тема 8. Каналы утечки информации при ее передаче по каналам связи. Проработка теоретической части курсового проекта.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.3 ОПК-10.1	Тема 9. Классификация и возможности технической разведки	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1	Тема 10. Технические средства доступа, перехвата и съема информации.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 11. Направленные микрофоны. Проводные системы, портативные диктофоны и электронные стетоскопы. Проработка практической части курсового проекта.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/	2 – ОТЗ 2 – ЗТЗ

		действие	
ОПК-10.1	Тема 12. Классификация устройств съема информации с телефонной линии. Перехват сигналов сотовых телефонов	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 13. Средства фотосъемки и видеонаблюдения. Защита курсовых проектов.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1	Тема 14. Принципы радиолокационного наблюдения	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1	Тема 15. Концепция инженерно-технической защиты информации	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.3	Тема 16. Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1	Тема 17. Классификация, виды и принцип действия средств обнаружения и локализации закладных устройств	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1	Тема 18. Многофункциональные комплекты и комплексы для выявления каналов утечки информации	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1 ОПК-9.3 ОПК-10.1	Тема 19. Обнаружение скрытых камер и закладных устройств с помощью нелинейного локатора	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 20. Методы и средства защиты от утечки информации по акустоэлектрическому каналу	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ

ОПК-9.3 ОПК-10.1	Тема 21. Подавление информативных сигналов в цепях заземления и электропитания	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1	Тема 22. Экранирование и компенсация информативных полей	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.3	Тема 23. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.3	Тема 24. Сетевые пассивные полосно-заграждающие и полосно-пропускающие фильтры	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1	Тема 24. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации от утечки по техническим каналам.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 25. Технический контроль эффективности защиты информации	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
ОПК-9.1 ОПК-9.3	Тема 26. Общие положения по специальным проверкам, специальным обследованиям и специальным исследованиям. Заключение	Знание	1 – ОТЗ 1 –ЗТЗ
		Умение	1 – ОТЗ 1 –ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 –ЗТЗ
		Итого	72 – ЗТЗ 72 – ОТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

1. К средствам защиты от ПЭМИ относятся?

А) Генераторы линейно-пространственного зашумления;+

Б) Генераторы НЧ;

В) Генераторы белого шума

Г) Генераторы «цветного» шума.

2. К средствам АВАК защиты относятся (выберите все возможные варианты)?
А) Генераторы АВАК сигналов;+
Б) Виброизлучатели;+
В) Пьезоизлучатели;
Г) «Глушилки».

3. Параметры антенных устройств (выберите все возможные варианты)?:
А) диаграмма направленности; +
Б) коэффициент усиления;+
В) сопротивление;
Г) напряжение.

4. Какой физический эффекты используют в электронных стетоскопах?:
А) твердотельный;
Б) воздушный;
В) пьезо-электрический;
Г) магнито-стрикционный.

5. ПЭМИ можно регистрировать с помощью? (выберите все возможные варианты):
А) спектрографа;+
Б) спектроанализатора;+
В) осцилографа;
Г) минивольтметра;
Д) селективного мультивольтметра+

6. К пассивным методам защиты от ПЭМИ относится (выберите неправильный ответ)?:
А) Экранирование;+
Б) Заземление; +
В) Заводнение;
Г) Генерирование шума.

7. Фильтры бывают (выберите все возможные варианты)?
А) Активными;+
Б) Пассивными; +
В) Полупассивными;
Г) Неактивными

8. Средство защиты от ПЭМИ имеет название?
А) «Гренада»;
Б) «Блокада»; +
В) «Турбо»;
Г) «Баррикада»

9. В состав «RS-turbo» входит?:
А) Анализатор спектра;
Б) Сканирующий приемник; +
В) Детектор слабого сигнала;
Г) Селективный микровольтметр.

10. «RS-turbo» в автоматизированном режиме определяет? (выберите все возможные варианты):
А) Опасные частоты;+
Б) Подозрительные частоты;+

В) Принципиально-опасные частоты;
Г) Спектральный частоты.

11. В состав лабораторной установки по измерению ПЭМИ входят (выберите все возможные варианты)?:
А) осциллограф;+
Б) вольтметр;
В) ПЭВМ;+
Г) антенная система;+
Д) ПО «Зебра»+

12. Название нелинейного локатора, используемого на ЛР?:
А) «Топаз»;
Б) «Бумеранг»;
В) «Катран»;+
Г) «Капкан».

13. Вычислите потенциальную частоту ПЭМИН видеоподсистемы ПЭВМ, которая рассчитывается по формуле:
Fтр=(x*y*w*m)/2
при следующих исходных данных:
x – число строк, x = 1024
y – число пикселей в строке, y = 768
w – частота кадров развертки, w = 60 Гц
m - учёт времени обратного хода луча кадров и строк, m=1.37

14. Какая из зон характеризует наводки информативного сигнала на ВТСС?:
А) 1;
Б) 2;
В) 3;
Г) 5.

15. Нелинейный локатор фиксирует излучения от:
А)t-c-p перехода;
Б) p-n-p перехода; +
В)r-n-b перехода;
Г) b-t-b перехода.

16. Подготовка к работе контрольно-измерительной аппаратуры включает?:
А) Калибровку; +
Б) Окантовку;
В) Упаковку.
Г) Оцифровку

17. Сколько зон используется для определения показателей защищенности объекта по каналу ПЭМИН?:
А) 1;
Б) 2;+
В) 3;
Г) 4;
Д) 5.

18. Для расчета ПЭМИ от ЭЛТ требуется?:
А) Разрешение экрана, частота излучения;

Б) Разрешение экрана, частота генератора;
В) Разрешение экрана, частота кадров;
Г) Частота развертки, разрешающая способность.

3.5 Типовые задания для выполнения курсового проекта и примерный перечень вопросов для его защиты

Типовые задания выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец задания для выполнения курсового проекта и примерный перечень вопросов для его защиты.

Образец типового задания для выполнения курсового проекта

1. Средства промышленного шпионажа.
2. Скрытие речевой информации в каналах связи.
3. Технические средства наблюдения и прослушивания двойного назначения.
4. Технический канал утечки видеоизображения за счет ПЭМИН.
5. Пассивные меры противодействия утечки информации по акустическому и виброакустическому каналу в защищаемом помещении.
6. Способы съема акустической (речевой) информации за пределами контролируемой зоны.
7. Анализ современных локаторов нелинейностей.
8. Анализ комплексов измерения ПЭМИН.
9. Анализ комплексов для измерения характеристик акустических сигналов.
10. Анализ многофункциональных комплектов для выявления каналов утечки информации.
11. Анализ комплексов радиомониторинга и выявления закладных устройств.
12. Устройства съема информации с волоконно-оптической линии связи.
13. Анализ средств пространственного электромагнитного зашумления.
14. Анализ средств виброакустического зашумления.
15. Параметрический канал утечки речевой информации. Способы выявления и защиты.
16. Оптико-электронный канал утечки речевой информации. Способы выявления и защиты.
17. Разработка системы защиты в кабинете руководителя.
18. Разработка системы защиты в организации.
19. Обзор средств негласного съема информации.
20. Мобильные средства и системы защиты информации.

Образец типовых вопросов для защиты курсовых проектов

1. Что такое демаскирующие признаки?
2. Демаскирующие признаки аналоговых сигналов?
3. Демаскирующие признаки цифровых сигналов?
4. Принцип работы направленного микрофона?
5. Принципы функционирования активных средств защиты информации?
6. Принципы функционирования пассивных средств защиты информации?
7. Различие между 2-ой и 3-ей гармоникой при поиске «закладок» с помощью «Катрана»?
8. Что такое модуляция?
9. Виды модуляции?
10. Принцип работы антенны «Альбатрос» при измерении ПЭМИН?
11. Возможности комплекса радиомониторинга «RS-turbo»?
12. Принцип работы обнаружителя скрытых видеокамер?
13. Возможности активных фильтров?
14. Способы применения сетевых помехоподавляющих пассивных фильтров низких и высоких частот?
15. Физическое обоснование возникновения вибрации в стенах помещения при разговоре людей?
16. Способы уменьшения уровня звукового давления и виброускороения?

3.6 Перечень теоретических вопросов к зачету

(для оценки знаний)

Раздел 4 «Методы, способы и средства технической защиты информации»

4.1 Скрытие речевой информации в каналах связи
4.2 Энергетическое скрытие акустических информативных сигналов
4.3 Скрытие речевой информации в каналах связи.
4.4 Способы и средства обнаружения закладных устройств
4.5 Классификация средств обнаружения и локализации закладных устройств
4.6 Средства обнаружения излучений закладных устройств
4.7 Сканирующие радиоприемники
4.8 Средства обнаружения неизлучающих закладок
4.9 Принцип действия нелинейного локатора.
4.10 Нелинейный локатор «Катран». Назначение, состав, основные характеристики, режимы работы.
4.11 Многофункциональные комплекты для выявления каналов утечки информации
4.12 Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М»
4.13 Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья»
4.14 Комплекс RS turbo
4.15. Радиотехнические системы передачи информации.
4.16. Радиолокационная система охраны периметра и территории объектов.
4.17. Классификация помех.
4.18. Естественные аддитивные помехи.
4.19. Искусственные аддитивные помехи.
4.20. Мультипликативные помехи.
4.21. Особенности частотных диапазонов.
4.22. Распространение радиоволн.
4.23. Диапазоны волн (частот).
4.24 Подавление опасных сигналов акустоэлектрических преобразователей телефонных линиях
4.25 Пассивные методы защиты от утечки информации по акустоэлектрическому каналу
4.26 Активные методы защиты от утечки информации по акустоэлектрическому каналу
4.27 Экранирование как пассивный способ защиты от утечек по техническим каналам
4.28 Заземление технических средств и подавление информационных сигналов в цепях заземления

Раздел 5 «Организация деятельности по технической защите информации»

5.1 Государственная система противодействия технической разведке. Структура и функции ГСПТР
5.2 Нормативные документы по противодействию технической разведке
5.3 Цели и задачи технического контроля эффективности мер защиты информации
5.4 Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ
5.5 Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации
5.6 Акустический и виброакустический контроль
5.7 Основное содержание мероприятий проводимых в ходе специальных проверок.
5.8 Основное содержание мероприятий проводимых в ходе специальных обследований.
5.9 Основное содержание мероприятий проводимых в ходе специальных исследований.

3.7 Перечень типовых простых практических заданий к зачету

(для оценки умений)

1. Какие основные меры безопасности могут помочь защитить информацию от угроз в реальном времени?

2. Что такое аутентификация и зачем она используется?
3. Какие методы аутентификации могут использоваться для проверки подлинности пользователя?
4. Что такое авторизация и почему она важна в контексте информационной безопасности?
5. Какие принципы безопасности помогают обеспечить аутентификацию и авторизацию пользователей?
6. Какой вид защиты информации является одним из видов инженерно-технической защиты?
7. Что такое информационная безопасность?
8. Какие основные принципы информационной безопасности существуют?
9. Что представляют собой объекты защиты информации?
10. Какие виды конфиденциальной информации выделяются в зависимости от области деятельности человека?
11. Какими свойствами обладает информация?
12. Какие объекты защиты информации существуют с точки зрения защиты?
13. Какие технические каналы могут использоваться для утечки информации?
14. Какие технические каналы относятся к несанкционированной передаче информации?
15. Какие основные задачи технической защиты информации?
16. Какие общие положения относятся к защите информации техническими средствам

3.8 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

1. Какие организации занимаются противодействием технической разведке?
2. Какие факторы могут влиять на эффективность технической разведки?
3. Как осуществляется оценка уровня угрозы технической разведки?
4. Какие методы сбора информации использует техническая разведка?
5. Какие последствия может иметь утечка конфиденциальной информации в результате технической разведки?
6. Какие меры безопасности могут быть применены для защиты от технической разведки?
7. Какой уровень секретности может быть использован при классификации технической разведки?
8. Какие источники разведывательной информации могут использоваться при классификации технической разведки?
9. По какой физической природе носителей информации может быть классифицирована техническая разведка?
10. Каковы основания классификации технической разведки по техническим характеристикам носителей информации?
11. Какова роль технической разведки в бизнесе?
12. Какие методы могут быть использованы при сборе информации с помощью технической разведки?
13. Какие типы информации могут быть получены с помощью технической разведки?
14. Какие факторы могут повысить эффективность технической разведки?
15. Что такое техническая разведка?
16. Какой вид разведки использует методы дистанционного зондирования Земли?
17. Какую роль играет техническая разведка в современном мире?
18. В рамках какого процесса техническая разведка может проводиться?
19. Какой вид разведки основан на использовании звуковых волн?
20. Какие методы и средства относятся к технической разведке?

3.9 Перечень теоретических вопросов к экзамену

(для оценки знаний)

Раздел 1 «Объекты информационной защиты»

1.1 Источники конфиденциальной информации в информационных системах.
1.2 Источники и носители информации в средствах вычислительной техники.
1.3 Сущность энтропийного подхода к оценке количества информации.
1.4 Количество информации по Шеннону.
1.5 Демаскирующие признаки (ДП). Технические демаскирующие признаки объекта. Основные понятия.
1.6 Классификация демаскирующих признаков.
1.7 Технические ДП.
1.8 Демаскирующие признаки объектов наблюдения.
1.9 Особенности видовых признаков в оптическом и радиодиапазонах. ДП объектов в ИК - диапазоне.
1.10 ДП объектов радиолокационного наблюдения.
1.11 Демаскирующие признаки аналоговых сигналов.
1.12 Демаскирующие признаки цифровых сигналов.

Раздел 2 «Технические каналы утечки информации»

2.1 Побочные электромагнитные излучения и наводки (ПЭМИН). Общие положения
2.2 Электромагнитные излучения систем СВТ
2.3 Классификация ТКУ И
2.4 ТКУ речевой информации
2.5 Краткие сведения по акустике
2.6 Звуковое давление
2.7 Акустические и электрические уровни
2.8 Акустические каналы
2.9 Направленные микрофоны
2.10 Проводные системы, портативные диктофоны и электронные стетоскопы
2.11 Виброакустические технические каналы утечки речевой информации
2.12 Акустоэлектрические каналы утечки речевой информации
2.13 Оптико-электронный технический канал утечки речевой информации
2.14 Параметрические технические каналы утечки речевой информации
2.15 ТКУ видовой информации
2.16 Каналы утечки информации при ее передаче по каналам связи

Раздел 3. «Способы и средства добывания информации техническими средствами»

3.1 Классификация технической разведки
3.2 Возможности видов технической разведки
3.3 Характеристики аппаратуры перехвата речевой информации
3.4 Характеристики аппаратуры перехвата видовой информации
3.5 Характеристики аппаратуры перехвата ПЭМИН
3.6 Классификация устройств съема информации с телефонной линии
3.7 Метод ВЧ навязывания (прослушивание помещений через микрофон телефонного аппарата)
3.8 Использование выносных микрофонов
3.9 Перехват сигналов сотовых телефонов.

3.10 Перечень типовых простых практических заданий к экзамену

(для оценки умений)

. Проведение измерений звукового давления с помощью ВШВ-003
2. Проведение измерений виброускорения с помощью ВШВ-003
3. Проведение измерений ПЭМИН ЭВМ с ЭЛТ
4. С помощью формулы рассчитать ПЭМИН видеоподсистемы

$$Fтр = \frac{x * y * w * m}{2}$$

x – число строк, x = 1024
y – число пикселей в строке, y = 768

w – частота кадров развертки, w = 60 ГГц
m - учёт времени обратного хода луча кадров и строк, m=1.37
5. Определение параметров дискретного и аналогового сигналов помощью осциллографа.
6. По осциллограмме, представленной на рис. 1, определить основные характеристики сигнала

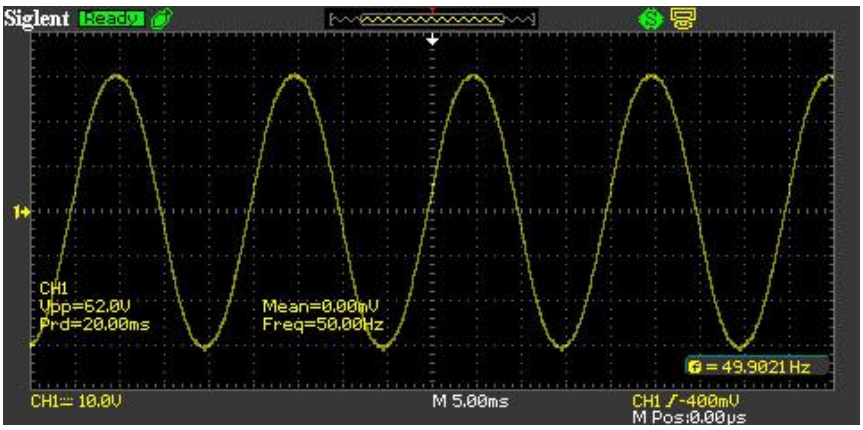

Рис. 1

7. Порядок настройки и подготовки к работе направленного микрофона «YUKON DSAS».

3.11 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

1. Анализ радиодиапазона и поиск закладных устройств с помощью «RS-turbo».
2. Подготовка, включение ПАК «RS-турбо» и настройка специализированного программного обеспечения на ПЭВМ (интерфейса комплекса)
3. Определение возможного местоположения закладного устройства
4. Порядок настройки и подготовки к работе нелинейного локатора «Катран».
5. Процесс обнаружения закладных устройств с помощью нелинейного локатора «Катран».
6. Поиск закладных устройств с помощью комплекса «Пиранья».

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Доклад	Защита докладов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему докладов и требования, предъявляемые к их выполнению и защите
Лабораторная работа	Защита лабораторных работ проводится во время лабораторных занятий. Во время проведения защиты лабораторной работы пользоваться учебниками, справочниками, конспектами лекций, тетрадями не разрешено. Преподаватель на лабораторной работе, предшествующей занятию проведения защиты лабораторной работы, доводит до обучающихся: номер защищаемой лабораторной работы, время на защиту лабораторной работы.

	Преподаватель информирует обучающихся о результатах защиты лабораторной работы сразу после ее контрольно-оценочного мероприятия
Курсовой проект	Ход выполнения разделов курсового проекта в рамках текущего контроля оценивается преподавателем исходя из объемов выполненных работ в соответствие со шкалами оценивания. Преподаватель информирует обучающихся о результатах оценивания выполнения курсового проекта сразу после контрольно-оценочного мероприятия. В ходе защиты курсового проекта обучающийся делает доклад протяженностью 5 – 7 минут. Преподаватель ставит окончательную оценку за курсовой проект после завершения защиты, учитывая уровень его защиты

Для организации и проведения промежуточной аттестации составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Перечень теоретических вопросов и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Шкала оценивания
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.

Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам или в форме компьютерного тестирования.

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к экзамену); другое практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике фондов оценочных средств.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.

Образец экзаменационного билета

<table>
<tr>
<td>ИРГУПС
2024-2025_
учебный год</td>
<td>Экзаменационный билет № 1
по дисциплине «<u>Защита информации от утечки по техническим каналам</u>»</td>
<td>Утверждаю:
Заведующий кафедрой
«ИСиЗИ» ИрГУПС
_____</td>
</tr>
<tr>
<td colspan="3">1. Классификация демаскирующих признаков
2. Направленные микрофоны.
3.Анализ радиодиапазона с помощью «RS-turbo».
4. Определение возможного местоположения закладного устройства</td>
</tr>
</table>