МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра математики и физики

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ Е.И. Луковникова
«_____» декабря 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Б1.В.14

НАПРАВЛЕНИЕ ПОДГОТОВКИ

01.03.02 Прикладная математика и информатика

ПРОФИЛЬ ПОДГОТОВКИ

Инженерия программного обеспечения

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

СОДЕРЖАНИЕ ПРОГРАММЫ **Стр.**

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Вид деятельности выпускника

Дисциплина Б1.В.14 «Технические средства и методы защиты информации» охватывает круг вопросов, относящихся к проектному, организационно-управленческому, производственно-технологическому виду профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Формирование у студентов знаний по основам инженерно-технической защиты информации, а также выработка навыков и умений в применении полученных знаний в условиях работы на конкретных объектах информационной безопасности.

Задачи дисциплины

Задачами изучения дисциплины являются:

- изучение технических средств добывания информации;
- назначения и функций видов разведки;
- способов доступа к источникам конфиденциальной информации без проникновения на объект защиты;
- способов и средств защиты конфиденциальной информации техническими средствами

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	**знать:** − информацию о современных разработках в области своей профессиональной деятельности и решаемых задачах, их позитивной значимости и возможности их негативных последствий. **уметь:** − сформировать и дать обоснованные суждения о значении и последствиях своей профессиональной деятельности, сформулировать обоснование актуальности и значимости результатов решаемых задач профессиональной деятельности с учетом социальных, профессиональных и этических позиций. **владеть:** − навыками формирования суждения о значении и последствиях своей профессиональной деятельности, формулировки актуальности и значимости результатов решаемых задач профессиональной деятельности с учетом социальных, профессиональных и этических позиций.
ПК-7	Способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	**знать:** − технические каналы утечки информации; − возможности технических разведок; − способы и средства защиты информации от утечки по техническим каналам; − методы и средства контроля эффективности технической защиты информации. **уметь:** − анализировать и оценивать угрозы информаци-

		онной безопасности объекта; **владеть:** − методами технической защиты информации; − методами формирования требований по защите информации; − методами расчета и инструментального контроля показателей технической защиты информации.
ПК-8	Способность приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности	**знать:** − организационно-управленческие навыки в профессиональной и социальной деятельности **уметь:** − приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности **владеть:** - способностью приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.14 Технические средства и методы защиты информации относится к вариативным дисциплинам.

Дисциплина Технические средства и методы защиты информации базируется на знаниях, полученных при изучении таких учебных дисциплин, как: Программные средства защиты информации, Теоретические основы защиты информации, Методы обеспечения безопасности компьютерных систем.

Основываясь на изучении перечисленных дисциплин, «Технические средства и методы защиты информации» представляет основу для преддипломной практики и подготовки к государственной итоговой аттестации.

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	***Курс***	***Семестр***	***Трудоемкость дисциплины в часах***						***Курсовая работа (проект), контрольная работа, реферат, РГР***	***Вид промежуточной аттестации***
			Всего часов (с экз.)	***Аудиторных часов***	***Лекции***	***Лабораторные работы***	***Семинары Практические занятия***	***Самостоятельная работа***		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Очная	4	8	144	72	24	48	-	18	-	Экзамен
Заочная	-	-	-	-	-	-	-	-	-	-
Заочная (ускоренное обучение)	-	-	-	-	-	-	-	-	-	-
Очно-заочная	-	-	-	-	-	-	-	-	-	-

3.2. Распределение объема дисциплины по видам учебных занятий и трудоемкости

Вид учебных занятий	*Трудоемкость (час.)*	*в т.ч. в интерактивной, активной, инновационной формах, (час.)*	*Распределение по семестрам, час*
			7
1	**2**	**3**	**4**
I. Контактная работа обучающихся с преподавателем (всего)	72	36	72
Лекции (Лк)	24	6	24
Лабораторные работы (ЛР)	48	48	48
II.Самостоятельная работа обучающихся (СР)	18	-	18
Подготовка к лабораторным работам	12	-	12
Подготовка к экзамену	6	-	6
III. Промежуточная аттестация экзамен	54		54
Общая трудоемкость дисциплины час.	144	-	144
зач. ед.	4	-	4

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий
- для очной формы обучения:

№ раздела и темы	*Наименование раздела и тема дисциплины*	*Трудоемкость, (час.)*	*Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)*		
			учебные занятия		*самостоятельная работа обучающихся**
			лекции	*лабораторные работы*	
1	**2**	**3**	**4**	**5**	**6**
1.	**Основы технических средств и методов защиты информации**	**90**	**24**	**48**	**18**
1.1.	Концепции инженерно-технической защиты информации	9	2	4	3
1.2.	Теоретические основы инженерно-технической защиты информации	21	6	12	3
1.3	Физические основы защиты информации	15	4	8	3
1.4	Технические средства добывания и инженерно-технической защиты	15	4	8	3
1.5	Организационные основы инженерно-технической защиты информации	15	4	8	3

1.6	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	15	4	8	3
	ИТОГО	**90**	**24**	**48**	**18**

4.2. Содержание дисциплины, структурированное по разделам и темам

№ разделаи темы	***Наименование раздела и темы дисциплины***	***Содержание лекционных занятий***	***Вид занятия в интерактивной, активной, инновационной формах, (час.)***
1	**2**	**3**	**4**
1.	**Основы технических средств и методов защиты информации**		
1.1	Концепции инженерно-технической защиты информации	Системный подход к защите информации. Основные проблемы инженерно-технической защиты информации. Основные концептуальные положения инженерно-технической защиты информации. Направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.	-
1.2	Теоретические основы инженерно-технической защиты информации	Информация как предмет защиты. Свойства информации, влияющие на ее безопасность. Демаскирующие признаки. Источники опасных сигналов. Виды побочных опасных электромагнитных излучений. Характеристика технической разведки. Технические каналы утечки информации. Методы инженерно-технической защиты информации. Методы инженерной защиты и технической охраны объекта. Методы скрытия информации и ее носителей.	Лекция-беседа (2 час.)
1.3	Физические основы защиты информации	Физические основы побочных электромагнитных излучений и наводок. Распространение сигналов в технических каналах утечки информации. Физические процессы подавления опасных сигналов. Паразитные связи.	Лекция-беседа (2 час.)
1.4	Технические средства добывания и инженерно-технической защиты	Средства технической разведки. Средства инженерной защиты и технической охраны. Средства предотвращения утечки информации по техническим каналам.	Лекция-беседа (2 час.)
1.5	Организацион-	Государственная система защиты ин-	-

	ные основы инженерно-технической защиты информации	формации. Контроль эффективности инженерно-технической защиты информации. Протоколы оценки защищенности.	
1.6	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	Моделирование инженерно-технической защиты информации. Методические рекомендации по оценке эффективности защиты информации.	-

4.3. Лабораторные работы

№ п/п	*Номер раздела дисциплины*	*Наименование лабораторной работы*	*Объем (час.)*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1.	**1.**	1. Техническая реализация маскировки средств вычислительной техники	2	Работа в малых группах (2 часа)
2.		2. Статистический анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещение	2	Работа в малых группах (2 часа)
3.		3. Обнаружение сигналов линейных и сетевых закладок	4	Работа в малых группах (4 часа)
4.		4. Обнаружение оптических сигналов передатчиков ИК - диапазона	4	Работа в малых группах (4 часа)
5.		5. Локатор нелинейностей	4	Работа в малых группах (4 часа)
6.		6. Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля	4	Работа в малых группах (4 часа)
7.		7. Программно-аппаратный комплекс «СПРУТ-7»	6	Работа в малых группах (6 часов)
8.		8. Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу комплексом «СПРУТ-7»	10	Работа в малых группах (10 часов)
9.		9. Сетевые помехоподавляющие	2	Работа в малых

		пассивные фильтры низких и высоких частот		группах (2 часа)
10.		10. Сетевые пассивные полосно-заграждающие и полосно-пропускающие фильтры	2	Работа в малых группах (2 часа)
11.		11. Активные фильтры низких и высоких частот	4	Работа в малых группах (4 часа)
12.		12. Расчет паразитных связей через посторонний провод	4	Работа в малых группах (4 часа)
		ИТОГО	**48**	**48**

4.4. Практические занятия

Учебным планом не предусмотрено.

4.5 Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат

Учебным планом не предусмотрено.

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Компетенции / *№, наименование разделов дисциплины*	*Кол-во часов*	*Компетенции*			*Σ комп.*	$t_{ср}$, *час*	*Вид учебных занятий*	*Оценка результатов*
		ПК						
		6	*7*	*8*				
1	2	3	4	5	6	7	8	9
1. Основы технических средств и методов защиты информации	144	+	+	+	3	48	Лк, ЛР	экзамен
всего часов	**144**	**48**	**48**	**48**	**3**	**48**		

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Зайцев А.П., Шелупанов А.А. Сборник лабораторных работ по техническим средствам и методам защиты информации. Учебное пособие.- Томск.: В-Спектр, 2010. - 228 с.

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	*Наименование издания*	*Вид занятия* (*Лк, ЛР, кр*)	*Количество экземпляров в библиотеке,* шт.	*Обеспеченность,* (экз./ чел.)
1	2	3	4	5
Основная литература				
1.	Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информ-вционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689	Лк, ЛР, кр	1 (ЭУ)	1
2.	Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092	Лк, ЛР, кр	1 (ЭУ)	1
Дополнительная литература				
3.	Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605	Лк, ЛР, кр	1 (ЭУ)	1

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе обучения студенты могут использовать общие ресурсы:

1.Электронный каталог библиотеки БрГУ
http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.

2. Электронная библиотека БрГУ
http://ecat.brstu.ru/catalog .

3. Электронно-библиотечная система «Университетская библиотека online»
http://biblioclub.ru .

4. Электронно-библиотечная система «Издательство «Лань»
http://e.lanbook.com .

5. Информационная система "Единое окно доступа к образовательным ресурсам"
http://window.edu.ru .

6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru .

7. Университетская информационная система РОССИЯ (УИС РОССИЯ)
https://uisrussia.msu.ru/ .

8. Национальная электронная библиотека НЭБ
http://xn--90ax2c.xn--p1ai/how-to-search /.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Обучающийся должен разработать собственный режим равномерного освоения дисциплины. Подготовка студента к предстоящей лекции включает в себя ряд важных познавательно-практических этапов:

– чтение записей, сделанных в процессе слушания и конспектирования предыдущей лекции, вынесение на поля всего, что требуется при дальнейшей работе с конспектом и учебником;

– техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);

– выполнение заданий преподавателя;

– знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе.

Успешность выполнения лабораторных работ определяется подготовкой к ним. Подготовка к лабораторным работами содержит

- изучение теоретического материала, содержащегося в учебной литературе, изучение лекционного материала;

- знакомство с заданиями на лабораторную работу;

- составление плана выполнения лабораторной работы.

Наиболее продуктивной является самостоятельная работа в библиотеке, где доступны основные и дополнительные печатные и электронные источники.

При выполнении приведенных выше рекомендаций подготовка к зачету сведется к повторению изученного и совершенствованию навыков применения теоретических положений и различных методов решения к стандартным и нестандартным заданиям.

9.1. Методические указания для обучающихся по выполнению лабораторных работ

Лабораторная работа №1 Техническая реализация маскировки средств вычислительной техники

Цель работы: Изучить методы маскировки информационных излучений средств вычислительной техники.

Задание: Провести установку генератора шума ГШК-1000 Оценить эффективность маскировки электромагнитных излучений

Порядок выполнения: Первая часть работы производится с применением генератора шума ГЩК-1000 , установленного в свободный слот персонального компьютера , и компьютеризированного комплекса RS turbo Mobile-L Для этого:

1. Снять частотную панораму в помещении с помощью комплекса RS turbo Mobile-L при выключенном генераторе шума
2. Снять частотную панораму при выключенном генераторе шума
3. Путем сравнения частотных панорам оценить эффективность маскировки электромагнитных излучений персонального компьютера и других находящихся в помещении электронных устройств с помощью генератора шума Вторая часть работы проводится с демонстрацией действий устройств ГРОМ-ЗИ-4 и УК-300.
4. Поочередно включить каждое из устройств и делаются попытаться установить и делать попытки установить связь с любым абонентом по сотовому телефону.
5. Для наблюдения сигналов зашумления использовать комплекс RS turbo Mobile-L. Составить отчет с описанием способов маскировки электромагнитных излучений средств вычислительной техники и устройств ГРОМ-ЗИ-4 и УК-300 и ответить на контрольные вопросы.

Форма отчетности:

Наименование лабораторной работы;

Разработанная программа;

Результаты тестирования;

Выводы по работе;

Задания для самостоятельной работы:

1.Псотроить графики, полученные при помощи генератора шума и сравнить их.

2. Установить сеанс сотовой связи и устранить шумовое загрязнение эфира.

Рекомендации по выполнению:

1. Ознакомиться с заданием
2. Изучить теоретические сведения полученные на лекции
3. Ознакомиться с примерами решение подробных задач в учебной литературе
4. Разработать и написать программу

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки:

1. Какие элементы компьютерной системы создают ПЭМИ, позволяющие восстановить конфиденциальную информацию?
2. Можно ли восстановить первичную информацию из ПЭМИ ,создаваемыми устройствами обработки параллельного кода ?
3. В чем заключаются достоинства и недостатки экранирования помещений для локализации ПЭМИ?
4. В чем заключается принцип маскировки информационных излучений средств электронной техники?

Лабораторная работа №2 Статистический анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещение

Цель работы

Изучить методы статистического анализа заданного радиодиапазона и обнаружения радиомикрофонных закладок с помощью компьютеризированных комплексов RS turbo, RS turbo Mobile-L.

Задание для работы

1. Ознакомиться с видами радиозакладок и изучить методы их обнаружения.
2. Изучить работу комплексов в режиме обнаружения радиозакладок.
3. Произвести настройку программы для работы в режиме «Радио».
4. Выполнить один или несколько циклов сканирования заданного радиодиапазона.
5. Обнаружить излучения без учета априорных данных за один цикл сканирования.
6. Посмотреть и проанализировать списки обнаруженных сигналов.

   Для интересующего сигнала выполнить:

- спектральный анализ сигналов излучений;
- анализ гармонического состава сигналов излучений;
- корреляционный анализ откликов на акустические импульсы.

7. Выявить наличие радиозакладного устройства в контролируемом помещении.

Порядок выполнения работы

Создать отдельное задание с несколькими операциями сканирования радиодиапазона. Для этого в меню «Настройки» выбрать «Установка параметров». В окне «Настройка программы» щелкнуть на закладку «Задание» (рис. 3). Выбрать режим «Радио».

В окне «Диапазон» установить диапазон сканирования частот от 10 до 1000 МГц, желаемое число циклов сканирования и заданный порог 50 при выключенном аттенюаторе. Щелкнуть по кнопке ОК (закрыть окно).

Запустить сканирование нажатием кнопки «Старт». Провести простое сравнение по масштабной сетке окна спектральной панорамы составляющих измеренного с разрешением 12,5 кГц спектра сигнала с указанным в задании порогом.

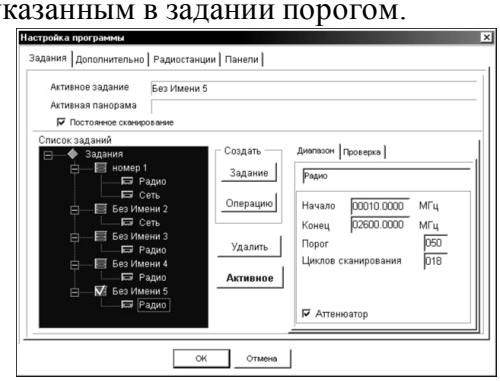


Рис. 3. Окно «Настройка программы»

Зафиксировать уровень сигналов, превышающих заданный порог. Программа запоминает частоту и уровень сигналов излучений. Данные о частоте и уровне сигналов, обнаруженных с помощью входящего в состав комплекса конвертора RS/L plus, заносятся в список сигналов. В центре окна монитора размещается экран панорамного отображения спектров. Вертикальная ось экрана панорамного отображения спектров отражает интенсивность принимаемого сигнала в децибелах относительно уровня шума приемника.

Горизонтальная ось соответствует частоте диапазона сканирования. Над экраном панорамы спектра находятся закладки «Радио», «Сеть» и «Панорама» (рис. 4).

Закладка «Радио» позволяет наблюдать процесс сканирования радио-диапазонов и текущие спектральные панорамы, полученные после выполнения заданных циклов сканирования, а закладка «Панорама» используется для просмотра файлов спектральных панорам.

Отображение спектральной панорамы в закладках «Радио» и «Панорама» ведется с разрешением 200 кГц. Линейка горизонтальной прокрутки закладках «Радио» и «Панорама» позволяет просматривать весь рабочий диапазон сканера участками по 10, 100, 500 или 1000 МГц в зависимости от выбранного масштаба отображения по оси частот (полосы обзора).

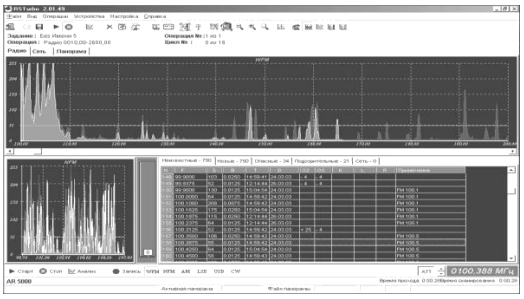


Рис. 4. Окно панорамного отображения спектров

Ниже окна спектральной панорамы (при выборе закладок «Радио » или «Панорама») помещается окно детального анализа спектра с полосой обзора, которая автоматически изменяется в процессе сканирования в зависимости от ширины спектра обнаруженного сигнала. Это окно отображает текущие спектры излучений с разрешением 12,5 кГц. Справа находится вертикальный (столбцовый) индикатор уровня принимаемого сигнала с дополнительной цифровой индикацией и окно списков обнаруженных частот. Кнопки «Старт» и «Стоп» в нижней части экрана запускают и останавливают процесс сканирования, а кнопка «Анализ» вызывает окно для выполнения операций идентификации и классификации излучений на выделен-ной в списке частоте. Рядом с кнопкой «Анализ» находятся кнопки выбора типа демодулятора сканера и управления аттенюатором , а также индикатор частоты настройки приемника с кнопками пошагового изменения частоты настройки сканера нижней части основного окна находятся две строки состояний первой отражается тип сканера, с которым работает комплекс, и время, затраченное на выполнение текущей операции сканирования. Во второй строке появляются поясняющие сообщения о функциях кнопок окна, а также имена файлов спектральной панорамы, которые используются в качестве диаграммы загрузки диа-

пазона при классификации сигналов (Активная панорама) и загружены для просмотра в закладке «Панорама» (Файл панорамы).

Форма отчетности:

Наименование лабораторной работы;

Результаты тестирования;

Выводы по работе.

Задания для самостоятельной работы:

1. Настроить приемник на выбранную частоту и выполнить анализ радиоизлучения. Настраивать приемник удобно с учетом полученных данных о радиообстановке. Текущая частота настройки приемника в основном окне программы отражается цифровым индикатором и положением курсоров в окнах спектральной панорамы.

Для изменения частоты настройки откройте закладку «Радио», установите в окне спектральной панорамы удобный масштаб отображения по оси частот (полосу обзора) и найдите интересующий участок спектра с помощью линейки прокрутки. Щелчок мыши в интересующей области диапазона переместит курсор и настроит приемник на ближайшую частоту из 200-кГц сетки. Одновременно программа включает широкую полосу про-пускания приемника (WFM). Точная настройка выполняется мышью в нижнем окне детального анализа спектра с шагом 12,5 кГц. При этом приемник переключается в узкополосный режим NFM. Для перестройки частоты на несколько шагов можно воспользоваться кнопками увеличить/уменьшить слева от индикатора частоты. Если включена (нажата) кнопка WFM, щелчок по кнопкам увеличить/уменьшить переместит курсор верхнем окне спектральной панорамы соответственно вправо или влево и перестроит приемник на 200 кГц. Если нажата кнопка NFM, двигаться бу-дет курсор нижнего окна спектральной панорамы и шаг перестройки составит 12,5 кГц. Кроме того, произвольное значение частоты настройки можно ввести с клавиатуры, щелкнув левой кнопкой мыши по индикатору часто-ты настройки основного окна.

2. Провести анализ подозрительных и опасных радиоизлучений.

Задании предусмотрено сканирование заданного диапазона с анализом гармонического состава обнаруженных излучений (обнаружение 2-й гармоники, обнаружение 3-й гармоники, одновременное обнаружение 2-й и 3-й гармоник). Программа, обнаружив сигнал и измерив его несущую частоту f, настраивает приемник на частоту $2f$ и/или $3f$, измеряет уровни гармоник при максимальной чувствительности (отключив аттенюатор) и сравнивает их с пороговым значением. В случае превышения порога про-грамма принимает решение о наличии излучения на гармониках основной частоты и в списках обнаруженных сигналов в графах гармоник (G2 и G3) указывается измеренный уровень с пометкой «+». Если гармоника не обнаружена – уровень указывается с пометкой «–».

Если проверка не выполнялась, например, из-за того, что частота гармоники лежит вне рабочего диапазона сканера, – графа остается пустой. Обнаружив одну из гармоник, программа помещает данные о сигнале в список «подозрительных» излучений. Если обнаружены обе гармоники – в список «опасных» сигналов процессе сканирования радиодиапазонов на экране панорамного об-зора будут отображаться 100-МГц участки с разрешением 200 кГц, а на эк-ране детального анализа – спектр последнего обнаруженного сигнала (сигналов) с разрешением 12,5 кГц. Кроме того, программа в соответствии с заданием выполняет операции автоматической классификации и идентификации обнаруженных источников излучений. При сканировании радио-диапазонов в системе «RSturbo» можно использовать любую комбинацию из перечисленных ниже методов идентификации и классификации сигналов.

3. Провести классификацию сигналов на «известные» и «неизвестные» с использованием диаграмм загрузки радиодиапазона. Диаграммы загрузки характеризуют внешние и внутренние излучения при продолжительных наблюдениях со статистической обработкой результатов измерений. Обнаружение излучений без учета априорных данных позволяет выявить и за-нести в список все без исключения источники, мощность которых в точке приема больше заданной. Однако полученный список обнаруженных сигналов в большинстве случаев оказывается слишком обширным. Необходимо сократить его, исключив те излучения, которые были обнаружены ранее, проверены и признаны не представляющими опасность. После необходимой проверки источники этих излучений можно считать «известными» в том смысле, что они регулярно присутствуют в эфире и не представляют опасности для контро-

лируемого объекта. Классификация сигналов на «известные» и «неизвестные» позволяет оставить в списке обнаруженных излучений только те, которые не содержатся в диаграмме загрузки.

Рекомендации по выполнению:

1. Если обнаружение планируется выполнять с классификацией излучений на «известные» и «неизвестные», необходимо использовать нужный файл диаграммы загрузки. Алгоритм обнаружения и классификации вы-глядит следующим образом. Выделив в цикле сканирования участок группы смежных частот, превышающих порог обнаружения, и определив максимальные уровни в каждой из них, программа проверяет, попадает ли текущий максимум каждой группы в одну из полос «известного» излучения, присутствующего в диаграмме. Полоса известного излучения определяется числом уровней в группе частот, превышающих порог обнаружения (рис. 5). Если ответ положительный, программа считает излучение известным. В противном случае принимается решение об обнаружении «неизвестного» излучения, данные о кото-ром заносятся в список «неизвестных» излучений с учетом результатов обнаружения на предыдущих циклах сканирования.

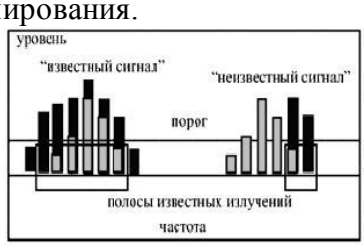


Рис. 5. Классификация сигналов на «известные» и «неизвестные»

Провести классификацию сигналов на «вновь появившиеся» и «обнаруженные ранее» на предыдущих циклах сканирования с использованием текущей спектральной панорамы.

2. Если в задании предписано выполнение нескольких циклов сканирования или панорама спектра предыдущего сеанса работы была сохранена, обнаружение выполняется следующим образом. Выделив в каждом цикле сканирования участка группы смежных частот, превышающих порог обнаружения, и определив максимальные уровни в каждой из них, программа проверяет, попадает ли текущий максимум каждой группы в полосу одного из сигналов, обнаруженных на предыдущем цикле сканирования (рис. 6).

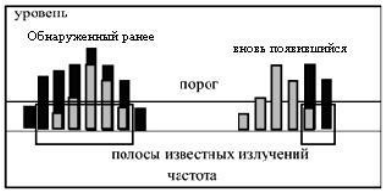


Рис. 6. Классификация сигналов на «обнаруженные ранее» и «вновь появившиеся»

Полоса излучения, обнаруженного на предыдущем цикле сканирования, определяется числом уровней в группе частот, превышающих порог. Если ответ отрицательный, то принимается решение об обнаружении «нового» излучения, данные о котором заносятся в списки. В противном случае программа считает излучение уже обнаруженным. В результате размер списков обнаруженных сигналов существенно сокращается. Кроме того, отдельный список «новых» излучений значительно упрощает контроль текущих изменений радиообстановки. Действительно, если очистить список «новых» излучений, то в последующих циклах сканирования в него будут попадать только вновь обнаруженные сигналы. Остальную информацию можно найти в списке «неизвестных» излучений , который содержит все сигналы, обнаруженные с момента последней очистки спектральной панорамы.

3. Провести акустическое зондирование. Кнопкой «Анализ» или ко-мандой «Анализ меню Операции» вызвать окно анализа обнаруженных сигналов, в названии которого указывается частота анализируемого сигнала. В этом окне выбирается закладка «Звуковой тест». В верхней части за-кладки отображается реверберационная картина помещения, для просмотра которой можно воспользоваться линейкой прокрутки (рис. 7).

Измерить расстояние от звуковой колонки до некоторой точки, напри-мер, одного из импульсов, можно, указав на него курсором мыши. При этом значение расстояния в метрах отображается в правом верхнем углу экрана реверберационной картины. В нижней части за-

кладки отображается корреляционная функция отклика, расстояния от звуковых колонок до микрофона и значение коэффициента корреляции. Чтобы выполнить акустический тест, необходимо из нужного списка выбрать интересующий сигнал, установить полосу приема (NFM или WFM), указать число циклов (импульсов) звукового зондирования и нажать кнопку с изображением левой или правой колонки. При повторном выполнении теста предыдущая рверберационная картина стирается. Закончив анализ, щелкните по кнопке «Выход».

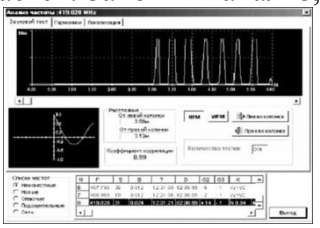


Рис. 7. Окно звукового зондирования

Провести акустическое зондирование в автоматическом режиме. Если в задании предусмотрено сканирование с идентификацией радиомикрофонов методом акустического зондирования, программа, обнаружив сигнал и измерив его несущую частоту и ширину спектра, выполняет на несущей частоте акустический тест, включив узкую полосу пропускания (режим NFM).

Звуковые импульсы, число которых задается при настройке, излучаются левой колонкой акустической системы. После этого вычисляется коэффициент корреляции отклика и сравнивается с порогом, величина которого составляет 0,6. Если порог превышен, программа принимает решение об идентификации сигнала радиомикрофона. Для повышения скорости работы в автоматическом режиме звуковой тест выполняется с высокой частотой повторения акустических импульсов. Полученные результаты (коэффициент корреляции, полоса пропускания, расстояния от радиомикрофона до колонок акустической системы) за-носятся в список «опасных» излучений. Если при тестировании через первую колонку порог не превышается, программа повторяет тест с помощью второй колонки, а затем – в широкой полосе пропускания приемника (ре-жим WFM). Если и в этом случае результаты звукового теста отрицательны, в списки «неизвестных» и «новых» излучений заносятся только значения коэффициента корреляции. При высокой частоте повторения акустических импульсов из-за реверберации измерение расстояний от колонок до радиомикрофона иногда выполняется с ошибками. Уточнить расстояния можно, выполняя акустический тест в ручном режиме.

4. Провести анализ излучений методом акустического зондирования

1. Ручном режиме. В ручном режиме оператор имеет возможность выполнять акустический тест отдельно для левой и правой колонок, наблюдать реверберационные картины помещения, корреляционную функцию отклика, выбирать число звуковых импульсов, переключать полосу пропускания приемника (NFM, WFM). Для проведения акустического теста необходимо настроить приемник на несущую частоту интересующего излучения, выбрав нужную запись из списка обнаруженных сигналов или указав значения частоты с клавиатуры, указать полосу пропускания, число зондирующих импульсов и нажать кнопку левой или правой колонки. В ручном режиме программа снижает частоту повторения акустических импульсов для того, чтобы избежать реверберационых помех и повысить достоверность измерений дальности. Окно реверберационной картины помещения отображает интенсивность принятого импульсного сигнала в зависимости от времени, которое пересчитано в расстояние. Вертикальная шкала градуируется в относительных единицах, а горизонтальная – в метрах. Линейка прокрутки окна позволяет наблюдать отклики на дистанциях до 30 м.

Пользователь может также измерить расстояние до любого импульса, указав на него курсором. Автокорреляционная функция отклика, отражающая зависимость коэффициента корреляции от времени служит дополнительным инструментом, облегчающим процесс идентификации сигналов сомнительных случаях.

На рис. 8 изображены корреляционные функции откликов для радио-микрофона и внешней станции. Как известно, форма корреляционной функции одиночного импульса близка к треугольной. Присутствие не-скольких отраженных импульсов в отклике вызывает появление боковых выбросов корреляционной функции той же формы.

Акустическое зондирование позволяет автоматически идентифицировать излучения только тех подслушивающих устройств, в которых используется стандартная узкополосная или широкополосная частотная модуляция. Если обнаружен сигнал с иными параметрами модуляции или цифровым кодированием (с поднесущими, с инверсией спектра, цифровой модуляцией и т. д.), значение коэффициента корреляции обычно не достигает порогового уровня . Вместе с тем оператор может идентифицировать такой сигнал, повторив операцию акустического зондирования несколько раз . В этом случае коэффициент корреляции будет небольшим (от 0,2 до 0,4 в зависимости от типа устройства), но относительно стабильным, тогда как для внешних станций его значение случайно изменяется в пределах от - 0,3 до +0,3. Сказанное не относится к микропередатчикам с цифровой модуляцией, в которых применяются специальные методы декорреляции акустического и модулирующего сигналов (скремблирование цифрового потока).

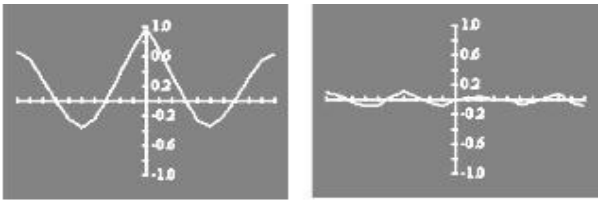


Рис. 8. Корреляционные функции откликов: *а* – для радиомикрофона;
2. б– для внешней станции

Провести анализ спектра. Анализатор спектра вызывается инструментальной кнопкой основного окна программы или командой «Спектр меню Операции». Полоса обзора анализатора отсчитывается вверх и вниз относительно центральной частоты. Значение полосы обзора соответствует ширине тракта ПЧ приемника – 8 МГц. Значение центральной частоты устанавливается программой при выделении записи в одном из списков обнаруженных сигналов или вводится оператором. В верхней части окна находятся позиции выбора состояния аттенюатора и полосы анализа (12,5 кГц или 200 кГц). После ввода этих параметров необходимо щелкнуть мышью по кнопке «Установить».

В нижней части окна находится выпадающий список выбора режима обработки спектральных составляющих в последовательных циклах обзора. В режиме обновления текущее значение заменяет предшествующее, в режиме накопления выбирается максимальное из этих двух значений, а в режиме усреднения – среднее. Щелчок по кнопке «Старт» включает циклический режим анализа спектра в заданной полосе обзора. Спектральные составляющие текущего цикла обзора отражаются зеленым цветом, предыдущего – красным (рис. 9).

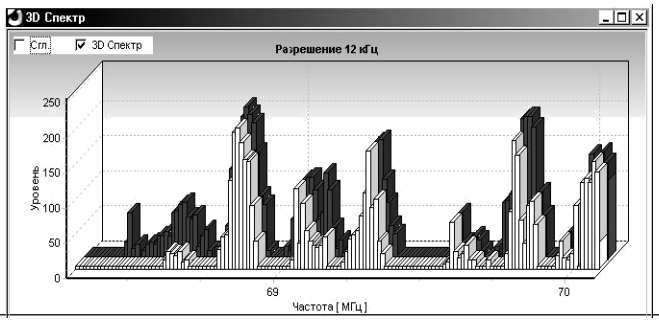


Рис. 9. Диаграмма спектра

Отмечая позиции «Сглаживание» и «3D» вид спектра можно изменять

3. В процессе анализа. Остановить анализ можно кнопкой «Стоп». При этом картина спектра запоминается. После остановки процесса анализа можно измерять частоты и уровни спектральных составляющих, поместив курсор мыши в нужную область экрана отображения спектра. Координаты курсора, соответствующие частоте и измеренному уровню спектральной составляющей отображаются в правой части окна ниже индикатора частоты.

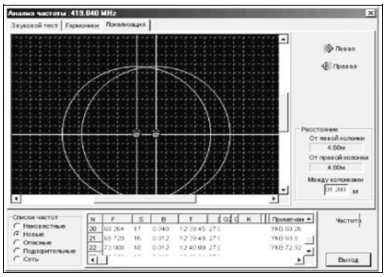


Рис. 10. Локализация радиомикрофона

Не выходя из окна спектроанализатора, можно анализировать сигналы на выходе демодулятора сканера. Подведите курсор к интересующей спектральной составляющей и щелкните левой кнопкой мыши. Сканер настроится на нужную частоту, которая отображается индикатором окна спектроанализатора. Теперь сигнал на выходе демодулятора можно прослушать или вывести на экран программы -осциллографа. Полоса пропускания сканера выбирается из выпадающего списка «Полоса анализа». Для выхода из окна анализатора спектра достаточно щелкнуть по кнопке «Выход».

Провести локализацию радиомикрофона. Для этого щелкнуть по кнопке «Анализ». В появившемся окне активизировать закладку «Локализация» и выбрать частоту обнаруженного опасного сигнала.

На экране окна появится графическая картина в виде двух пересекающихся окружностей (рис. 10). Одна из точек пересечения окружностей будет соответствовать местоположению радиомикрофона.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. Приведите определение закладочного устройства.
2. Перечислите демаскирующие признаки автономных некамуфлированных акустических закладок.
3. Перечислите демаскирующие признаки полуактивных акустических радиозакладок.
4. Какие технические средства применяют для выявления радиозакладочных устройств?
5. Назначение комплекса «RS turbo Mobile-L».
6. Перечислите состав комплекса «RS turbo Mobile-«L.
7. Радиозакладки с каким видом модуляции обнаруживает комплекс RS turbo?
8. Назовите базовую операцию в комплексе «RS turbo», предшествующую обнаружению и идентификации источников излучений.
9. Как на следующем цикле сканирования формируется новая (текущая) таблица и модифицируются значения уровней в таблице предыдущей панорамы в соответствии с выбранным методом обработки?
10. С помощью каких операций выполняется автоматически или в ручном режиме идентификация (опознавание) сигналов подслушивающих устройств в программе «RS turbo»?

Лабораторная работа №3 Обнаружение сигналов линейных и сетевых закладок

Цель работы: Изучить методы обнаружения сетевых и линейных закладок с помощью комплексов «RS turbo», «RS turbo Mobile-L».

Задание:

1. Изучить способы внедрения сетевых и линейных закладок.
2. Изучить принцип действия и порядок работы комплекса «RS turboMobile-L» на выявление сетевых и линейных закладок.
3. Выявить наличие скрытно установленного выносного микрофона с питанием от телефонной линии связи.
4. Выявить наличие выносного скрытно установленного микрофона с питанием от линии сети электропитания.

Порядок выполнения:

1. Создать отдельное задание с одной или несколькими операциями сканирования сети.
2. В меню «Настройки» выбрать «Установка параметров». В окне «Настройка программы» щелкнуть на закладку «Задание» (рис 1).

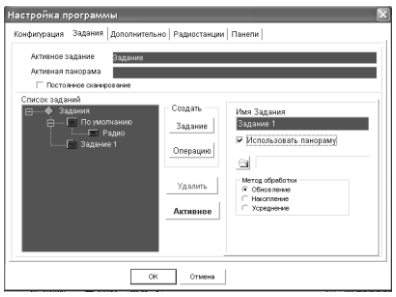


Рис. 1. Окно «Настройка программы»

3. Настроить параметры программы.

В закладке «Настройка программы» ввести дополнительные параметры настройки программы: принимаемый по умолчанию метод сортировки списков обнаруженных сигналов, способ оповещения о занесении в список сигнала, идентифицированного методом акустического зондирования, а также частоту преобразования конвертера RS/L. Метод сортировки определяет порядок размещения записей в списках частот обнаруженных сигналов: по возрастанию несущей частоты, максимального уровня, времени, даты обнаружения и ширине спектра обнаруженного сигнала. В данной работе выбрать метод сортировки списков обнаруженных сигналов по возрастанию несущей частоты. Выбранный в закладке метод сортировки запоминается и используется по умолчанию при каждом запуске программы. Его можно оперативно изменить, вызвав инструментальной кнопкой или командой «Сортировка меню – Вид – Окно – Сортировка списков» в основном окне программы. При следующем запуске программы расположение записей в списках будет соответствовать позиции, отмеченной в разделе «Сортировка списков» закладки«Дополнительно»(рис.2).

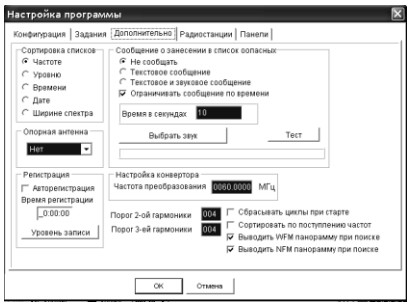


Рис. 2. Закладка «Дополнительно»

Форма отчетности:

Наименование лабораторной работы;
Результаты тестирования;
Выводы по работе;

Задания для самостоятельной работы:

1. Ввести дополнительные параметры настройки программы.

2. Измерить уровень и настройку параметров приемника.

Рекомендации по выполнению:

В разделе «Сообщение о занесении в список» можно выбрать метод оповещения об идентификации сигнала методом акустического зондирования или по возрастанию несущей частоты или отказаться от оповещения. Если выделить позицию «Текстовое сообщение», то при обнаружении сигнала микрофона методом акустического зондирования на экране появится сообщение: «Внимание! Обнаружен звуковой отклик! Частота 450,18 МГц». При этом процесс сканирования будет остановлен. Если отметить позицию «Ограничивать по времени и ввести время в секундах», сканирование будет возобновлено по истечении этого времени.

Отметив позицию «Текстовое и звуковое сообщение», пользователь будет дополнительно получать звуковое оповещение, которое воспроизводится через звуковую плату компьютера. Звуковое сообщение выбирается щелчком по кнопке «Выбрать звук», которая открывает стандартное окно загрузки файлов Windows. Звуковые файлы с расширением .wav из стандартного комплекта поставки Windows могут находиться в папке win409 dows\media. Имя выбранного звукового файла отображается в нижней час- ти этого раздела закладки. Файл можно предварительно прослушать, щелкнув по кнопке «Тест». Сначала необходимо отрегулировать громкость звучания стандартной программой Windows.

В позиции ввода частоты преобразования конвертора RS/L plus необходимо записать ее значение в мегагерцах, указанное на корпусе устройства, программа сама автоматически пересчитает это значение к 12,5-кГц сетке. После завершения ввода дополнительных параметров необходимо щелкнуть по кнопке ОК. Отказаться от внесенных изменений можно щелчком по кнопке «Отмена».

4. Настроить частоту. Программа RS turbo располагает возможностями быстрой настройки приемника на заданную частоту. Для настройки частоты приема сигналов в питающей сети 220 В или в проводных линиях необходимо открыть закладку «Сеть» в главном окне. Теперь цифровой индикатор отражает частоту настройки сканера относительно частоты преобразования конвертора RS/L plus, которая вводится при настройке программы и указывается слева от индикатора уровня.

Полоса обзора выбирается в закладке «Сеть» кнопками управления масштабом отображения по оси частот и может принимать только два значения: 1 и 16 МГц (значение по умолчанию – 16 МГц), причем для 1-МГц полосы отображается линейка прокрутки. Щелчок мыши в интересующей области диапазона переместит курсор и настроит сканер на ближайшую частоту из 12,5-кГц сетки. Одновременно программа включает узкую полосу пропускания сканера (нажата кнопка NFM). Для перестройки частоты на несколько 12,5 кГц-шагов можно воспользоваться кнопками увеличить/уменьшить слева от индикатора частоты. Кроме того, значение частоты можно ввести с клавиатуры, щелкнув левой кнопкой мыши по индикатору частоты настройки.

5. В окне ввода набрать частоту диапазона проводных линий (от 0,6 до 16 МГц) и щелкнуть по кнопке ОК. Введенное значение частоты про- грамма приведет к ближайшему значению из 12,5-кГц сетки и установит частоту 16 МГц, если пользователь по ошибке укажет большее значение.

Для расширения возможностей ручного управления приемником предусмотрен быстрый просмотр частот, занесенных в списки в процессе сканирования. Если открыть соответствующий список и выделить щелчком мыши нужную запись, сканер настроится на частоту обнаруженного сигнала. Таким образом, оператор может быстро прослушать демодулированный сигнал на частотах, зафиксированных в автоматическом режиме. Последовательно настраивать приемник на частоты из списка удобно с помощью клавиш «стрелка вверх/вниз».

6. Измерить уровень и настройку параметров приемника.

Для измерения уровня необходимо навести на индикатор курсор мыши и нажать левую кнопку. Индикатор отражает текущее значение уровня до тех пор, пока кнопка не будет отпущена, и сохраняет это значение после отпускания кнопки мыши до выполнения очередного измерения или цикла сканирования. Тип демодулятора приемника и полоса пропускания выбирается кнопками: NFM – узкополосная частотная модуляция (ЧМ), WFM - широко-

полосная ЧМ, АМ – амплитудная модуляция. Справа от кнопок выбора полосы пропускания и режима демодулятора расположена кнопка управления аттенюатором АТТ. Нажатая кнопка соответствует включению дополнительного затухания, отжатая отключению аттенюатора.

7. Выполнить без учета априорных данных простое сравнение со ставляющих измеренного с разрешением 12,5 кГц спектра сигнала с указанным в задании порогом.

8. Зафиксировать превышение порога. Программа запоминает часто- ту и уровень сигналов закладок и заносит данные в список сигналов, обнаруженных с помощью конвертора RS/L plus.

В центре главного окна размещается экран панорамного отображения спектров. Вертикальная ось экрана панорамного отображения спектров отражает интенсивность принимаемого сигнала в децибелах относительно уровня шума приемника. Горизонтальная ось соответствует частоте. Над экраном панорамы спектра находятся закладки «Радио», «Сеть» и «Панорама» (рис. 3).

Закладка «Сеть» отображает процесс и результаты сканирования диапазона поднесущих частот проводных линий от 0,6 до 16 МГц с помощью конвертера RS/L plus, а закладка «Панорама» используется для просмотра файлов спектральных панорам. Отображение спектральной панорамы в закладках «Сеть» и «Панорама» ведется с шагом 12,5 кГц. Справа находится вертикальный (столбцовый) индикатор уровня принимаемого сигнала с дополнительной цифровой индикацией и окно списков обнаруженных частот. Кнопки «Старт» и «Стоп» в нижней части экрана запускают и останавливают процесс сканирования, а кнопка «Анализ» вызывает окно для выполнения операций идентификации и классификации излучений на выделенной в списке частоте.

Рядом с кнопкой «Анализ» находятся кнопки выбора типа демодулятора сканера и управления аттенюатором, а также индикатор частоты настройки приемника с кнопками пошагового изменения частоты настройки сканера. В нижней части основного окна находятся две строки состояний. В первой отражается тип сканера, с которым работает комплекс, и время, затраченное на выполнение текущей операции сканирования. Во второй строке появляются поясняющие сообщения о функциях кнопок окна, а также имена файлов спектральной панорамы, которые используются в качестве диаграммы загрузки диапазона при классификации сигналов (Активная панорама) и загружены для просмотра в закладке «Панорама» (Файл панорамы).

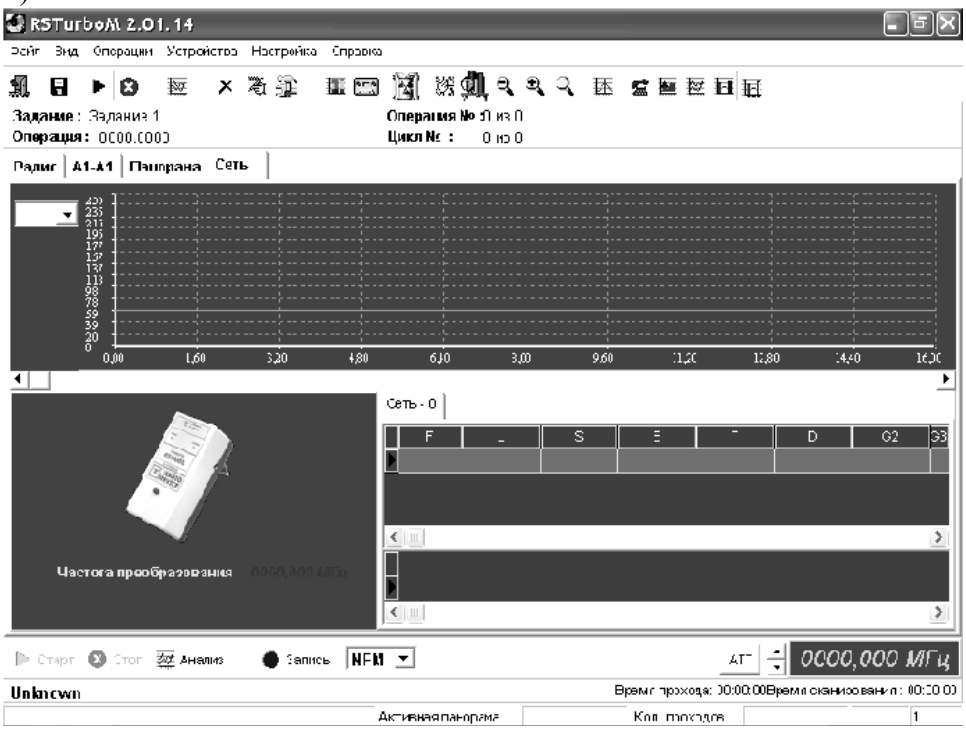


Рис. 3. Экран панорамы спектра

Для настройки частоты приема сигналов в сети 220 В или в проводных линиях необходимо открыть закладку «Сеть». В этом режиме цифровой индикатор отражает частоту настройки сканера относительно частоты пре- образования конвертора RS/L plus, которая вводится при настройке про- граммы и указывается слева от индикатора уровня. Полоса обзора выбирается в закладке «Сеть» кнопками управления масштабом отображения по оси частот и может принимать только два значения: 1 и 16 МГц (значение по умолчанию – 16 МГц), причем для 1-МГц полосы отображается линейка прокрутки. Щелчок кнопки мыши в интересующей области диапазона переместит курсор и настроит сканер на ближайшую частоту из 12,5-кГц сетки. Одновременно программа включает узкую полосу пропускания сканера (нажата кнопка NFM).

Для перестройки частоты на несколько 12,5-кГц шагов можно воспользоваться кнопками увеличить/уменьшить слева от индикатора частоты. Кроме того, значение частоты можно ввести с клавиатуры, предварительно щелкнув левой кнопкой мыши при наведенном на индикатор частоты настройки курсоре. В окне ввода набрать частоту диапазона про- водных линий (от 0,6 до 16 МГц) и щелкнуть по кнопке ОК. Введенное значение частоты программа приведет к ближайшему значению из 12,5-кГц сетки и установит частоту 16 МГц, если пользователь по ошибке укажет большее значение. Для расширения возможностей ручного управления приемником предусмотрен быстрый просмотр частот, занесенных в списки в процессе сканирования.

Если открыть соответствующий список и выделить щелчком левой кнопки мыши нужную запись, то сканер настроится на частоту обнаруженного сигнала. Таким образом, оператор может быстро прослушать де- модулированный сигнал на частотах, зафиксированных в автоматическом режиме. Последовательно настраивать приемник на частоты из списка удобно с помощью клавиш стрелка вверх/вниз.

9. Произвести акустическое зондирование.

Кнопкой «Анализ» или командой «Анализ меню – Операции» вызвать окно анализа обнаруженных сигналов, в названии которого указывается частота анализируемого сигнала. В этом окне выбирается закладка «Звуковой тест». В верхней части закладки отображается реверберационная кар- тина помещения, для просмотра которой можно воспользоваться линейкой прокрутки (рис. 4).

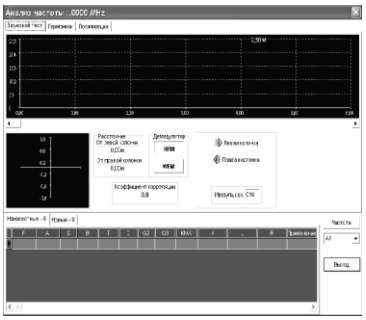


Рис. 4. Окно «Анализ частоты»

Измерить расстояние от звуковой колонки до некоторой точки, напри- мер, одного из импульсов можно, указав на него курсором мыши. При этом значение расстояния в метрах отображается в правом верхнем углу экрана реверберационной картины. В нижней части закладки отображается корреляционная функция отклика, расстояния от звуковых колонок до микрофона и значение коэффициента корреляции.

Чтобы выполнить акустический тест, необходимо из нужного списка выбрать интересующий сигнал или ввести произвольную частоту с помо- щью кнопки Частота, установить полосу приема (NFM или WFM), указать число циклов (импульсов) звукового зондирования и нажать кнопку с изображением левой или правой колонки. При повторном выполнении теста предыдущая реверберационная картина стирается. Закончив анализ, щелк- ните по кнопке Выход.

10. Провести анализ спектра.

Анализатор спектра вызывается инструментальной кнопкой основного окна программы или командой «Спектр – меню – Операции» (рис. 5). Полоса обзора анализатора отсчи-

тывается вверх и вниз относительно центральной частоты. Значение полосы обзора соответствует ширине тракта ПЧ-приемника – 8 МГц. Значение центральной частоты устанавливается программой при выделении записи в одном из списков обнаруженных сигналов или вводится оператором. В последнем случае произвольно установленная центральная частота, которая может не совпадать с сеткой режима сканирования, корректируется программой.

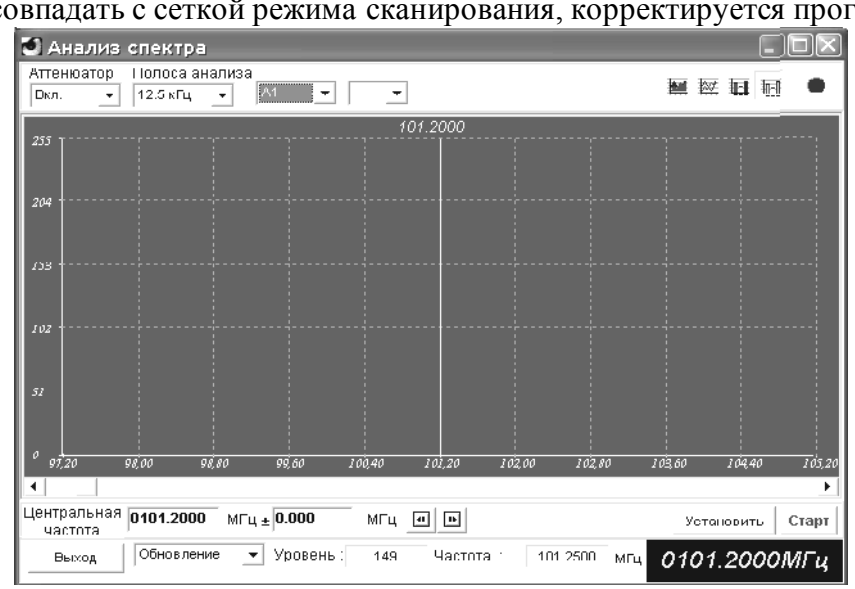


Рис. 5. Окно «Анализ спектра»

В верхней части окна находятся позиции выбора состояния аттенюатора и полосы анализа (200 или 12,5 кГц). После ввода этих параметров необходимо щелкнуть мышью по кнопке «Установить». В нижней части окна находится выпадающий список выбора режима обработки спектральных составляющих в последовательных циклах обзора.

В режиме обновления текущее значение заменяет предшествующее, в режиме накопления выбирается максимальное из этих двух значений, а в режиме усреднения – среднее. Щелчок по кнопке «Старт», включает циклический режим анализа спектра в заданной полосе обзора. Спектральные составляющие текущего цикла обзора отражаются зеленым цветом, предыдущего – красным. Отмечая позиции «Сглаживание» и «3D» вид спектра можно изменять в процессе анализа. Остановить анализ можно кнопкой «Стоп». При этом картина спектра запоминается.

После остановки процесса анализа можно измерять частоты и уровни спектральных составляющих, поместив курсор мыши в нужную область экрана отображения спектра. Координаты курсора, соответствующие частоте и измеренному уровню спектральной составляющей, отображаются в правой части окна ниже индикатора частоты.

Не выходя из окна спектроанализатора, можно анализировать сигналы на выходе демодулятора сканера. Подведите курсор к интересующей спек- тральной составляющей и щелкните левой кнопкой мыши. Сканер настроится на нужную частоту, которая отображается индикатором окна спектроанализатора. Теперь сигнал на выходе демодулятора можно прослушать или вывести на экран программы-осциллографа. Полоса пропускания сканера выбирается из выпадающего списка «Полоса анализа». Для выхода из окна анализатора спектра достаточно щелкнуть по кнопке «Выход».

11. Сохранить и просмотреть спектральную панораму.

Спектральную панораму, полученную в результате текущего и/или предшествующих циклов сканирования радиодиапазонов можно сохранить в виде файла. Для этого, после остановки сканирования, с помощью инструментальной кнопки или команды «Сохранить» меню «Файл» вызывается стандартное окно сохранения файлов Windows, где предлагается ввести имя файла и указать место его хранения. По умолчанию программа комплекса RS turbo размещает файлы спектральных панорам в папке RSturbo/ Panorama. Файлы спектральных панорам должны иметь расширение .pan. Пользователь может создавать и хранить любое число таких файлов. При сохранении файла с именем, которое уже есть в папке, программа запрашивает подтверждение на перезапись.

Удалить файлы панорам можно стандартными действиями в окне Windows. Сохранение результатов сканирования диапазонов проводных линий в виде файлов не предусмотрено. Для просмотра спектральных па- норам, которые сохранены в виде файлов, необходимо щелкнуть мышью по закладке «Панорама» (рис. 6).

Рис. 6. Закладка «Панорама»

В режиме просмотра панорам доступна инструментальная кнопка за- грузки файлов. Загрузить файл спектральной панорамы можно также командой, открыть меню «Файл», которая вызывает стандартное окно загрузки файлов Windows, где необходимо выбрать имя файла и щелкнуть по кнопке «Открыть». На экранах спектры файла панорамы отображаются синим цветом. Кнопками управления полосой обзора установите в окне спектральной панорамы удобный масштаб отображения по оси частот и найдите интересующий участок спектра с помощью линейки прокрутки и движка, которые позволяют «листать» картины спектра и быстро переходить к нужному участку диапазона. Если щелкнуть мышью на экране спектральной панорамы, в окне детального анализа будет показан спектр соответствующего участка с разрешением 12,5 кГц. Следует учитывать, что просмотр спектральной панорамы в закладке Панорама не изменяет частоты настройки сканера. Спектральная картина в закладке «Панорама» сохраняется в течение всего сеанса работы и может использоваться для сравнения с текущими спектрами, полученными в процессе сканирования.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. Назовите демаскирующие признаки сетевых акустических закладок.
2. Назовите демаскирующие признаки проводной микрофонной системы подслушивания.
3. Перечислите демаскирующие признаки акустических и телефонных закладок с передачей на высокой частоте.
4. Перечислите способы прослушивания беседы, ведущейся в ком- нате, при положенной на рычаг трубке.

5. По каким признакам в RS turbo возможна сортировка списков час- тот обнаруженных сигналов?
6. Поясните назначение акустического зондирования при выявлении линейной или сетевой закладки.
7. Результаты сканирования какого диапазона поднесущих частот проводных линий отображает закладка меню «Сеть»?

Лабораторная работа №4 Обнаружение оптических сигналов передатчиков ИК - диапазона

Цель работы: Изучить методы обнаружения оптических сигналов передатчиков ИКдиапазона с помощью комплексов «RS turbo», «RS turbo Mobile-L».

Задание

1. Сформировать список опасных излучений которые могут быть сделаны передатчиком
2. Выполнить операции анализа, необходимые для выявления среди множества обнаруженных сигналов подслушивающих устройств

Порядок выполнения:

1. Отобразить результаты экспериментальных данных с помощью комплекса «RS turbo.
2. Отобразить результаты экспериментальных данных с помощью комплекса «RS turbo Mobile-L».

Форма отчетности:

1. Привести задание на выполнение лабораторной работы.
2. Отобразить результаты экспериментальных данных, полученных при выполнении задания.
3. Сделать выводы по результатам работы.
4. Ответить на контрольные вопросы.

Задания для самостоятельной работы:

1. Ввести дополнительные параметры настройки программы.
2. Измерить уровень и настройку параметров приемника.

Рекомендации по выполнению:

Для доступа к нужному списку обнаруженных сигналов необходимо щелкнуть левой кнопкой мыши по закладке, на которой указано название списка и текущее число записей обнаруженных сигналов в нем. Графы списков содержат следующие данные: F – несущая частота обнаруженного сигнала в МГц; S – максимальный уровень в полосе обнаруженного сигнала, дБ; B – ширина спектра обнаруженного сигнала в МГц; T – время первого обнаружения сигнала, час и минуты текущих суток; D – дата первого обнаружения сигнала; G2 – уровень второй гармоники обнаруженного сиг- нала, дБ; G3 – уровень третьей гармоники обнаруженного сигнала, дБ; K – коэффициент корреляции при выполнении акустического теста; L – рас- стояние до микрофона от левой колонки, метры; R – расстояние до микрофона от правой колонки, метры. Пользователь может добавить или изменить примечание к любой записи в специальном окне, если выделить запись мышью в списке и щелкнет по ней правой кнопкой. После ввода текста примечания необходимо щелкнуть по кнопке ОК или отказаться от ввода (изменений) кнопкой «Отмена». При большом числе записей в списке появляется линейка вертикальной прокрутки. Листать списки можно также с помощью клавиш «стрелка вверх/вниз».

В программе предусмотрена возможность настройки ширины столбцов списков. Для этого необходимо навести курсор мыши на границу между столбцами в заголовке списка. После изменения формы курсора нажать левую кнопку мыши и, не отпуская ее, переместить границу столбца. Таким образом, можно настроить вид списков для отображения только тех данных, которые интересуют пользователя. Настройка ширины столбцов списка сохраняется для всех списков во всех окнах программы.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. Укажите на основные особенности канала для сигналов ИК-диапазона
2. Каким образом передается речевой сигнал с помощью ИК-диапазона

Лабораторная работа №5 Локатор нелинейностей

Цель работы: изучение принципа работы локатора нелинейностей на основе моделирования схемы замещения в среде программы Electronics Workbench.

Задание:

1. Снять временные диаграммы сигналов на передатчике и приемнике нелинейного локатора для элементов с ВАХ ложного и полупроводникового соединений.
2. Сравнить полученные характеристики сигналов.
3. Снять спектры амплитуд гармоник сигналов, отраженных от нелинейных элементов с несимметричной и симметричной ВАХ.
4. Сравнить численно амплитуды второй и третьей гармоник отраженных сигналов от нелинейных элементов с несимметричной и симметричной ВАХ и сделать выводы о причине различия соотношений гармоник в первом и втором случаях.

Порядок выполнения:

1. Запустить моделирующую программу EWB 5.
2. Зайти в меню File -> Open -> radar2.ewb либо на стандартной панели инструментов нажать кнопку «Открыть » и выбрать файл «radar2.ewb», соответствующий модели локатора нелинейностей для p-n-перехода.
3. Включить симулятор.
4. Для наблюдения сигналов локатора двойным щелчком мыши по значку осциллографа открыть окно осциллографа, а для увеличения окна нажать кнопку «Expand». Оба канала осциллографа перевести в режим «АС».
5. Нажать кнопку «В/А» и снять ВАХ полупроводникового прибора.
6. Закрыть окно осциллографа и зайти в меню Analysis -> Fourier -> Simulate. На экране появится гармонический спектр сигнала, по которому определить значения амплитуд 2-й и 3-й гармоник сигнала.
7. Открыть схему «radar2.ewb» и выполнить действия по всем шести пунктам задания для схемы «radar2.ewb». Примечание. В схеме «radar2.ewb» симметричная ВАХ нелинейного элемента сформирована встречно-параллельным соединением двух диодов.

Форма отчетности:

Оформить отчет, в котором привести задание для выполняемой работы, результаты экспериментов согласно заданию, выводы, ответить на контрольные вопросы.

Задания для самостоятельной работы:

1. Сравнить полученные характеристики сигналов.
2. Снять спектры амплитуд гармоник сигналов, отраженных от нелинейных элементов с несимметричной и симметричной ВАХ.

Рекомендации по выполнению:

Программа комплекса «RS turbo» выполняет сортировку списков обнаруженных сигналов по различным критериям: частоте, уровню, времени, дате и ширине спектра. Для сортировки списков с помощью инструментальной кнопки или команды «Сортировка» меню – «Вид» необходимо вызвать окно сортировки, выбрать критерий сортировки и щелкнуть по кнопке ОК. Для очистки списков нажмите инструментальную кнопку «Очистить списки» или выполните команду «Очистка списков» – меню «Настройка». Появится окно (рис. 7).

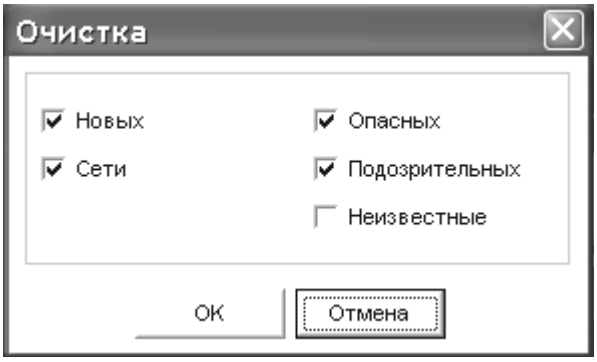


Рис. 7. Окно «Очистка»

В котором нужно отметить те списки, все записи в которых необходимо удалить.

Если отметить позицию «Неизвестные», будут удалены не только записи в списке неизвестных частот, но и данные спектральной панорамы, полученные на предыдущих циклах сканирования.

Более широкие возможности предоставляет редактор списков, который можно вызвать инструментальной кнопкой или командой «Редактор списков» меню «Вид». С его помощью в нужном списке можно удалить конкретную запись. Для этого необходимо открыть список, выделить мышью запись и щелкнуть по кнопке «Удалить». Если при этом пометить Рис. 7. Окно «Очистка» позицию Удалять из панорамы спектральные компоненты этого сигнала будут удалены из текущей панорамы. Завершив работу, щелкните по кнопке ОК.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. Приведите определение нелинейного элемента и назовите несколько видов нелинейных объектов.
2. В чем заключается принцип нелинейной локации?
3. Почему в отраженном сигнале от нелинейного элемента с p-n-переходом преобладает вторая гармоника?
4. Как зависит мощность сигнала, отраженного от объекта, от частоты локатора?

Лабораторная работа №6 Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля.

Цель работы**:** Обнаружение активных прослушивающих устройств с помощью поискового прибора D008.

Задание:

1) Обнаружить замаскированный радиопередатчик с помощью поискового прибора D008 в режиме работы радиодетектер.
2) Прослушать аудиосигнал от прослушивающего устройства в головных телефонах с использованием режима акустической обратной связи.
3) Обнаружить прослушивающие устройство с помощью поискового прибора D008 в режиме работы анализатор проводных линий.

Порядок выполнения:

1. Обнаружить замаскированный радиопередатчик.

2. Прослушать аудиосигнал.
3. Обнаружить прослушивающие устройство.

Форма отчетности:

В отчете привести задание на выполнение работы, результаты поиска универсальным поисковым прибором D008 в соответствии с пунктами задания на лабораторную работу. Сделать выводы по проделанной работе и ответить на контрольные вопросы.

Задания для самостоятельной работы:

1. Ввести дополнительные параметры настройки программы.
2. Измерить уровень и настройку приемника.

Рекомендации по выполнению:

Суть измерения коэффициентов виброизоляции состоит в следующем:

− производится измерение так называемого тестового вибросигнала непосредственно на поверхности ОК или контролируемого элемента ИК внутри помещения. Исходный тестовый акустический сигнал излучается акустической системой (АС) комплекса;
− измеряется уровень фоновых виброшумов в контрольной точке;
− измеряется уровень вибросигнала на поверхности ОК/ИК в контрольной точке. Исходный тестовый акустический сигнал излучается акустической системой комплекса;
− рассчитывается коэффициент виброизоляции;
− делается вывод о достаточности/недостаточности виброизолирующей способности ОК.
− По окончании измерении оформляется протокол установленной формы. 4.5.1. Измерение уровня тестового вибросигнала Для измерения уровня тестового сигнала необходимо:
− расположить акустическую систему на высоте 1,5 м от пола на штативе на расстоянии 1 м от обследуемой ОК/ИК (при всех остальных измерениях АС должна располагаться на расстоянии 1,5 м от обследуемой ОК/ИК). Ось апертуры АС направляется в сторону ОК по нормали к ее поверхности. Если ОК является пол (потолок), то АС размещается в центре помещения на высоте 1…1,5 м от пола. Ось апертуры направляется соответственно в пол или потолок по нормали к поверхности ОК;
− закрепить измерительный вибродатчик на заданной ОК/ИК. Датчик закрепляется по возможности напротив диффузора динамика акустической системы, перпендикулярно ему. В случае с оконным остеклением, датчик необходимо прикрепить в центре самого большого стекла изнутри помещения и установить АС по возможности на высоте вибродатчика.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689
2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. Опишите кратко принцип действия поисковго устройства D008.
2. Для чего предназначен режим РД?
3. Для чего используется режим акустической обратной связи.
4. Для чего предназначен режим АПЛ?

Лабораторная работа №7 Программно-аппаратный комплекс «СПРУТ-7»

Цель работы: Изучить методику применения комплекса Спрут-7 при оценке защищенности ограждающих конструкций помещения от утечки информации по виброакустическому кана-

лу. Научиться рассчитывать коэффициенты виброизоляции ограждающих конструкций помещения и оформлять результаты измерений.

Задание:

1. Изучить особенности заданных ограждающих конструкций или инженерных коммуникаций.
2. Подготовить комплекс «Спрут-7» для проведения виброакустических измерений.
3. Провести измерения степени виброизоляции заданных ОК или ИК.
4. Оформить протокол контроля и дать рекомендации по применению дополнительных мер защиты.

Порядок выполнения:

1. Проведите осмотр и анализ заданной ОК/ИК помещения с целью определения возможного направления утечки информации.

2. Составьте план схему помещения, отметьте на ней предложенную для оценки виброизоляции ОК/ИК.

3. На плане помещения и предложенной ОК выберите точки контроля (контрольные точки (КТ)). Контрольные точки выбираются в местах, наиболее опасных с точки зрения перехвата информации.

Форма отчетности*:*

Отчетом по данной работе является протокол инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации а также ответы на контрольные вопросы.

Задания для самостоятельной работы:

1. Осуществить выбор места расположения контрольных точек.
2. Подготовить комплекс «Спрут-7» для проведения виброакустических измерений.

Рекомендации по выполнению:

Выбор места расположения контрольных точек производится по следующим правилам:

1. на подводимой к проверяемому помещению трубопроводной коммуникации контрольные точки располагаются на расстоянии 0,3…0,5 м от места ее выхода из проверяемого помещения. Если это невозможно, то не-обходимо найти ближайшую к помещению доступную для съема информации точку;

2. при наличии вентиляционного короба, подводимого к помещению, две-три контрольные точки располагаются на поверхности воздухопровода на расстоянии 0,3…0,5 м от места выхода из проверяемого помещения;

3. на сплошном однородном ограждении (стена, перекрытие) кон-трольные точки располагаются в соответствии с рис. 1, по диагонали от центра к углу с шагом 0,3…1 м. Крайние точки располагаются на расстоянии не менее 0,25 м от вершин углов ОК;

4. на сплошном неоднородном ограждении, например стене, отдельные участки которой имеют различную толщину или выполнены из различных материалов, контрольные точки располагаются в соответствии с предыдущей рекомендацией по отношению к каждому однородному участку;

5. на остеклении оконных проемов контрольные точки располагаются в соответствии с рис. 1 для каждой рамы окна и каждого участка остекления;

на дверном проеме контрольные точки располагаются в соответствии с рис. 1, а также на поверхности коробки двери по периметру.

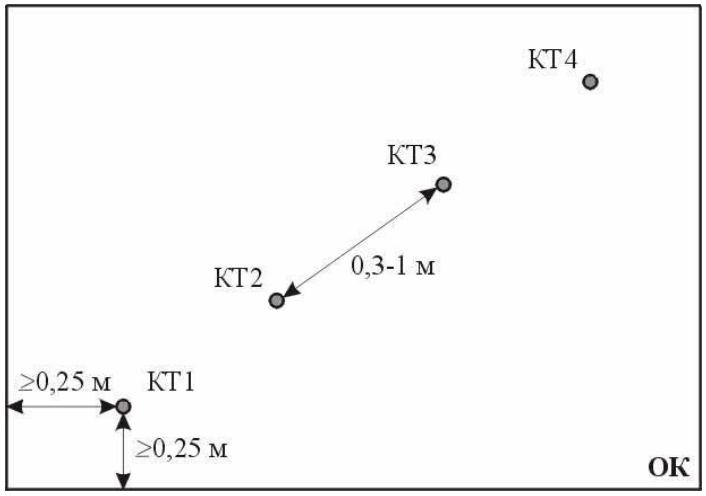


Рис. 1. Схема расположения контрольных точек на однородном участке ограждающей конструкции

Подготовьте комплекс «Спрут-7» для проведения виброакустических измерений. Для этого:

- подключите модуль сопряжения к ПЭВМ;
- подключите измерительный вибродатчик к измерительному модулю.

2. Подключите антенну к измерительному модулю. Включите питание измерительного модуля. На ЖК-индикаторе модуля в правом верхнем углу отобразится уровень заряда батарей модуля. При необходимости замените батареи измерительного модуля.

- подключите источник тестового акустического сигнала к акустической системе. Включите питание источника тестового акустического сигнала (светодиод на передней панели модуля должен загореться зеленым светом). Включите питание акустической системы.
- запустите программное обеспечение для управления комплексом. Через несколько секунд произойдет инициализация оборудования. Убедитесь, что:

- тип входного датчика – акселерометр;
- кнопка «Полный спектр» отжата;
- чувствительность – низкая;
- фильтры 1/1 октавы;
- панель источника тестового сигнала – активна;
- уровень выходного сигнала источника тестового акустического сиг-нала – минимум;
- тип выхода – блокировка.

5. Проведение измерений

Крепление вибродатчика на ОК/ИК должно быть механически жест-ким. Для этого в комплект комплекса входят различные крепежные эле-менты: хомут для крепления вибродатчика на трубы системы отопления и водоснабжения, площадка для крепления на стекла окон, шпильки с резь-бой для стен. Внешний вид крепежных элементов и примеры крепления приведены в приложении А.

На хомут для труб и дюбели вибродатчик закрепляется резьбовым соединением. Для прикрепления вибродатчика к стеклу необходимо закрепить на вибродатчике площадку для крепления на окна, нанести на площадку немного пчелиного воска (прилагается к комплексу), разогреть воск при помощи зажигалки или спички, и пока воск не остыл приклеить площадку вместе с вибродатчиком к стеклу в выбранной контрольной точке. На подоконник под местом установки вибродатчика необходимо положить какой-нибудь предмет, который предохранит вибродатчик от удара при падении при неудачном приклеивании, либо принять другие меры для исключения падения датчика;

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 4.2,

6. графу $V_{c1\ i}$, где i – номер октавной полосы (от 1 до 5).

Измерение уровня фонового виброшума

Для измерения уровня фонового виброшума в контрольной точке вы-полните следующие действия:

- закрепите измерительный вибродатчик в контрольной точке при помощи необходимых элементов крепления;
- установите АС на расстоянии 1,5 м от ОК/ИК;
- используя программное обеспечение, на панели управления измерительным модулем включите режим графика №1 – накопление минимумов, количество циклов накопления – Нажмите кнопку «Пуск». На панели анализатора спектра будут отображаться минимальные значения спек-тральных составляющих фоновой обстановки. Измерения необходимо проводить при минимальных уровнях внешних шумов (при отсутствии персо-нала, при выключенных системах кондиционирования и вентиляции и пр.). Через 30 сек, после того, как загорится зеленый индикатор справа от эле-мента «Количество циклов накопления», нажмите кнопку «Стоп».

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 4.2,

7. графу $V_{ш\,i}$, где i – номер октавной полосы (от 1 до 5).

Измерение уровня вибросигнала в контрольной точке

На панели управления модулем акустического сигнала с помощью элемента «Выход» установите «Белый шум». Запустите сбор информации, нажатием кнопки «Пуск» на панели управлении измерительным модулем. Через 30 сек нажмите кнопку «Стоп ». Отключите генерацию шума (в окне управления модулем акустического сигнала установите режим «Выход» – «Блокировка»).

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 4.2 в графу $V_{(с+ш)\,i}$, где i – номер октавной полосы (от 1 до 5).

Примечание: если выбранная контрольная точка находится на одном из внутренних стекол оконного проема, то очевидно, что ввиду большой жесткости стекла измерения тестового вибросигнала (п. 4.5.1) и вибросигнала в данной контрольной точке дадут практически одинаковый результат (разница будет небольшой из-за того, что при оценке тестового сигнала акустическая система располагается на расстоянии 1 м от ОК/ИК, а при измерении вибросигнала в контрольной точке требуется располагать АС на расстоянии 1,5 м от поверхности ИК/ОК). Поэтому понятно без всяких измерений, что коэффициент виброизоляции в данном случае будет стремиться к нулю, если не применяются средства активной защиты.

Расчет коэффициентов виброизоляции

Рассчитайте октавные уровни виброакустического сигнала $V_{с2i}$ по фор-мулам (1):

где – поправка в дБ, определяемая из табл. 4.1.

Таблица 4 . 1

V(с+ш) i	> 10	6…10	4…6	3	2	1	0,5
, дБ	0	1	2	3	4	7	10

Запишите рассчитанные значения $V_{с2i}$ в табл. 4.2.

Октавные уровни виброизоляции G_i рассчитываются по формуле (2):

$$G_i = V_{с1\,i} - V_{с2\,i} \qquad (2)$$

Запишите рассчитанные значения G_i в табл. 4.2.

Сравните полученные значения G_i с требуемыми нормативными значениями, приведенными в табл. 4.3. Если хотя бы один из коэффициентов виброизоляции меньше, чем нормированное значение, делается вывод о недостаточности виброизоляции и следовательно о незащищенности помещения от утечки речевой информации.

Завершение измерений

Выключите комплекс «СПРУТ-7». Для этого:

1. завершите работу с программой;

2. выключите АС выключателем питания;
3. выключите модуль тестового акустического сигнала;
4. выключите измерительный модуль;

3. отсоедините измерительный вибродатчик, упакуйте его в предназначенную коробку.
4. отключите модуль сопряжения;
5. сложите все компоненты комплекса в сумку.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. Какими особенностями характеризуются распространение звуковых колебаний в инженерных конструкциях?
2. Каким образом осуществляется съем речевой информации по виброакустическому каналу?
3. Зависит ли спектральный состав виброшума в контрольной точке от механической жесткости проверяемой ОК?
4. Назовите наиболее известные генераторы акустического и виброакустического маскирующего шума.
5. Цель проведения технического контроля акустической защищенности выделенного помещения.
6. Относительно каких мест проводится технический контроль акустической защищенности выделенного помещения?
7. Что предполагает инструментальный контроль акустической защищенности выделенных помещений?

Лабораторная работа №8 Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу комплексом «СПРУТ-7»

Цель работы: Изучить методику применения комплекса Спрут-7 при оценке защищенности помещения от утечки речевой информации по каналам акусто-электрических преобразований в технических средствах. Научиться оценивать октавные соотношения «сигнал/шум» и оформлять результаты измерений.

Задание:

1. Изучить особенности заданного технического средства, предвари-тельно оценить возможность возникновения АЭП.
2. Подготовить комплекс «Спрут-7» для проведения измерений АЭП.
3. Провести измерения сигналов АЭП.
4. Оформить протокол оценки защищенности помещения.
5. Ответить на контрольные вопросы.

Порядок выполнения :

1. Составьте план-схему размещения ТС в помещении, отметьте ли-нии, выходящие за пределы помещения.
2. Подготовьте комплекс «Спрут-7» для проведения акустических измерений. Для этого:

− подключите модуль сопряжения к ПЭВМ;

− подключите измерительный микрофон к измерительному модулю. Подключите антенну к измерительному модулю. Включите питание измерительного модуля;
− подключите источник тестового акустического сигнала к акустической системе. Включите питание источника тестового акустического сиг-нала (светодиод на передней панели модуля должен загореться зеленым светом). Включите питание акустической системы.
− запустите программное обеспечение для управления комплексом. Через несколько секунд произойдет инициализация оборудования. Убедитесь, что:
− тип входного датчика – микрофон;
− кнопка «Полный спектр» отжата;
− чувствительность – низкая;
− фильтры 1/1 октавы;
− панель источника тестового сигнала – активна;
− уровень выходного сигнала источника тестового акустического сиг-нала – минимум;
− тип выхода – блокировка.

Форма отчетности:

Отчетом по данной работе является протокол инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации (рекомендуемая форма протокола приведена в приложении), а также ответы на контрольные вопросы.

Задания для самостоятельной работы:

1. Составьте план-схему размещения ТС в помещении.
2. Подключите модуль сопряжения к ПЭВМ.

Рекомендации по выполнению:

Измерение октавных уровней тестового акустического сигнала

В качестве тестового акустического сигнала при измерении уровней АЭП необходимо использовать гармонические тональные сигналы с опре-деленными уровнями. Поэтому необходимо «откалибровать» комплекс
«Спрут-7».

Разместите микрофон на расстоянии 1 м от АС. Используя про-граммное обеспечение, на панели управления измерительным модулем включите режим графика №1 – текущий спектр.

На панели управления модулем акустического сигнала с помо-щью элемента «Синус» установите частоту выходного сигнала в соответст-вии с табл. 5.1, в элементе управления «Выход» установите «Синус».

Нажмите кнопку «Пуск». С помощью регулятора уровня в пане-ли источника тестового акустического сигнала начинайте увеличивать громкость воспроизводимого тонального сигнала. Добейтесь октавного уровня сигнала, указанного в табл. 5.1. Измерения уровня производитекурсором в окне анализатора спектра по центру соответствующей октавной полосы (не спутайте октавный уровень сигнала с интегральным).

Запишите значение регулятора уровня панели источника акусти-ческого сигнала в табл. 5.1.

Повторите для каждого значения часто-ты, указанной в табл. 4.1.

Таблица 5.1

Октавные уровни тестовых сигналов

Среднегеометрическая частота октавной по-лосы, Гц	Требуемый октавный уровень тестового сигнала, дБ	Значение уровня громко-сти в панели источника акустического сигнала
250	66	
500	66	
1000	61	
2000	56	
4000	53	

Завершите измерения уровней тестового акустического сигнала. Выключите измерительный модуль, отключите и упакуйте измерительный микрофон.

Измерение уровня октавного шума

Подключите ко входу измерительного модуля дифференциальный усилитель №1,2. Входы усилителя при помощи прилагаемых осцилло-графических пробников подключите к исследуемой линии по симметричной (рис. 1) или несимметричной схеме (рис. 2)

Рис. 1. Симметричная схема подключения

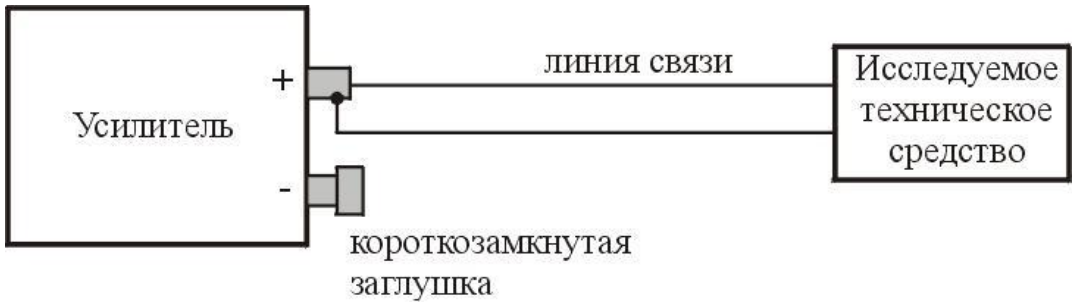


Рис. 2. Несимметричная схема подключения

Если исследованию подвергается ТС, требующее подачи пита-ния (телефон, датчики пожарной сигнализации и т.п.), подключите питание ТС от источника питания «SZPS-01». К разъему переходника (рисунок 3.4) подключите один из входов дифференциального усилителя (в этом случае возможно только несимметричное подключение).

Включите дифференциальный усилитель. Включите измерительный модуль. Проведите настройку программного обеспечения (на панели датчиков):

– тип входного датчика – прямой вход;

– усилитель №1,2 (20 дБ, 40 дБ или 60 дБ) в зависимости от положения переключателя на задней панели усилителя.

На панели управления измерительным модулем включите режим графика №1 – текущий спектр. Нажмите кнопку «Пуск». В окне анализа-тора спектра должен отобразиться текущий спектральный состав напряжения шумов, присутствующих на входном разъеме дифференциального усилителя.

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 5.2,
графу $U_{\text{ш.окт } i}$, где i – номер октавной полосы (от 1 до 5).

Завершение измерений

Выключите комплекс «СПРУТ-7». Для этого:

1. завершите работу с программой;
2. выключите АС выключателем питания;
3. выключите модуль тестового акустического сигнала;
4. выключите измерительный модуль;
5. выключите дифференциальный усилитель;
6. отключите модуль сопряжения;
7. сложите все компоненты комплекса в сумку.

Выполнение расчетов

Результаты измерений заносятся в табл. 5.2. Значения в графах «Уро-вень шума в линии связи, $U_{ш.окт\ i}$, мкВ» и «Уровень сигнала АЭП в линии связи $U_{с\ i}$, мкВ» рассчитываются по формуле 1.

Расчет отношения «сигнал/шум» в каждой октавной полосе производится по формуле 2. Нормативное значение отношения «сигнал/шум» = 0,3, т.е. информация считается защищенной, если $\Delta i < 0{,}3$.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. В чем заключается эффект акустоэлектрических преобразований?
2. Какие физические эффекты лежат в основе АЭП предложенного Вам в лабораторной работе технического средства?
3. Какие устройства с акустоэлектрическим эффектом могут входить в состав некоторых ВТСС?
4. В чем заключается эффект модуляционного акустоэлектрического преобразования?
5. В каком случае проводную линию следует рассматривать как не-симметричную?
6. Назовите наиболее простой способ выявления факта модуляции сигнала модуляционного акустоэлектрического преобразователя.
7. По какому признаку делается вывод о наличии акустоэлектрических преобразований ВТСС?
8. Если акустоэлектрические преобразования обнаружены, то каким образом можно оценить их опасность?
9. Причины и последствия модуляции информационным речевым сигналом высокочастотных колебаний у генераторов технических средств.
10. Каким образом осуществляется перехват речевого сигнала в акустоэлектрическом канале?

Лабораторная работа №9 Сетевые помехоподавляющие пассивные фильтры низких и высоких частот

Цель работы: изучение свойств и методов расчета фильтров низких и высоких частот с заданными свойствами, моделирование работы фильтров в среде программы Electronics Workbench.

Задание:

1. Для фильтра низких частот по заданной полосе пропускания F2 и нагрузке R рассчитать параметры L и C Т-образной и П-образной структур.
2. Снять экспериментальные амплитудно-частотные характеристики фильтров низких частот с расчетными параметрами и сравнить заданную (расчетную) и экспериментальную полосы пропускания для обеих структур фильтра.
3. Для фильтра высоких частот по заданной полосе подавления F1 и нагрузке R рассчитать параметры L и C Т-образной и П-образной структур.
4. Снять экспериментальные амплитудно-частотные характеристики фильтров высоких частот с расчетными параметрами и сравнить заданную (расчетную) и экспериментальную полосы подавления для обеих структур фильтра.

Порядок выполнения:

1. Запустить моделирующую программу EWB 5. Набрать схему Т-образного фильтра нижних частот.
2. Согласно заданному преподавателем варианту рассчитать параметры фильтра L и C.
3. Отредактировать схему согласно расчетным параметрам.
4. Включить схему, двойным щелчком клавиши мыши по измерителю частотных характеристик раскрыть его и в линейном режиме снять амплитудно-частотную характеристику.
5. Определить полосу пропускания (в том месте, где значение амплитудно-частотной характеристики снизится до 0,707 от максимального значения). Сравнить значение полосы пропускания с расчетным значением.

Форма отчетности:

В отчете привести задание, принципиальные схемы фильтров, результат отчетов, экспериментальные амплитудно-частотные характеристики фильтров и отразить полученные результаты измерений. Сделать выводы и ответить на контрольные вопросы.

Задания для самостоятельной работы:

Снять экспериментальные амплитудно-частотные характеристики фильтров высоких частот с расчетными параметрами и сравнить заданную (расчетную) и экспериментальную полосы подавления для обеих структур фильтра.

Рекомендации по выполнению:

1. Ознакомиться с заданием
2. Изучить теоретические сведения полученные на лекции
3. Ознакомиться с примерами решение подробных задач в учебной литературе
4. Разработать и написать программу

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. Какое назначение имеют пассивные фильтры?
2. Назовите типы помехоподавляющих пассивных фильтров.
3. Приведите определения полосы пропускания и полосы подавления фильтров низких и высоких частот.
4. На каких элементах реализуются пассивные фильтры?

Лабораторная работа №10 Сетевые пассивные полосно-заграждающие и полосно-пропускающие фильтры

Цель работы: изучение свойств и методов расчета сетевых помехоподавляющих полосно-заграждающих и полосно-пропускающих фильтров с заданными свойствами, моделирование работы фильтров в среде программы Electronics Workbench.

Задание:

1. Для полосно-заграждающего фильтра по заданной полосе подавления F1 – F2 и нагрузке R рассчитать параметры L и C Т-образной и П-образной структур.
2. Снять экспериментальные амплитудно-частотные характеристики полосно-заграждающих фильтров с расчетными параметрами и сравнить заданную (расчетную) и экспериментальную полосы подавления для обеих структур фильтра.

3. Для полосно-пропускающего фильтра по заданной полосе пропускания F1 – F2 и нагрузке R рассчитать параметры L и C Т-образной и П-образной структур.
4. Снять экспериментальные амплитудно-частотные характеристики полосно-пропускающих фильтров с расчетными параметрами и сравнить заданную (расчетную) и экспериментальную полосы пропускания для обеих структур фильтра.

Порядок выполнения:

1. Запустить моделирующую программу EWB5. Набрать схему Т-образного полосно-заграждающего фильтра.
2. Согласно заданному преподавателем варианту рассчитать параметры L и C.
3. Отредактировать схему согласно расчетным параметрам.
4. Включить схему, двойным щелчком клавиши мыши по измерителю частотных характеристик раскрыть его и в линейном режиме снять амплитудно-частотную характеристику.
5. Определить полосу подавления (в том месте, где значение амплитудно-частотной характеристики снизится до 0,707 от максимального значения). Сравнить значение полосы подавления с расчетным значением.
6. Набрать схему П-образного полосно-заграждающего фильтра.
7. Отредактировать схему согласно расчетным параметрам.
8. Включить схему, двойным щелчком клавиши мыши по измерителю частотных характеристик раскрыть его и в линейном режиме снять амплитудно-частотную характеристику.

Форма отчетности:

В отчете привести задание, принципиальные схемы фильтров, результаты отчетов, экспериментальные амплитудно-частотные характеристики фильтров и отразить полученные результаты измерений. Сделать выводы и ответить на контрольные вопросы.

Задания для самостоятельной работы:

Снять экспериментальные амплитудно-частотные характеристики фильтров высоких частот с расчетными параметрами и сравнить заданную (расчетную) и экспериментальную полосы подавления для обеих структур фильтра.

Рекомендации по выполнению:

1. Ознакомиться с заданием
2. Изучить теоретические сведения полученные на лекции
3. Ознакомиться с примерами решение подробных задач в учебной литературе
4. Разработать и написать программу

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. Приведите определения полосы пропускания и полосы подавления полосно-пропускающего и полосно-заграждающего фильтров.
2. За счет каких свойств полосно-пропускающих и полосно-заграждающих фильтров обеспечивается полоса пропускания или подавления?
3. Как определяются полосы пропускания и подавления полосных фильтров?

Лабораторная работа №11 Активные фильтры низких и высоких частот

Цель работы*:* изучение свойств и методов расчета активных фильтров низких частот на основе моделирования схемы в среде программы Electronics Workbench.

Задание:

1. Для фильтра низких частот по заданной полосе пропускания F и нагрузке RH рассчитать параметры фильтра.
2. Снять экспериментальную амплитудно-частотную характеристику фильтра низких частот с расчетными параметрами и сравнить расчетную и экспериментальную полосы пропускания.

Порядок выполнения*:*

1. Запустить моделирующую программу EWB5. Набрать схему активного фильтра низких частот.
2. Согласно заданному преподавателем варианту рассчитать параметры фильтра по вышеприведенным расчетным соотношениям.
3. Отредактировать схему согласно расчетным параметрам.
4. Включить схему, двойным щелчком клавиши мыши по измерителю частотных характеристик раскрыть его и в линейном режиме снять амплитудно-частотную характеристику.
5. Определить полосу пропускания (в том месте, где значение амплитудно-частотной характеристики снизится до 0,707 от максимального значения). Сравнить значение полосы пропускания с расчетным значением.

Форма отчетности:

В отчете привести задание на выполнение работы, принципиальную схему фильтра, результаты расчетов, экспериментальную амплитудно-частотную характеристику фильтра и отразить полученные результаты измерений. Сделать выводы и ответить на контрольные вопросы.

Задания для самостоятельной работы:

Снять экспериментальные амплитудно-частотные характеристики фильтров высоких частот с расчетными параметрами и сравнить заданную (расчетную) и экспериментальную полосы подавления для обеих структур фильтра.

Рекомендации по выполнению:

1. Ознакомиться с заданием
2. Изучить теоретические сведения полученные на лекции
3. Ознакомиться с примерами решение подробных задач в учебной литературе
4. Разработать и написать программу

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. В чем заключаются преимущества активных фильтров по сравнению с пассивными?
2. Назовите недостатки активных фильтров.

Лабораторная работа №12 Расчет паразитных связей через посторонний провод

Цель работы изучение причин появления паразитных связей через потусторонний провод, моделирование эквивалентных схем замещения в среде программы Electronics Workbench.

Задание: В схемах с паразитной емкостной и индуктивной связью через посторонний провод рассчитать и проверить экспериментально напряжение наводки второго канала на первый.

Порядок выполнения:

1. Запустить моделирующую программу EWB 5. Набрать схему с указанными на ней параметрами.

2. При замкнутом и разомкнутом положениях переключателя на осциллографе наблюдать сигнал помехи в цепи нагрузки постороннего провода.
3. Набрать схему с указанными на ней параметрами.
4. Установить необходимые параметры трансформатора по методике занятия 9.
5. При замкнутом и разомкнутом положениях переключателя на осциллографе наблюдать сигнал помехи в цепи постороннего провода.

Форма отчетности:

В отчете привести задание, принципиальные эквивалентные схемы, результаты экспериментов. Сделать выводы и ответить на контрольные вопросы.

Задания для самостоятельной работы:

Снять экспериментальные амплитудно-частотные характеристики фильтров высоких частот с расчетными параметрами и сравнить заданную (расчетную) и экспериментальную полосы подавления для обеих структур фильтра.

Рекомендации по выполнению:

1. Ознакомиться с заданием
2. Изучить теоретические сведения полученные на лекции
3. Ознакомиться с примерами решение подробных задач в учебной литературе
4. Разработать и написать программу

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689
2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1. Чем обусловлены помехи в каналах связи с посторонним проводом?
2. Как влияет величина собственного сопротивления постороннего провода на величину наводки в случаях емкостной и индуктивной паразитных связей?
3. Какие существуют способы снижения помех через посторонний провод?

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

ОС Windows 7 Professional
Microsoft Office 2007 Russian Academic OPEN No Level
Антивирусное программное обеспечение Kaspersky Security.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Вид занятия (*Лк, Лр , кр)*	***Наименование аудитории***	***Перечень основного оборудования***	***№ Лр***
1	**3**	**4**	**5**
Лк	Лекционная аудитория		№ 1.1 -3.2
ЛР	Лаборатория технических средств защиты информации	Оборудование 16-ПК i5-2500/H67/4Gb/500Gb (монитор TFT19 Samsung E1920NR); интерактивная доска Smart Board X885ix со встроенным проектором UX60	№ 1-5
СР	Читальный зал №1	Оборудование 10 ПК i5-2500/H67/4Gb(монитор TFT19 Samsung); принтер HP LaserJet P2055D	-

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-6 ПК-7 ПК-8	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций Способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения Способность приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности	**1.** Основы технических средств и методов защиты информации	1.1. Концепции инженерно-технической защиты информации	Вопросы к экзамену 1 – 7
			1.2. Теоретические основы инженерно-технической защиты информации	Вопросы к экзамену 8 – 12
			1.3 Физические основы защиты информации	Вопросы к экзамену 13 – 19
			1.4. Технические средства добывания и инженерно-технической защиты	Вопросы к экзамену 20 - 28
			1.5. Организационные основы инженерно-технической защиты информации	Вопросы к экзамену 29 - 32
			1.6. Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	Вопросы к экзамену 33 -46

2. Вопросы к экзамену, 7 семестр

№ п/п	Компетенции		ВОПРОСЫ К ЭКЗАМЕНУ	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1.	ПК-6	Способность формировать суждения о значении и послед-	1. Технические каналы утечки информации, общие понятия, технические каналы утечки речевой информации.	

		ствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	2. Воздушные каналы утечки речевой информации.	**1.** Основы технических средств и методов защиты информации
			3. Вибрационные технические каналы.	
			4. Электроакустические каналы утечки информации.	
			5. Оптико-электронный технический канал утечки информации.	
			6. Параметрические каналы утечки информации .	
			7. Технические каналы утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи.	
			8. Электрические линии связи.	
			9. Электромагнитные каналы утечки информации: электромагнитные излучения элементов ТСПИ, электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ и ВТСС, электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ, ПЭМИ ПК.	
			10. Электрические каналы утечки информации.	
			11. Способы скрытого видеонаблюдения и съемки.	
			12. Демаскирующие признаки объектов и акустических закладок: в видимом диапазоне электромагнитного спектра, в инфрокрасном диапазоне электромагнитного спектра.	
2.	ПК-7	Способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	13. Демаскирующие признаки радиоэлектронных средств, демаскирующие признаки акустических закладок.	
			14. Средства акустической разведки: микрофоны, направленные микрофоны, проводные системы, портативные диктофоны и электронные стетоскопы, радиомикрофоны, лазерные микрофоны, гидроакустические датчики, СВЧ и ИК передатчики.	
			15. Средства радио и радиотехнической разведки: сканирующие компьютерные радиоприемники, радиопеленгаторы, анализаторы спектра, радиочастотметры.	
			16. Средства обеспечения информационной безопасности в компью-	

			терных системах: соболь, secret net, аккорд, secret dist, крипто-про, астра.
			17. Технические средства радиомониторинга и обнаружения закладных устройств: индикаторы поля, комплексы обнаружения закладок и радиомониторинга
			18. Нелинейная локация: технология, эффект затухания, тип излучения промышленные образцы
3.	ПК-8	Способность приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности	19. Средства защиты информации в телефонных системах (с использованием криптографических методов)
			20. Металлодетекторы
			21. Контроль слаботочных линий
			22. Защита слаботочных линий
			23. Системы слежения за транстортными средствами
			24. Контроль телефонных каналов связи
			25. Прослушивание телефонных каналов связи
			26. Экранирование электромагнитных волн
			27. Экранирование соединительных проводников
			28. Безопасность оптоволоконных линий связи
			29. Заземление технических средств
			30. Фильтрация информационных сигналов
			31. Основные сведения и выбор помехоподавляющих фильтров
			32. Какие существуют инженерно-технические средства обеспечения безопасности объектов
			33. Угрозы утечки информации по техническим каналам в ИСПДн .
			34. Виды, источники и носители защищаемой информации.
			35. Характеристика государственной системы противодействия технической разведке.
			36. Основные положения методологии инженерно-технической защиты

			информации.	
			37. Основные свойства электромагнитного поля (ЭМП) элементарного электрического излучателя в ближней зоне.	
			38. Основные свойства электромагнитного поля (ЭМП) элементарного магнитного излучателя в ближней зоне.	
			39. Электрическое и магнитное поля однопроводных и двухпроводных линий.	
			40. Акустоэлектрические технических каналов утечки акустической информации(ТКУАИ).	
			41. Характеристика зонового принципа защиты информации.	
			42. Защита информации, обрабатываемой ТСПИ, методом экранирования.	
			43. Защита информации, обрабатываемой ТСПИ, методом фильтрации.	
			44. Пассивные методы защиты акустической информации.	
			45. Активные методы защиты акустической информации.	
			46. Классификация объектов охраны, особенности задач охраны различных типов объектов.	

3. Описание показателей и критериев оценивания компетенций

Показатели	**Оценка**	**Критерии**
Знать: *(ПК-6)* информацию о современных разработках в области своей профессиональной деятельности и решаемых задачах, их позитивной значимости и возможности их негативных последствий. *(ПК-7)* − технические каналы утечки информации; − возможности технических разведок; − способы и средства защиты информации от	**Отлично**	Студент демонстрирует сформированность дисциплинарных компетенций на высоком уровне, обнаруживает всестороннее, систематическое и глубокое знание специфики современных разработок, особенностей технических каналов утечки информации, приемов разведки информации посредством технических средств. Владеет способами защиты информации от несанкционированного доступа по техническим каналам, методами контроля эффективности защиты. Умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями,

утечки по техническим каналам; методы и средства контроля эффективности технической защиты информации. *(ПК-8)* организационно-управленческие навыки в профессиональной и социальной деятельности. **Уметь:** *(ПК-6)* сформировать и дать обоснованные суждения о значении и последствиях своей профессиональной деятельности, сформулировать обоснование актуальности и значимости результатов решаемых задач профессиональной деятельности с учетом социальных, профессиональных и этических позиций *(ПК-7)* анализировать и оценивать угрозы информационной безопасности объекта. *(ПК-8)* приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности. **Владеть:** *(ПК-6)* навыками формирования суждения о значении и последствиях своей профессиональной деятельности, формулировки актуальности и значимости результатов решаемых задач профессиональной деятельно-		применяет их в ситуациях повышенной сложности, включая ситуации анализа угроз информационной безопасности.
	Хорошо	Студент демонстрирует сформированность дисциплинарных компетенций на среднем уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации в частности в области знаний специфики современных разработок, особенностей технических каналов утечки информации, приемов разведки информации посредством технических средств. Владеет способами защиты информации от несанкционированного доступа по техническим каналам, методами контроля эффективности защиты
	Удовлетворительно	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по дисциплинарной компетенции, студент испытывает значительные затруднения при оперировании знаниями и умениями в областях специфики современных разработок, особенностей технических каналов утечки информации, приемов разведки информации посредством технических средств. Владеет способами защиты информации от несанкционированного доступа по техническим каналам, методами контроля эффективности защиты
	Неудовлетворительно	− Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже базового, проявляется недостаточность знаний, умений, навыков. Не владеет навыками формирования суждения о значении и последствиях своей профессиональной деятельности, формулировки актуальности и значимости результатов решаемых задач профессиональной деятельности с учетом социальных, профессиональных и этических позиций, методами формирования требований по защите информации;

сти с учетом социальных, профессиональных и этических позиций. *(ПК-7)* − методами технической защиты информации; − методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации. *(ПК-8)* способностью приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности.		методами расчета и инструментального контроля показателей технической защиты информации.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Дисциплина Технические средства и методы защиты информации направлена на ознакомление обучающихся с основами технических средств и методов защиты информации; на получение теоретических знаний в области инженерно-технической защиты информации, и практических навыков в применении полученных знаний в условиях работы на конкретных объектах информационной безопасности, а так же осуществления поиска, хранения, обработки и анализа информации из различных источников и представления ее в соответствующем виде для дальнейшего использования в практической деятельности.

Изучение дисциплины Технические средства и методы защиты информации предусматривает:

- лекции,
- лабораторные работы;
- экзамен;
- самостоятельную работу студента в объеме 18 часов.

Для фиксирования успешности обучения предусматривается экзамен.

В ходе освоения раздела 1 «Основы технических средств и методов защиты информации» обучающиеся должны уяснить основные средства и методы защиты информации.

Студентам необходимо овладеть навыками и умениями применения изученных методов для разработки и реализации защитных средств информации.

В процессе изучения дисциплины рекомендуется на первом этапе обратить внимание на специфику применения технических средств и методов для защиты информации.

Овладение ключевыми понятиями является основой усвоения учебного материала по дисциплине.

При подготовке к экзамену особое внимание необходимо уделить рекомендациям и замечаниям преподавателей, ведущих аудиторные занятия по дисциплине

В процессе проведения лабораторных занятий происходит закрепление знаний, фор-

мирование умений и навыков применения различных методов решения стандартных ситуаций, связанных с защитой информации.

Самостоятельную работу необходимо начинать с чтения лекций и учебников.

В процессе консультации с преподавателем обучающийся выясняет наличие пробелов в знаниях и способах решения разных ситуаций.

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и Интернете.

Предусмотрено проведение аудиторных занятий в виде разнообразных тренингов и ситуаций общения в сочетании с внеаудиторной работой.

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
Технические методы и средства защиты информации

1. Цель и задачи дисциплины

Формирование у студентов знаний по основам инженерно-технической защиты информации, а также выработка навыков и умений в применении полученных знаний в условиях работы на конкретных объектах информационной безопасности.

Задачами изучения дисциплины являются:

- изучение технических средств добывания информации;
- назначения и функций видов разведки;
- способов доступа к источникам конфиденциальной информации без проникновения на объект защиты;
- способов и средств защиты конфиденциальной информации техническими средствами

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: Лк.-24 час., ЛР-48 час.; СР-18 час.

Общая трудоемкость дисциплины составляет 144 часов, 4 зачетных единиц.

2.2 Основные разделы дисциплины:

1 – Технические методы и средства защиты информации.

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-6 – Способность понимать, совершенствовать и применять современный математический аппарат;

ПК-7 – Способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения;

ПК-8 – Способность составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы.

4. Вид промежуточной аттестации: экзамен.

Приложение 3

Протокол о дополнениях и изменениях в рабочей программе
на 20___-20___ учебный год

1. В рабочую программу по дисциплине вносятся следующие дополнения:
_____
_____

2. В рабочую программу по дисциплине вносятся следующие изменения:

_____
_____
_____

Протокол заседания кафедры №____ от «___» _____ 20 __ __ г.,
(разработчик)

Заведующий кафедрой _____ _____
(подпись) *(Ф.И.О.)*

Приложение 4

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	**1.** Технические методы и средства защиты информации	1.1. Концепции инженерно-технической защиты информации	Тест
			1.2. Теоретические основы инженерно-технической защиты информации	Тест
			1.3. Физические основы защиты информации	Тест
ПК-7	Способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения		1.6. Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	Тест
ПК-8	Способность приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности		1.4 Технические средства добывания и инженерно-технической защиты	Тест
			1.5 Организационные основы инженерно-технической защиты информации	Тест

2. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать: *(ПК-6)* информацию о современных разработках в области своей профессиональной деятельности и решаемых задачах, их позитивной значимости и возможности их негативных последствий. *(ПК-7)* – технические каналы утечки информации;	**Отлично**	Демонстрирует все показатели на высоком уровне. Обучающийся всесторонне и глубоко владеет знаниями, сложными навыками в области современных информационных и программных разработок, способен уверенно ориентироваться в специфике каналов передачи информации и особенностей их защиты; анализе угрозы информационной безопасности и принятия мер по их устранению. Достигнут высокий уровень формирования компетенций.

− возможности технических разведок; − способы и средства защиты информации от утечки по техническим каналам; методы и средства контроля эффективности технической защиты информации. *(ПК-8)* организационно-управленческие навыки в профессиональной и социальной деятельности. **Уметь:** *(ПК-6)* сформировать и дать обоснованные суждения о значении и последствиях своей профессиональной деятельности, сформулировать обоснование актуальности и значимости результатов решаемых задач профессиональной деятельности с учетом социальных, профессиональных и этических позиций *(ПК-7)* анализировать и оценивать угрозы информационной безопасности объекта. *(ПК-8)* приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности. **Владеть:** *(ПК-6)* навыками формирования суждения о значении и последствиях своей профессиональной деятельности, формулировки актуальности и зна-	**Хорошо**	Демонстрирует более половины показателей на достаточном и высоком уровне. Обучающийся владеет знаниями, проявляет соответствующие навыки в практических ситуациях, но имеют место некоторые неточности в демонстрации освоения материала в области современных информационных и программных разработок, в специфике каналов передачи информации и особенностей их защиты; анализе угрозы информационной безопасности и принятия мер по их устранению. Достигнут повышенный уровень формирования компетенции.
	Удовлетворительно	Демонстрирует основную часть показателей на достаточном уровне. Обучающийся частично проявляет знания и навыки, в области современных информационных и программных разработок; анализе угрозы информационной безопасности и принятия мер по их устранению. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается. Достигнут только базовый уровень формирования компетенции.
	Неудовлетворительно	Демонстрирует большинство показателей на недостаточном и крайне низком уровне. Обучающийся не владеет необходимыми знаниями и навыками в области современных информационных и программных разработок, в специфике каналов передачи информации и особенностей их защиты; анализе угрозы информационной безопасности и принятия мер по их устранению и не старается их применять. Не достигнут базовый уровень формирования компетенции.

чимости результатов решаемых задач профессиональной деятельности с учетом социальных, профессиональных и этических позиций. *(ПК-7)* − методами технической защиты информации; − методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации. *(ПК-8)* способностью приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности.		

Фонд тестовых заданий

по дисциплине

Б1.В.14 Технические средства и методы защиты информации

ТЕМАТИЧЕСКАЯ СТРУКТУРА ТЕСТОВ

N раздела	Наименование радела	N задания	Тема задания
1.	Технические методы и средства защиты информации	1 - 5	1.1 Концепции инженерно-технической защиты информации
		6 - 10	1.2 Теоретические основы инженерно-технической защиты информации
		11 - 14	1.3. Физические основы защиты информации
		15 - 18	1.4.Технические средства добывания и инженерно-технической защиты
		19 - 22	1.5.Организационные основы инженерно-технической защиты информации

Тестовые задания

1. Что является выходами системы защиты информации?

1 сведения

2 средства и методы защиты

3 злоумышленники и владельцы информации

4 внешние и внутренние угрозы

2. Непосредственная причина возникновения угрозы называется? (отметьте один правильный вариант ответа):

1 атака

2 злоумышленник

3 источник угрозы

4 источник сигнала

3. Как называется состояние информации, при котором доступ к ней могут осуществить только субъекты, имеющие на него право? (отметьте один правильный вариант ответа):

1 доступность

2 целостность

3 конфиденциальность

4 неотказуемость

4. Анна послала письмо Степану. Злоумышленник прочитал письмо Анны, подсунул вместо него свое и отправил Степану от имени Анны. Какое свойство(а) информации было(и) нарушено? (ответ считается верным, если отмечены все правильные ответы):

1 целостность

2 доступность

3 неотказуемость

4 конфиденциальность

5. Если в результате DDOS-атаки новостной сайт на какое-то время вышел из строя и был недоступен для пользователей, какое свойство информации было нарушено? (отметьте один правильный вариант ответа)

1 целостность

2 неотказуемость

3 доступность

4 конфиденциальность

6. Формирование политики безопасности организации относится к (отметьте один правильный вариант ответа) :

1 организационным мерам обеспечения безопасности

2 морально0этическим мерам обеспечения безопасности

3 техническим мерам обеспечения безопасности

4 правовым мерам обеспечения безопасности

7. Установка генератора шума для создания эффекта маскировки речевого сигнала в защищаемом помещении относится к (отметьте один правильный вариант ответа):

1 физическим мерам обеспечения безопасности

2 техническим мерам обеспечения безопасности

3 организационным мерам обеспечения безопасности

4 морально-этическим мерам обеспечения безопасности

8. Как называется документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров? (отметьте один правильный вариант ответа):

1 аттестат

2 лицензия

3 удостоверение

4 сертификат

9. Информация ограниченного доступа делится на (отметьте один правильный вариант ответа):

1 государственную тайну и общедоступную

2 общедоступную и общеизвестную

3 конфиденциальную и общедоступную

4 конфиденциальную и государственную тайну

10. Юрист в процессе своей служебной деятельности узнал цену недвижимости некоего известного человека. К какой категории информации относятся данные сведения? (отметьте один правильный вариант ответа):

1 конфиденциальной информации

2 государственной тайне

3 общедоступной информации

4 информации, доступ к которой нельзя ограничить

11. В каком техническом канале утечки информации в качестве носителей используются упругие волны? (отметьте один правильный вариант ответа):

1 оптический

2 акустический

3 радиоэлектронный

4 материально-вещественный

12. Информативность канала оценивается по (отметьте один правильный вариант ответа):

1 величине помех в канале

2 количеству информации, которую может передать канал

3 величине затухания сигнала в канале

4 ценности информации, которая передается каналом

13. В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля? (отметьте один правильный вариант ответа):

1 оптический

2 материально-вещественный

3 акустический

4 радиоэлектронный

14. По физической природе возможны следующие средства переноса информации(допишите недостающие):

- световые лучи;
- звуковые волны;
- электромагнитные волны;
- _____.

15. Технический канал утечки информации (ТКУИ) представляет собой _____ объекта технической разведки, физической _____ распространения информативного сигнала и _____, которыми добывается защищаемая информация.

16. Что является источником информации?

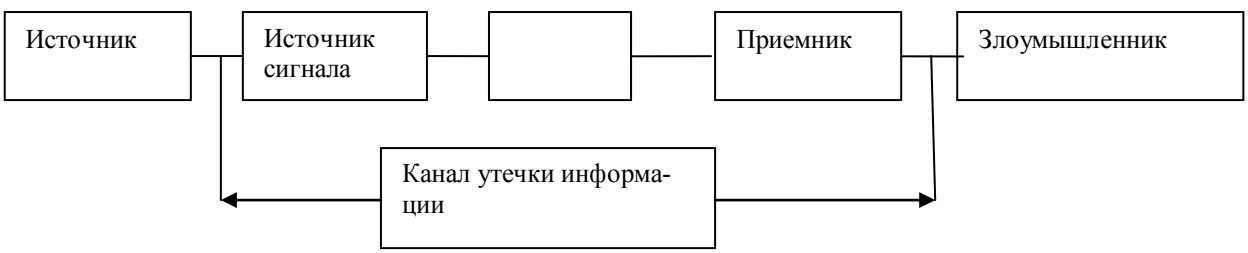
1 технические средства обработки информации

2 средства вычислительной техники

3 линии связи

4 человеческая речь

17. Восстановить структуру канала утечки информации



18. В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата,

акустические каналы утечки информации можно разделить на (ответ считается верным, если отмечены все правильные варианты ответов):

1 воздушные

2 вибрационные

3 электроакустические

4 оптико-электронные

5 параметрические

19. В акустической разведке используются (ответ считается верным, если отмечены все правильные варианты ответов):

1 пассивные методы перехвата

2 активные методы перехвата

3 контактные методы перехвата

20. Стетоскопы – это устройства (отметьте один правильный вариант ответа):

1 использующие микрофонный эффект

2 высокочастотного (ВЧ) навязывания

3преобразующие упругие механические колебания твердых физических сред в акустический сигнал

21. Какими характеристиками должен обладать источник информации для образования визуально-оптических каналов (ответ считается верным , если отмечены все правильные варианты ответов):

1 угловыми размерами

2 собственной яркостью

3 яркость фона

4 контрастностью

22. Основными источниками информации материально-вещественного канала утечки информации являются: (Написать)

23. Наиболее уязвимым каналов по видовым демаскирующим признакам является (отметьте один правильный вариант ответа):

1 оптический

2 материально-вещественный

3 акустический

4 радиоэлектронный

.

Ответы к тесту

№		№		№	
2	2	12	2	22	бумага и т.д.
3	3	13	4	23	1
4	1	14	материалы и вещества		
5	3	15	совокупность…среды…средство		
6	1	16	1, 2, 3, 4		
7	2	17	среда передачи		
8	4	18	1, 2, 3, 4, 5		
9	4	19	1, 2		
10	3	20	1		

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.02 Прикладная математика и информатика от «12» марта 2015 г. №228

для набора 2015 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «13» июля 2015 г. №475

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06»июня 2016 г. №429

для набора 2017 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06» марта 2017 г. №125

для набора 2018 года и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «12» марта 2018 г. №130

Программу составил:

Сташок О.В. к.т.н, доцент каф. Математики и физики _____

Рабочая программа рассмотрена и утверждена на заседании кафедры математики и физики

от «21» ноября 2018 г., протокол № 3

Заведующий кафедрой
Математики и физики _____ О.И.Медведева

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой МиФ _____ О.И Медведева

Директор библиотеки _____ Т.Ф.Сотник

Рабочая программа одобрена методической комиссией ЕН факультета

от «20» декабря 2018 г., протокол № 4
Председатель методической комиссии факультета _____ М.А. Варданян

СОГЛАСОВАНО:
Начальник
учебно-методического управления _____ Г.П. Нежевец

Регистрационный №_____

(методический отдел)