

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Шебзухова Татьяна Александровна

Должность: Директор Пятигорского института (филиал) Северо-Кавказского

федерального университета

Дата подписания: 18.04.2024 15:49:04

Уникальный программный ключ:

d74ce93cd40e39275c3ba2f58486412a1b8e9b1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению самостоятельных работ
по дисциплине
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2024 г.

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	3
2. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ	3
3. ТЕХНОЛОГИЧЕСКАЯ КАРТА САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА	4
4. ТЕМЫ ДЛЯ САМОСТОЯТЕЛЬНОГО ИЗУЧЕНИЯ	5
5. ПОДГОТОВКА К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ И КУРСОВОЙ РАБОТЕ	6
6. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ	10
7. КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ	11
8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	
.....	12

1. Цель и задачи освоения дисциплины

Целью дисциплины является изучение студентами принципов построения и особенностей функционирования средств технической защиты объектов информатизации, заключающаяся в обеспечении некриптографическими методами безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Задачами дисциплины являются:

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

2. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД-1 ОПК-9 Понимать корректность криптографической алгоритмов в современных программных комплексах. ИД-2 ОПК-9 Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. ИД-3 ОПК-9 Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	Осуществляет поиск, критический анализ и синтез информации, в том числе юридически значимой, применяет системный подход для решения задач профессиональной деятельности с использованием информационных технологий, и с учетом требований информационной безопасности.
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики	ИД-1 ОПК-10 Знает меры по обеспечению информационной безопасности и методы	Способен в качестве технического специалиста принимать участие в формировании политики

участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	управления процессом их реализации на объекте защиты. ИД-2 ОПК-10 Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности. ИД-3 ОПК-10 Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.	информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты
---	---	---

3. Технологическая карта самостоятельной работы студента

№	Раздел (тема) дисциплины	Реализуемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
5 семестр							
1	Введение в цифровые технологии	ОПК-9,(ИД-1.ИД-2,ИД-3) ОПК-10,(ИД-1.ИД-2,ИД-3)	4	8	8		18
2	Интернет-технологии	ОПК-9,(ИД-1.ИД-2,ИД-3) ОПК-10,(ИД-1.ИД-2,ИД-3)	4	8	8		
3	Электронные почтовые сервисы	ОПК-9,(ИД-1.ИД-2,ИД-3) ОПК-10,(ИД-1.ИД-2,ИД-3)	4	8	8		
4	Информационная безопасность и её составляющие	ОПК-9,(ИД-1.ИД-2,ИД-3) ОПК-10,(ИД-1.ИД-2,ИД-3)	6	12	12		
	Итого за 5 семестр		18	36	36		18
	Итого		18	36	36		18

4. ТЕМЫ ДЛЯ САМОСТОЯТЕЛЬНОГО ИЗУЧЕНИЯ

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, используя рекомендуемые источники информации
Работа с литературой:

№ п/п	Виды самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая литература	Интернет-ресурсы
1.	изучение литературы по темам 1-14	1,2	1,2	1-3	1-2
2.	проработка лекционного материала	1,2	1,2	1-3	1-2

Оценочные средства: собеседование

5. ПОДГОТОВКА К ЛАБОРАТОРНЫМ РАБОТАМ И КУРСОВОЙ РАБОТЕ

№ п/п	Виды самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая литература	Интернет-ресурсы
3.	подготовка к лабораторным работам	1,2	1,2	1-3	1-2
4.	Выполнение курсовой работы	1,2	1,2	1-3	1-2

Оценочные средства: отчёт письменный

7. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Вопросы к экзамену

Вопросы к экзамену (6 семестр)

Вопросы для проверки уровня обученности:

Знать:

1. Нормативно - правовые основы информационной безопасности в РФ.
2. Основные понятия в области технической защиты информации.
3. Структура технического канала утечки информации.
4. Типы носителей информации в технических каналах связи.
5. Классификация технических каналов утечки информации.
6. Понятие информационного сигнала. Модуляция сигналов.
7. Опасные сигналы и их источники.
8. Основные показатели технического канала утечки информации.
9. Основные понятия в области акустики.
10. Классификация акустических каналов утечки информации.
11. Критерии оценки эффективности защиты акустической (речевой) информации.

12. Физические основы возникновения ТК АЭП в ВТСС.
13. Порядок проведения специальных исследований ВТСС на утечку по каналу АЭП.
14. Общий порядок проведения измерений по каналу АЭП.
15. Средства пассивной защиты информации по каналу АЭП.
16. Средства активной защиты информации по каналу АЭП.

Уметь, владеть:

1. Методика проведения специальных исследований в области акустики и виброакустики.
2. Средства акустической разведки.
3. Методы и средства пассивной защиты акустической речевой информации.
4. Методы и средства активной защиты акустической речевой информации.
5. Подавление диктофонов.
6. Перехват побочных электромагнитных излучений ТСПИ средствами разведки ПЭМИН.
7. Паразитные связи и наводки.
8. Средства перехвата радиосигналов.
9. Пассивные и активные методы защиты.

Вопросы к экзамену (5 семестр)

Вопросы для проверки уровня обученности:

Знать:

1. Структура технического канала утечки информации за счет ПЭМИН.
2. Заземление.
3. Фильтрация опасных сигналов.
4. Зашумление.
5. Низкочастотные и высокочастотные излучения технических средств.
6. Паразитные связи и наводки.
7. Средства перехвата радиосигналов.
8. Пассивные и активные методы защиты.
9. Индикаторы электромагнитных излучений. Радиочастотометры.
10. Сканирующие приемники.
11. Автоматизированные поисковые комплексы.
12. Оценка защищенности помещений от утечки речевой информации по акустическому и виброакустическому каналам и по каналу электроакустических преобразований.
13. Оценка защищенности информации от утечки за счет ПЭМИН.

Уметь, владеть:

1. Индикаторы электромагнитных излучений.
2. Радиочастотометры.
3. Сканирующие приемники.
4. Автоматизированные поисковые комплексы.
5. Досмотровая техника.
6. Специальные проверки технических средств и систем.

7. Методы оценки опасности угроз.
8. Способностью проводить эксперименты по заданной методике.
9. Способностью проводить обработку результатов, оценку погрешности и достоверности результатов.
10. Способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.

8. КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценка «отлично» выставляется студенту, если глубокие, исчерпывающие знания и творческие способности в понимании, изложении и использовании учебно-программного материала; логически последовательные, содержательные, полные, правильные и конкретные ответы на все поставленные вопросы и дополнительные вопросы преподавателя; свободное владение основной и дополнительной литературой, рекомендованной учебной программой.

Оценка «хорошо» выставляется студенту, если твердые и достаточно полные знания всего программного материала, правильное понимание сущности и взаимосвязи рассматриваемых процессов и явлений; последовательные, правильные, конкретные ответы на поставленные вопросы при свободном устранении замечаний по отдельным вопросам; достаточное владение литературой, рекомендованной учебной программой.

Оценка «удовлетворительно» выставляется студенту, если твердые знания и понимание основного программного материала; правильные, без грубых ошибок ответы на поставленные вопросы при устранении неточностей и несущественных ошибок в освещении отдельных положений при наводящих вопросах преподавателя; недостаточное владение литературой, рекомендованной учебной программой.

Оценка «неудовлетворительно» выставляется студенту, если неправильные ответы на основные вопросы, допущены грубые ошибки в ответах, непонимание сущности излагаемых вопросов; неуверенные и неточные ответы на дополнительные вопросы.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1. Рекомендуемая литература

9.1.1. Основная литература:

1. Технические средства и методы защиты информации: учеб. пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.

2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. М.: НПЦ «Аналитика», 2017.

10.1.2. Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Электронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – [URL: http://biblioclub.ru/index.php?page=book&id=93349](http://biblioclub.ru/index.php?page=book&id=93349)
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

9.1.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине:

1. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине Техническая защита информации.
2. Методические указания по выполнению лабораторных работ по дисциплине Техническая защита информации.
3. Методические указания по выполнению курсовой работы по дисциплине Техническая защита информации.

9.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

1. <http://biblioclub.ru>
2. <http://elibrary.ru/>

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
по дисциплине
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Комплексная защита объектов информатизации**

Пятигорск, 2024 г.

Введение

Дисциплина «Техническая защита информации» относится к вариативной части блока 1. Ее освоение происходит в 7 корпусе ОП ВО подготовки бакалавра направления 10.03.01 «Информационная безопасность». Для изучения данной дисциплины необходимы знания, навыки и компетенции, полученные при изучении дисциплины «Основы информационной безопасности». Полученные в ходе изучения данной дисциплины знания, навыки и компетенции пригодятся при изучении дисциплины «Комплексная система защиты информации на предприятии», «Многоканальные цифровые системы передачи и средства их защиты».

Главной целью методических рекомендаций для студентов по организации самостоятельной работы по дисциплине «Техническая защита информации» является развитие умений и навыков, необходимых для практического применения знаний по технической защите информации при решении профессиональных задач. Данные методические рекомендации способствуют достижению этой цели.

В результате освоения содержания дисциплины «Техническая защита информации» студент должен знать: способы несанкционированного доступа к конфиденциальной информации на объекты информатизации; программно-аппаратные и технические средства защиты информации; современные концепции защиты объектов информации. Студент должен владеть: навыками проведения технико-экономического обоснования проектных решений; навыками работы в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации; уметь: применять комплексный подход к обеспечению информационной безопасности объекта защиты; формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих; проводить технические расчёты основных тактико-технических характеристик проектируемых систем охраны объектов.

Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Техническая защита информации» составлены в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, рабочим учебным планом и рабочей программой дисциплины «Техническая защита информации».

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №1. Разработка пространственной модели объекта информационной защиты. Описание угроз утечки информации по техническим каналам	5
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №2. Разработка системы активной защиты речевой информации по акустическому и виброакустическому каналу	6
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №3. Разработка системы защиты от утечек за счет побочных электромагнитных излучений и наводок	7
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №4. Разработка системы защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований	8

Практическое занятие № 1.

Тема: Разработка пространственной модели объекта информационной защиты. Описание угроз утечки информации по техническим каналам.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: угрозы информационной безопасности объектов информатизации; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.

Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

Теоретическая часть:

Пространственная модель представляет собой подробное описание выделенного помещения, инженерных конструкций, коммуникаций и средств связи, характеристику и основные параметры электронных устройств, находящихся на объекте защиты, а также технических средств безопасности. Пространственная модель объекта – это модель пространственных зон с указанным месторасположением источников защищаемой информации.

Предусматривается пространственная характеристика по таким элементам как:

- Этаж, граница КЗ на ситуационном плане
- Соседние помещения, название, толщина стен
- Помещение над потолком, название, толщина перекрытий
- Помещение под полом, название, толщина перекрытий
- Количество окон, наличие штор на окнах
- Двери (кол-во, одинарные, двойные)
- Вентиляционные отверстия, места размещения, размеры отверстий
- Батареи отопления, типы, куда выходят трубы
- Цепи электропитания
- Телефон
- Электрические часы
- Бытовые радиосредства
- Бытовые электроприборы
- ПЭВМ
- Технические средства охраны
- Телевизионные средства наблюдения
- Пожарная сигнализация
- Другие средства

Описание элементов сопровождаются функциональной, конструктивной и технической характеристиками.

Для объекта защиты, назначенного преподавателем из приложения В, разработать пространственную модель объекта информационной защиты – табличное описание пространственных зон с указанием месторасположения источников защищаемой информации. При составлении модели использовать в качестве образца таблицу П.1, приложения А.

Описание угроз утечки информации по техническим каналам.

Рассматривается актуальность угроз утечки информации по техническим каналам. Источником угрозы безопасности информации является ОСВТ и физические явления, являющиеся причиной возникновения угрозы безопасности информации. За счет реализации технических каналов утечки информации возникают следующие угрозы безопасности:

- угроза утечки акустической (речевой) информации;
- угроза утечки видовой информации;
- угроза утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН);
- угроза утечки акустической информации по каналу АЭП.

Устранение угрозы утечки видовой информации возможно без применения технических средств защиты, поэтому детально разберем остальные угрозы. Количественные результаты оценки утечки информации по каналам, полученные при проведении специальных исследований, приведены в приложении А, таблицы П.2, П.3. Измерения напряжения в канале НЧ АЭП проводились на контактах всех устройств ВТСС в рабочем режиме и в режиме холостого хода. При проведении измерений было выявлено превышение показателей противодействия относительно нормированных показателей.

Предоставленные результаты специальных исследований служат исходными данными для разработки технического решения по обеспечению защиты конфиденциальной информации от утечки по техническим каналам.

Вопросы:

1. Построить пространственную модель выделенного помещения.
2. Описать угрозы утечки информации по техническим каналам.
3. Оформить результаты специальных исследований.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб. пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.
2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НИЦ «Аналитика», 2017.

Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Элек-тронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:<http://biblioclub.ru/index.php?page=book&id=93349>.
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

Приложение А.

Таблица П.1. Пространственная модель защищаемого объекта

№ эл.	Наименование элемента пространственной зоны	Характеристики пространственной зоны
1	2	5
1.	Название выделенного помещения,	№ 1*
2.	Класс защищённости АС (на основании требований РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", 1992г.)	Класс 1Г
3.	Этаж	1
4.	Контролируемая зона	Контролируемая зона (КЗ) объекта проходит по ограждающим конструкциям, потолку и полу помещения для переговоров
5.	Количество окон, наличие штор, количество фрамуг, размеры (мм)	2 окна, на всех окнах жалюзи; окна выходят на проезжую часть улицы со зданиями
6.	Двери: количество и из какого материала изготовлены	1 дверь; стальная, усиленная
7.	Стены здания: толщина, материал	Перегородки: кирпичная кладка 65 см, облицовка. Перекрытие: монолитное
8.	Вентиляционные отверстия: места размещения, размеры	15x20см
9.	Система отопления	1 чугунная батарея вдоль окон, трубы стальные. Все трубы выведены к теплоцентрали.
10.	Цепи электропитания	Количество вводов линий 220В: две линии. Цепь электропитания подключена к городской сети напряжением 220 В, частотой 50 Гц. Электро-щитовая находится в глубине здания около служебного помещения. К цепи электропитания подключены все кабинеты и помещения. Всего 2 розетки. Критические узлы подключены к источникам бесперебойного питания.
11.	Телефон	1 шт. 2-х жильный кабель (RJ – 11) от мини-АТС

№ эл.	Наименование элемента пространственной зоны	Характеристики пространственной зоны
1	2	5
12.	Радиотрансляция	Отсутствует
13.	Электрические часы	Отсутствует
14.	Бытовые радиосредства, теле-, аудио- и видеотехника	Согласно индивидуального задания
15.	Система охраны	Имеется, автономная
16.	СКУД	Имеется, автономная
17.	Система пожарной сигнализации	Имеется
18.	Компьютерная система	1 ноутбук и 1 принтер имеют соединение через коммутатор HUB, размещенный в коридоре второго этажа; имеется соединение с сетью Интернет
* - здесь и далее поля, выделенные красным, для заполнения согласно индивидуального задания		

Таблица П.2. Результаты виброакустических исследований без САЗ

№	Место исследования	Отношение Сигнал/шум	Разборчивость речи W
Акустика			
1	Дверь	+	+
2	Вент. канал	+	-
Виброакустика			
3	Стены	+	+
4	Окно (рамы/стёкла)	+	+
5	Перекрытие нижнего этажа	+	-
6	Перекрытие верхнего этажа	+	-
7	Система отопления	+	-

Таблица П.3. Выписка из Протокола специальных исследований основного технического средства (монитор) по ПЭМИН

R2воз, м	r1, м	r1', м
75	3,9	0,9

где:

R2 - минимальный радиус зоны вокруг технического средства обработки информации (объекта), в пределах которого возможен перехват побочных электромагнитных излучений и последующее восстановление содержащейся в них информации.

Зона 1 (r1) - минимальный радиус зоны вокруг ОТСС, в пределах которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах* превышает допустимое (нормированное) значение.

Зона 1' (r1') - минимальный радиус зоны вокруг ОТСС, в пределах которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах** превышает допустимое (нормированное) значение.

Примечание:

* - Сосредоточенная случайная антенна представляет собой компактное техническое средство (например, телефонный аппарат, громкоговоритель радиотрансляционной сети, датчик пожарной сигнализации и т.д.), подключенное к линии, выходящей за пределы контролируемой зоны.

** - К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы контролируемой зоны.

Практическое занятие № 2.

Тема: Разработка системы активной защиты речевой информации по акустическому и виброакустическому каналу.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: методику расстановки средств активной защиты речевой информации от утечки по акустическому, виброакустическому каналам; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.

Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

Теоретическая часть:

Система виброакустической защиты (СВАЗ)

Проектирование системы защиты акустической речевой информации, как и любой другой, должно опираться на исходные данные. В рассматриваемой задаче проектирования системы защиты информации от утечки по виброакустическим каналам такими изысканиями являются предварительное экспертное обследование помещения.

Исходя из характеристик материала, геометрических размеров ограждающей конструкции и известного среднего радиуса действия того или иного типа излучателей, для каждой ограждающей конструкции можно определить необходимое ориентировочное количество каждого типа и моделей излучателей для создания эффективного шумления. В итоге ориентировочно может быть определено общее число каждого типа излучателей, требуемое для шумления всех ограждающих конструкций, коммуникаций и прилегающих пространств помещения в целом. Исходя из этого количества, могут быть сформулированы требования к количеству независимых каналов и нагрузочной способности базового блока СВАЗ, т.е. определена ориентировочная конфигурация СВАЗ в целом, включающая:

- тип и модель базового блока;
- тип излучателей (пассивные излучатели или генераторы-излучатели);
- общее число акустических излучателей;
- общее число вибрационных легких излучателей;
- общее число вибрационных тяжелых излучателей.

В качестве средства активной защиты информации от утечки по техническим каналам предлагается использовать Комплекс (3095) технических средств защиты информации (ТСЗИ) (СВАЗ, ПЭМИН, размыкатели), локальное проводное управление, производства ООО "Анна". Комплекс служит для защиты выделенного помещения и должен иметь возможность включения и выключения уполномоченным пользователем с помощью единого пульта управления, находящегося в выделенном помещении.

Схема комплекса представлена на рис.2.

INCLUDEPICTURE

"http://npoanna.ru/Data/Uploads/Images/Models/complex/new/3095/image006.jpg" *
MERGEFORMATINET

INCLUDEPICTURE

"http://npoanna.ru/Data/Uploads/Images/Models/complex/new/3095/image006.jpg" *
MERGEFORMATINET



Рисунок 2 - Схема комплекса "3095"

Состав комплекса представлен в Приложении Б, таблице П.4.

Методика расстановки САЗ

На основе имеющегося опыта большинство различных ситуаций, встречающихся при создании систем защиты информации от утечки по виброакустическим каналам, можно свести к следующим типовым задачам создания вибрационных и акустических зашумляющих полей на различных конструкциях:

- вибрационное зашумление окна;
- акустическое зашумление пространства за окном.
- вибрационное зашумление массивных ограждающих конструкций (стена, межкомнатная перегородка, двери, люки и т.п.) и жестких архитектурных конструкций;
- вибрационное зашумление инженерных коммуникаций круглого сечения (труб);
- акустическое и вибрационное зашумление смежных замкнутых объемов (смежных помещений, входных тамбуров, воздухопроводов систем вентиляции и кондиционирования и т.п.).

1 Акустическое зашумление

1) Очень эффективным решением для зашумления элементов окна является применение аудиогенераторов-излучателей «СА-4Б». Такое применение акустических излучателей возможно для окон, конструкция которых позволяет их размещать между рамами окна. Пример такого применения аудиоизлучателей представлен на рис. 4.

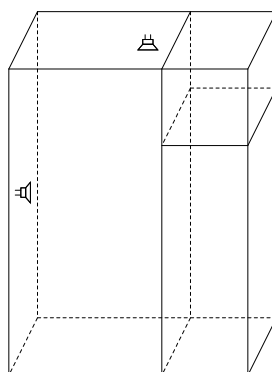


Рисунок 4 - Пример применения аудиоизлучателей для окна

Условные обозначения:

 - Генераторы-акустоизлучатели "СА-4Б1"

INCLUDEPICTURE "http://www.npoanna.ru/Data/Uploads/Images/new/izluch/image007.png" *
MERGEFORMATINET INCLUDEPICTURE
"http://www.npoanna.ru/Data/Uploads/Images/new/izluch/image007.png" *



MERGEFORMATINET

Рисунок 5 - Генераторы-акустоизлучатели "СА-4Б1"

Суть такого решения заключается в следующем. Акустический шумовой сигнал, создаваемый аудиоизлучателями, распространяясь в замкнутом пространстве сравнительно небольшого объема, многократно отражается от конструкций окна. При этом он очень эффективно возбуждает в них вибрации, особенно в протяженных жестких конструкциях, которыми являются большие стекла. Дополнительно такое решение может использоваться в случаях, когда звукоизоляция окна не обеспечивает необходимого ослабления акустического сигнала при его распространении за пределы помещения, и требуется создание акустической шумовой помехи в пространстве за окном.

2) Дверные проемы, в том числе и оборудованные тамбурами, также являются источниками повышенной опасности и в случае недостаточной звукоизоляции также нуждаются в применении активных методов защиты. Акустические излучатели систем зашумления в этом случае желательно располагать снаружи тамбура, вблизи дверной коробки со стороны смежного помещения. При таком размещении колонок системы зашумления (САЗ) «просачивающийся сигнал» имеет наименьшую величину, для его зашумления нужна минимальная мощность шума, как правило, уже не мешающая персоналу. А в защищаемое помещение шум вообще не проникает. Контроль выполнения норм защиты информации в этом случае, проводится вблизи внешней поверхности внешней (по отношению к защищаемому помещению) двери тамбура.



Рисунок 6 – Размещение акустического излучателя у дверного проёма с одним створом.

При отсутствии в конструкции двери порога независимо от площади проёма рекомендуется установка не менее 4-х излучателей на уровнях 1,5 и 0,5 м от уровня пола (см. рисунок 7). Акустические излучатели могут размещаться как открыто, на плоскости ограждающей конструкции, так и полускрыто, в стенных нишах, закрытых декоративными решётками и затянутых радиотканью.

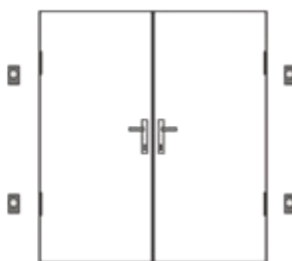


Рисунок 7 - Вариант размещения акустических излучателей для защиты дверного проёма с двумя створами.

3) При защите систем вентиляции наилучшим местом размещения колонки системы активной защиты является короб (канал) вентиляции на расстоянии не менее 1,5 м в глубину от плоскости его выхода в ВП. При таком размещении шум колонки не слышен в выделенном помещении, а защищенность достигается при невысоких уровнях громкости колонки.

Очень эффективным является размещение колонки в отдельном кожухе, «пристыкованном» к коробу вентиляции в том месте, где от него выполнен отвод в защищаемое выделенное помещение. Естественно, в стенке короба, там, где закреплен кожух с колонкой, должны быть проделаны отверстия для прохода звука. При таком размещении колонку легко извлечь для ремонта, очистки от пыли, она не уменьшает своими габаритами сечение вентиляционного канала и не мешает нормальному воздухообмену.

Такое размещение обеспечивает защищённость и не мешает воздухообмену (рисунок 8).



Рисунок 8 – Размещение акустического излучателя вне воздуховода

4) акустическое и вибрационное зашумление смежных замкнутых объемов. Для этих целей ЗАО «АННА» предлагаются Генераторы-акустоизлучатели "СА-4Б".



Рисунок 9 - Генераторы-акустоизлучатели "СА-4Б"

Вибрационное зашумление

- 1) Вибрационное зашумление массивных ограждающих конструкций и жестких архитектурных конструкций. Такие элементы, как правило, сделаны из материалов, характеризующихся высокими плотностью, массой и модулем упругости. Поэтому в данной задаче предпочтительным является применение тяжелых генераторов-вибровозбудителей "СВ-4Б1".
- 2) Особым случаем применения тяжелых генераторов-вибровозбудителей "СВ-4Б1" является зашумление различных инженерных коммуникаций круглого сечения.
- 3) Одной из наиболее часто решаемых задач является задача вибрационного зашумления элементов остекления окна. Для решения этой задачи ООО «АННА» предлагает применение легких генераторов-вибровозбудителей "СВ-4Б". Легкие генераторы-вибровозбудители "СВ-4Б" обычно применяют на окнах, конструкция которых позволяет наклеивать их прямо на стекло, как показано на рис. 10.

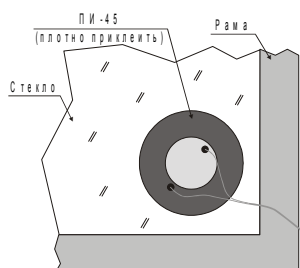


Рисунок 10 – Крепление генераторов-вибровозбудителей "СВ-4Б" на стекло

Определение мест установки, типов и количества излучателей.

а) Акустика. Ориентировочное количество аудиогенераторов-излучателей "СА-4Б"/"СА-4Б1" может быть определено исходя из следующих норм:

- 1) один "СА-4Б" на каждый вентиляционный канал,
- 2) один "СА-4Б1" на дверной тамбур или входную дверь;
- 2) один "СА-4Б" на каждые 8...12 м² надпотолочного пространства или других пустот.

б) Виброакустика. Для оценки необходимого количества виброгенераторов-излучателей "СВ-4Б"/ "СВ-4Б1" необходимо исходить из следующих норм:

- 1) при установке на стену – один "СВ-4Б1" на каждые 15...25 м² площади поверхности стены (при этом излучатели должны устанавливаться на уровне половины высоты стены при высоте стены менее 5 м или на высоте от пола помещения не менее 2.5 м при высоте стены 5 м и более, далее – через каждые 5 м высоты);
- 2) при установке на потолок (пол) – один "СВ-4Б1" на каждые 15...25 м² плиты перекрытия;
- 3) при установке на оконный переплет - один "СВ-4Б1" на каждое окно или отдельную раму;
- 4) при установке на дверь – один "СВ-4Б1" на каждое полотно двери;
- 5) при установке на трубы систем водо-, тепло- или газоснабжения – один "СВ-4Б1" на каждую отдельную трубу перед выходом из помещения.

6) Ориентировочное количество "СВ-4Б" определяется из расчета: один "СВ-4Б" на каждый элемент остекления.

Вопросы:

1. Подобрать средства активной защиты. Описать состав комплекса защиты.
2. Нарисовать схему расстановки средств защиты при акустическом зашумлении.
3. Нарисовать схему расстановки средств защиты при вибрационном зашумлении.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.
2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НПЦ «Аналитика», 2017.

Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Элек-тронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:<http://biblioclub.ru/index.php?page=book&id=93349>.
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

Приложение Б.

Таблица П.4. Состав комплекса.

Обозначение на схеме	Полное наименование (комментарии)	ID
----------------------	-----------------------------------	----

электропитание и управление		
Блок питания и управления	"Соната-ИП4.1" ("Соната-ИП4.3"), универсальный блок питания и управления	309 (312)
Система виброакустической защиты (СВАЗ)		
СА-4Б	"СА-4Б" . Генератор-акустоизлучатель	956
СА-4Б1	"СА-4Б1" . Генератор-акустоизлучатель большой мощности	955
СВ-4Б	"СВ-4Б" . Генератор-вибровозбудитель	938
СВ-4Б1	"СВ-4Б1" . Генератор-вибровозбудитель пониженной шумности	937
Система защиты от утечек за счет побочных электромагнитных излучений и наводок (ПЭМИН)		
Соната-РЗ.1*)	"Соната-РЗ.1" Средство активной защиты информации от утечек за счет ПЭМИН (кл2)	232
Соната-РЗ*)	"Соната-РЗ" Средство активной защиты информации от утечек за счет ПЭМИН (кл1)	233
Соната-РСЗ	"Соната-РСЗ" Средство активной защиты информации от утечки за счет наводок информативного сигнала на сети электропитания и заземления	240
Система защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований		
Соната-ВК4.1	Размыкатель телефонной линии "Соната-ВК4.1"	975
Соната-ВК4.2	Размыкатель линий оповещения и сигнализации "Соната-ВК4.2"	976
Соната-ВК4.3	Размыкатель линий компьютерной сети "Соната-ВК4.3"	977
Блоки сопряжения с внешними устройствами**)		
Соната-ДУ4.1	Соната-СК4.1 . Силовой коммутатор нагрузок 220 В большой мощности, обратная связь, сухой контакт	530
Соната-ДУ4.2	"Соната-СК4.2", адаптер электропривода (окон), сухой контакт	531
Устройство дистанционного управления		
Проводной пульт управления	"Соната-ДУ4.1" ("Соната-ДУ4.3"), пульт управления комплексом ТСЗИ	523 (528)

*) Выбор устройства активной защиты информатизации от утечки каналам ПЭМИН Соната-РЗ или Соната-РЗ.1 зависит от требований к защите помещения (класс 1 или класс 2).

Практическое занятие № 3.

Тема: Разработка системы защиты от утечек за счет побочных электромагнитных излучений и наводок.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: угрозы информационной безопасности объектов информатизации; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.

Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

Теоретическая часть:

Естественные каналы утечки информации образуются за счёт побочных электромагнитных излучений, возникающих при обработке информации СВТ (электромагнитные каналы утечки информации), а также вследствие наводок информативных сигналов в линиях электропитания и заземления СВТ, соединительных линиях ВТСС и посторонних проводниках (электрические каналы утечки информации).

В **электромагнитных каналах утечки информации** носителем информации являются электромагнитные излучения (ЭМИ), возникающие при обработке информации техническими средствами. Основными причинами возникновения электромагнитных каналов утечки информации в ТСОИ являются побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСОИ.

Причинами возникновения **электрических каналов утечки информации** являются наводки информативных сигналов (под которыми понимаются токи и напряжения в токопроводящих элементах), вызванные побочными электромагнитными излучениями, ёмкостными и индуктивными связями.

Наводки информативных сигналов могут возникнуть:

- в линиях электропитания ТСОИ;
- в линиях электропитания и соединительных линиях ВТСС;
- в цепях заземления ТСОИ и ВТСС;
- в посторонних проводниках (металлических трубах систем отопления, водоснабжения, металлоконструкциях и т.д.).

Основными источниками возникновения ПЭМИ при работе СВТ являются:

- Процессор, шина данных процессора и цепи питания.
- Контроллеры и мост чипсета.

- Модули памяти и шина данных.
- Инверторы питания перечисленных выше устройств.
- HDD и шины IDE (ATA) и SATA.
- CD и шина IDE (ATA).
- Видеокарта и шина AGP или E-PCI.
- COM порт и внешние подключения по нему.
- LTP порт и внешние подключения по нему.
- USB порт.
- VGA и другие виды портов, предназначенные для подключения мониторов.
- Беспроводные сетевые адаптеры IEEE 802 для локальных сетей.



Рис 3.1 Основные источники возникновения ПЭМИ при работе СВТ

Понятие Электромагнитная наводка. Электромагнитная наводка – передача (индуцирование) электрических сигналов из одного устройства (цепи) в другое, непредусмотренная схемными или конструктивными решениями и возникающая за счет паразитных электромагнитных связей. Электромагнитные наводки могут приводить к утечке информации по токопроводящим коммуникациям, имеющим выход за пределы контролируемой зоны.

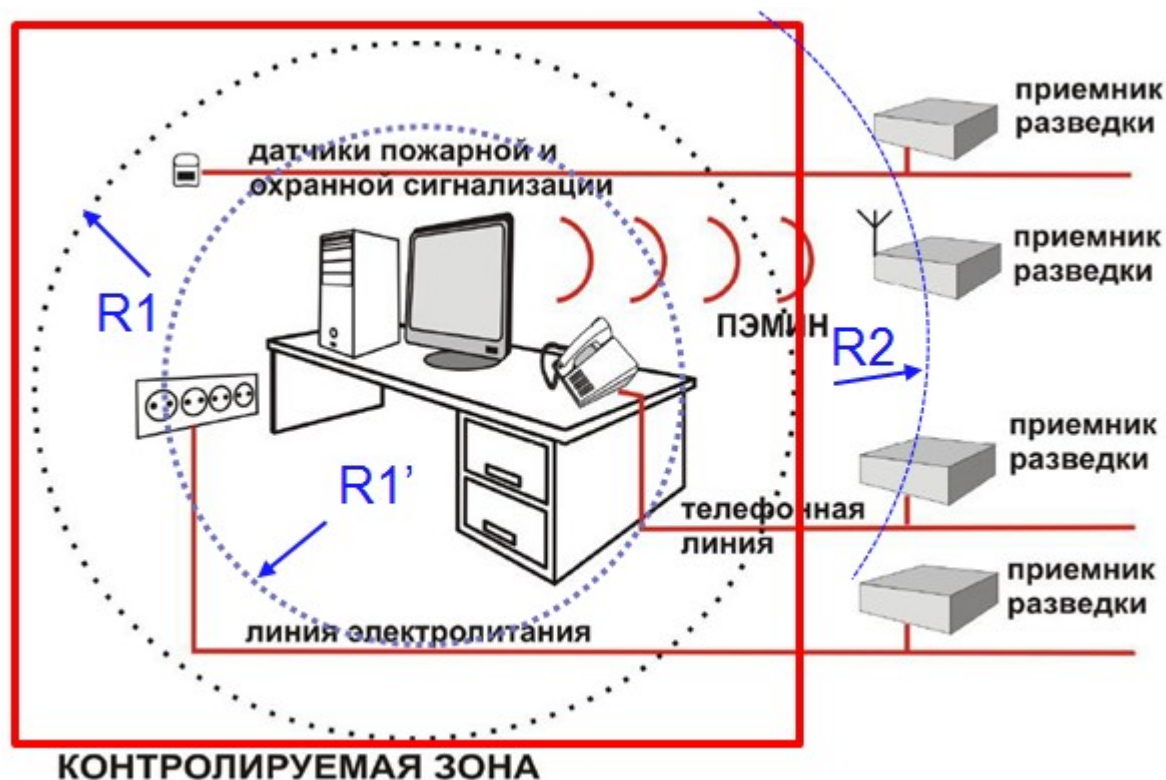


Рис 3.2 Радиусы опасных зон для перехвата информативных сигналов

В зависимости от физических причин возникновения наводки информативных сигналов можно разделить на:

- наводки информативных сигналов в электрических цепях ТСОИ, вызванные информативными ПЭМИ ТСОИ;
- наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными ПЭМИ ТСОИ;
- наводки информативных сигналов в электрических цепях ТСОИ, вызванные внутренними ёмкостными и индуктивными связями (“просачивание” информативных сигналов в цепи электропитания через блоки питания ТСОИ);
- наводки информативных сигналов в цепях заземления ТСОИ, вызванные информативными ПЭМИ ТСОИ, а также гальванической связью схемной (рабочей) земли и блоков ТСОИ.

Отсюда:

- **r1** - минимальный радиус зоны для устройства ВТСС, линии которых имеют выход за границы контролируемой зоны.
- **r1'** - минимальный радиус зоны для линий и кабелей ВТСС, имеющие выход за границы контролируемой зоны.

Система защиты от утечек за счет побочных электромагнитных излучений и наводок (ПЭМИН). Реализация пассивных методов защиты, основанных на применении экранирования и фильтрации, приводит к ослаблению уровней побочных электромагнитных излучений и наводок (опасных сигналов) ТСПИ и тем самым к уменьшению отношения опасный сигнал/шум (с/ш), рисунок 11. Однако в ряде случаев, несмотря на применение пассивных методов защиты, на границе контролируемой зоны отношение с/ш превышает

допустимое значение. В этом случае применяются активные меры защиты, основанные на создании помех средствам разведки, что также приводит к уменьшению отношения с/ш.

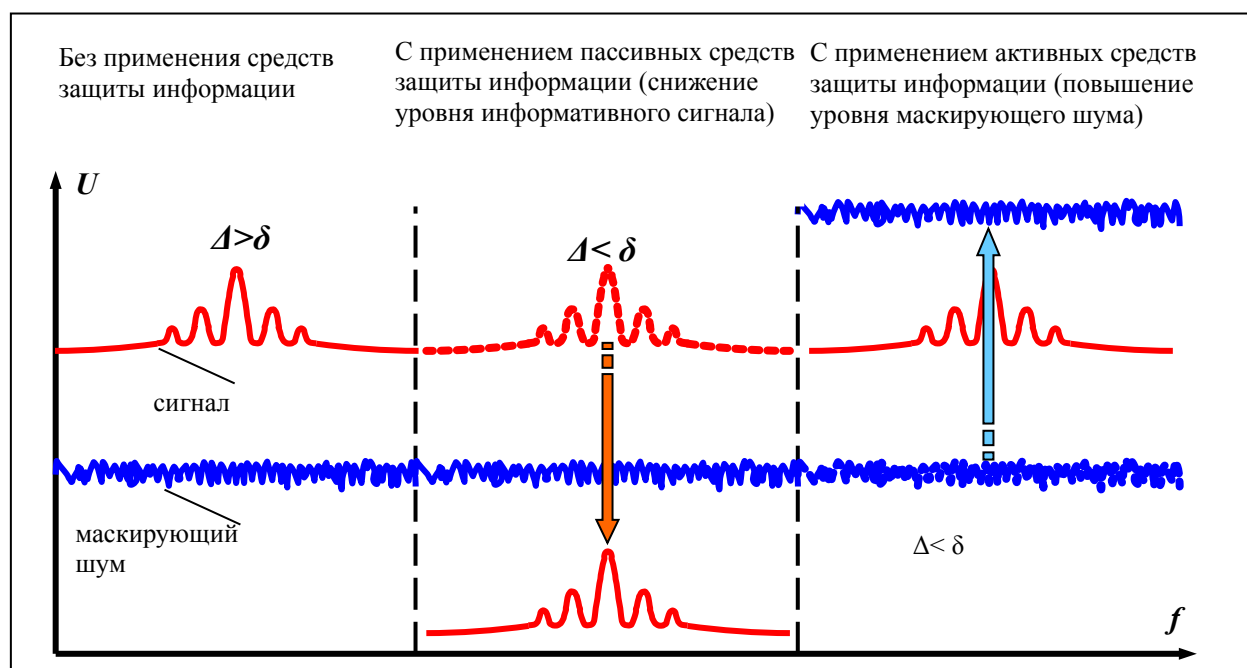


Рисунок 3.3 - Физические основы пассивных и активных методов защиты информации

1. Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется **пространственное зашумление**, схема представлена на рисунке.

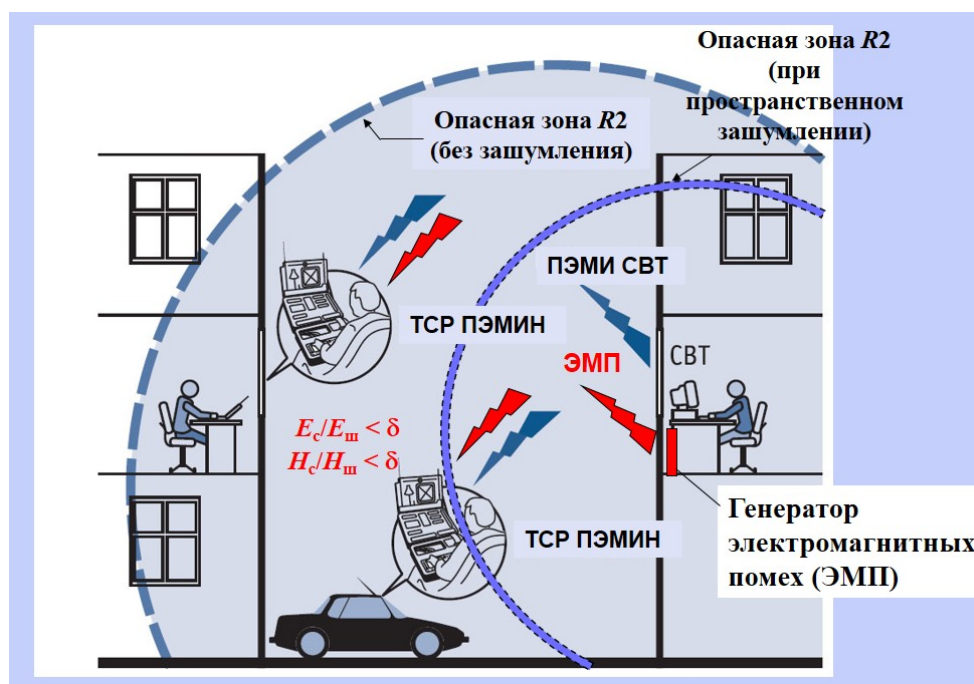


Рис 3.4– схема пространственного электромагнитного зашумления

К системе пространственного зашумления, применяемой для создания маскирующих электромагнитных помех, предъявляются следующие требования:

- система должна создавать электромагнитные помехи в диапазоне частот возможных побочных электромагнитных излучений ТСПИ;
- создаваемые помехи не должны иметь регулярной структуры, генерируемый шум должен иметь нормальное распределение плотности вероятности мгновенных значений амплитуд компонентов E (H , U) по отношению к нормальному (Гауссовскому) шуму не ниже заданных;
- уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечить отношение с/ш на границе контролируемой зоны меньше допустимого значения во всем диапазоне частот возможных побочных электромагнитных излучений ТСПИ;
- система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией (поэтому выбору антенн для генераторов помех уделяется особое внимание).

В настоящее время в основном применяются системы пространственного зашумления, использующие помехи типа "белый шум", то есть излучающие широкополосный шумовой сигнал (как правило, с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот), существенно превышающий уровни побочных электромагнитных излучений. Такие системы применяются для защиты широкого класса технических средств: электронно-вычислительной техники, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения и т.д.

2. Защита объектов ВТСС от утечки информации, возникающей за счет наводок побочных электромагнитных излучений, достигается: установкой помехоподавляющих фильтров в цепях электропитания ТСПИ, диэлектрических вставок в инженерные коммуникации и экраны кабелей электропитания, а также использованием систем **линейного электромагнитного зашумления**.

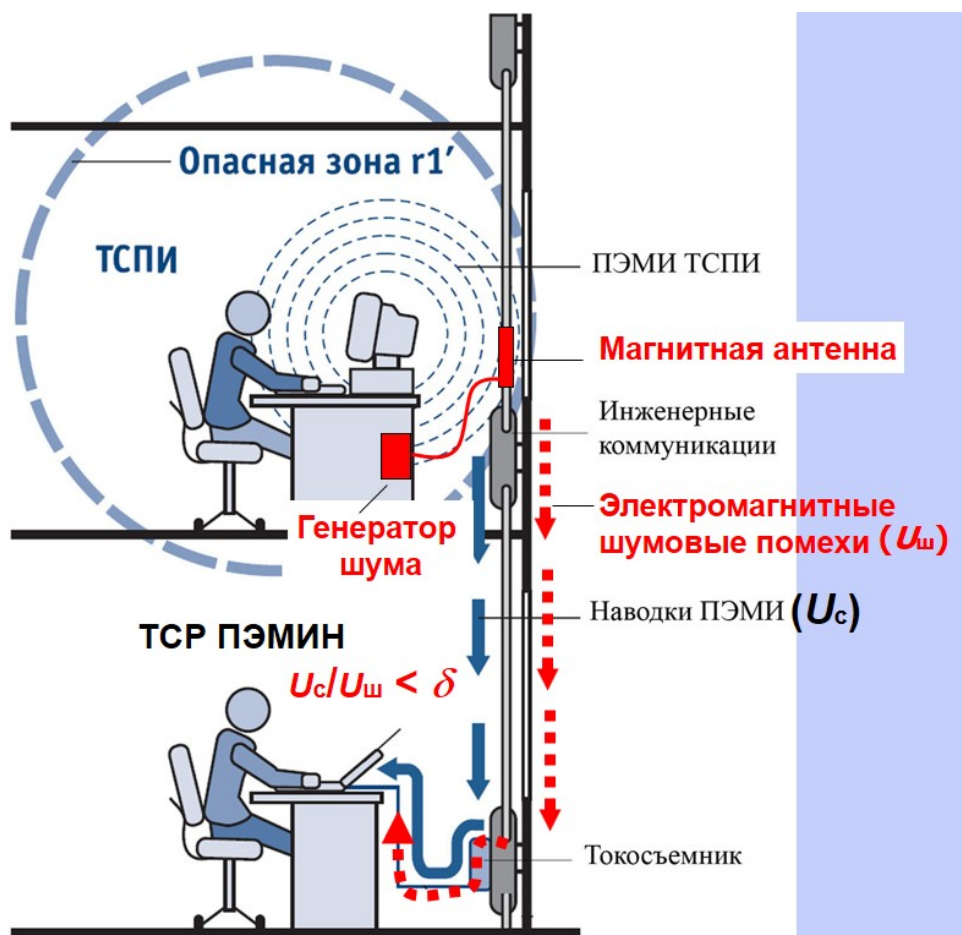


Рис 3.5 – Схема создания шумовых помех в системе отопления

Генератор шума «ГШ-1000У» предназначен для маскировки побочных информативных электромагнитных излучений и наводок персональных компьютеров, компьютерных сетей и комплексов в диапазоне частот 0,1-1800 МГц путем формирования и излучения в окружающее пространство маскирующего электромагнитного поля шума. Внешний вид устройства представлен на рисунке 3.6.



Рисунок 3.6 – внешний вид генератора шума ГШ-1000У

Дополнительно имеет 4 независимых коаксиальных выхода некоррелированного напряжения шума, к которым можно подключать:

- устройства ввода маскирующего напряжения шума (например, ответвитель «Дух») в сети электропитания, заземления, инженерные коммуникации и т.д.;
- дополнительные выносные антенны.



Рис 3.7 Внешний вид и способ крепления ответвителя «Дух»

Средство активной защиты информации "Соната-РЗ.1" предназначено для защиты информации от утечки за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие проводные коммуникации. "Соната РЗ.1" обеспечивает защиту путем излучения в окружающее пространство электромагнитное поле шума, а также инъекции шумовых токов в линии сети электропитания и заземления.

Изделие может быть включено в состав комплекса ТСЗИ. В этом случае управление его работой и контроль режима работы (исправности) будет осуществляться от пульта управления "Соната-ДУ4.1" в комплексе с блоком питания "Соната-ИП4.х" (Комплекс 3095).



Соната-Р3.1



Соната-Р3.1
с дополнительной антенной

Рисунок 3.8 – Внешний вид устройства "Соната-РЗ.1"



Рисунок 3.9 – Внешний вид Пульта управления "Соната-ДУ 4.2"

Средство активной защиты информации от утечки за счет наводок информативного сигнала на цепи заземления и электропитания "Соната-РС3" (далее Изделие) предназначено для защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет наводок информативного сигнала на цепи заземления и электропитания и может устанавливаться в выделенных помещениях до 1 категории включительно.

INCLUDEPICTURE "http://npoanna.ru/Data/Uploads/Images/new/r/r s3/rs3new.jpg" * MERGEFORMATINET INCLUDEPICTURE "http://npoanna.ru/Data/Uploads/Images/new/r/r s3/rs3tail.jpg" * MERGEFORMATINET
INCLUDEPICTURE "http://npoanna.ru/Data/Uploads/Images/new/r/r s3/rs3new.jpg" * MERGEFORMATINET INCLUDEPICTURE "http://npoanna.ru/Data/Uploads/Images/new/r/r s3/rs3tail.jpg" * MERGEFORMATINET



Рисунок 3.10 – Внешний вид устройства «Соната-РС3» спереди и сзади

Особенности конструкции устройств позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники (СВТ).

Вариант установки устройства «Соната-РС3» на объекте ВП с одним вводом линии 220В на рис. 3.11.

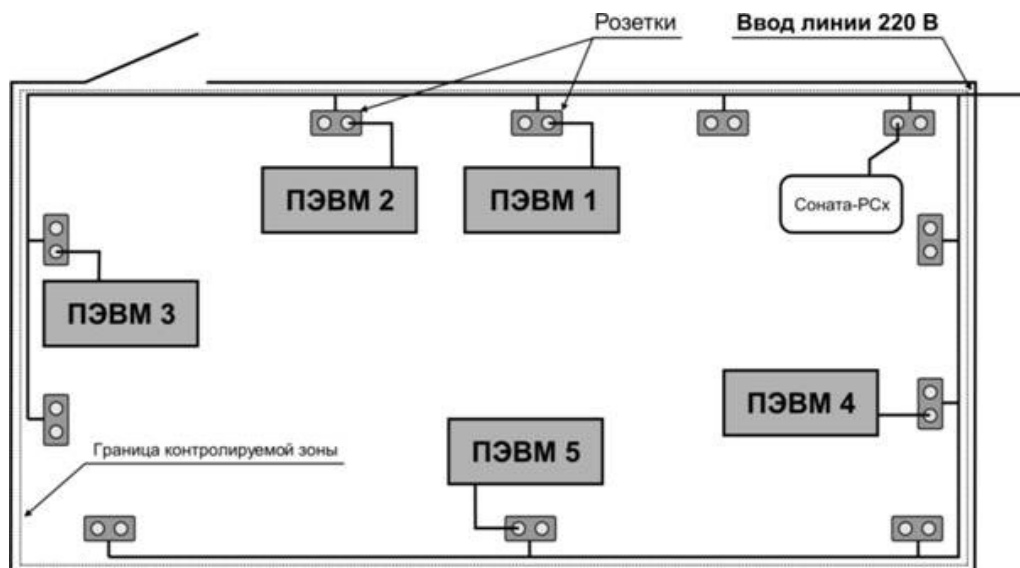


Рисунок 3.11 - Вариант установки устройства «Соната-РС3» на объекте ВП с одним вводом линии 220В

Вариант установки устройства «Соната-РС3» на объекте ВП с двумя вводами линий 220В на рис. 3.12.

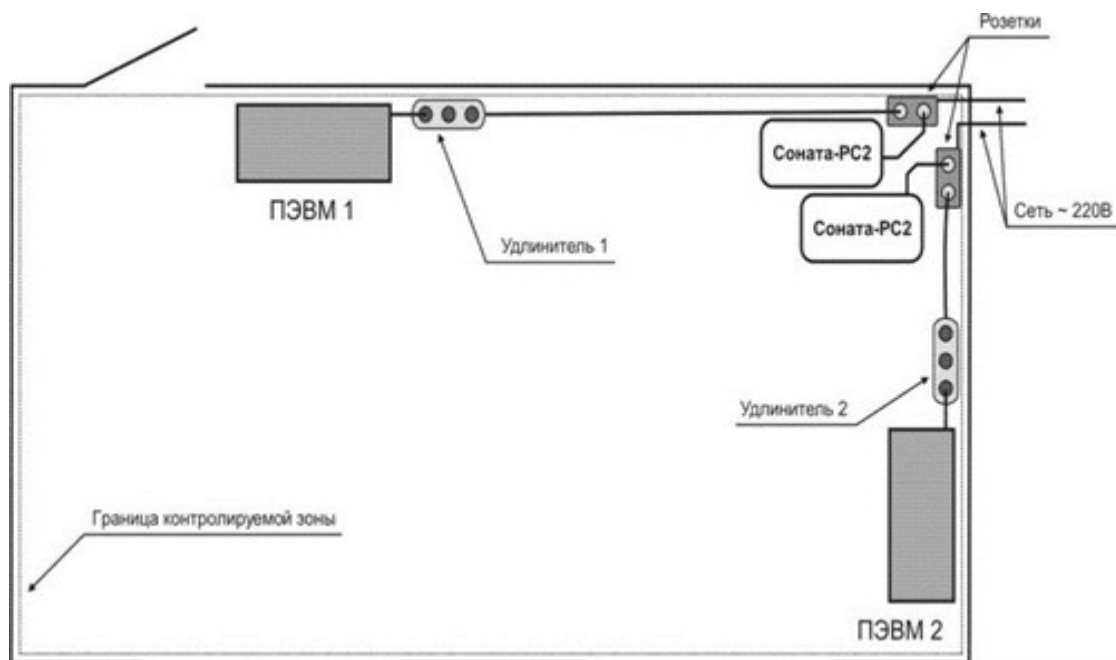


Рисунок 3.12 - Вариант установки устройств «Соната-РС3» на объекте ВП с двумя вводами линий 220В

Вопросы:

1. Описать системы защиты от утечек за счет побочных электромагнитных излучений и наводок (ПЭМИН).
2. Подобрать средства для пространственного зашумления.
3. Подобрать средства для линейного зашумления.
4. Нарисовать схему расстановки средств защиты от утечек за счет ПЭМИН.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб. пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.
2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НПЦ «Аналитика», 2017.

Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Элек-тронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:<http://biblioclub.ru/index.php?page=book&id=93349>.
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

Практическое занятие № 4.

Тема: Разработка системы защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: угрозы информационной безопасности объектов информатизации; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.

Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

Теоретическая часть:

Проектирование системы защиты акустической речевой информации, как и любой другой, должно опираться на исходные данные.

На рисунке 1 показана схема расположения линий ВТСС со стороны окна. Измерения напряжения в канале НЧ АЭП проводились на контактах всех устройств ВТСС в рабочем режиме и в режиме холостого хода.

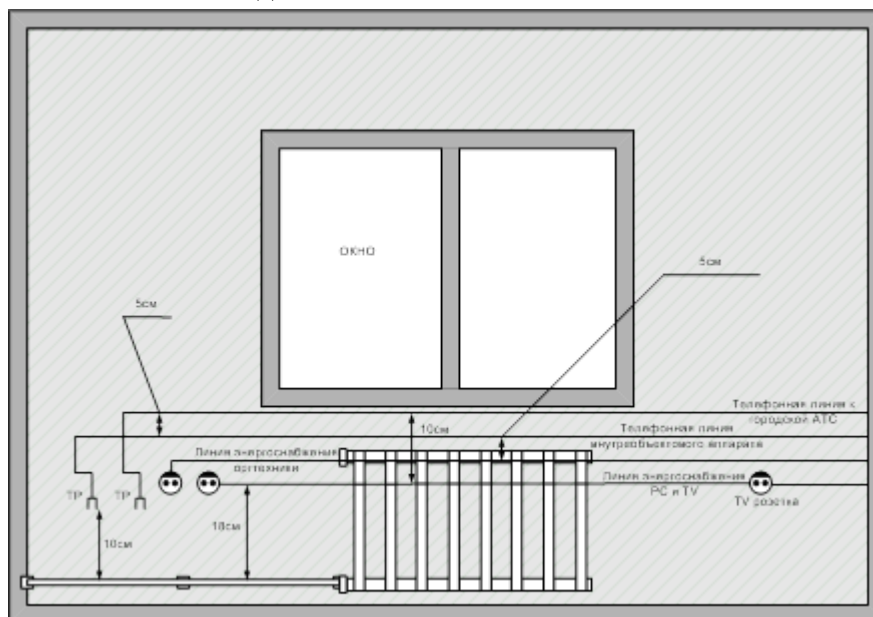


Рисунок 1 – Схема расположения линий ВТСС со стороны окна

При проведении измерений было выявлено превышение показателей противодействия относительно нормированных показателей.

Система защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований.

Технические меры сводятся к включению в линию связи специальных устройств локализации микрофонного эффекта. Размыкатели слаботочных линий “Соната-ВК4.1” предназначены для защиты информации от утечки за счет акустоэлектрических преобразований и ВЧ-навязывания по телефонным линиям, “Соната-ВК4.2” по соединительным линиям систем оповещения и сигнализации, а “Соната-ВК4.3” по линиям компьютерных сетей.

INCLUDEPICTURE "http://npoanna.ru/Data/Uploads/Images/new/vk/vk4-2.jpg" *
MERGEFORMATINET INCLUDEPICTURE



Рисунок 16 – Внешний вид устройства Соната-ВК4.2

Таблица 5. Основные технические характеристики размыкателей “Соната-ВКх”

Параметр	Соната-ВК4.1	Соната-ВК4.2	Соната-ВК4.3
Проводность линии		4-х	8-ми
Параметры коммутируемой линии	Аналоговая телефонная линия	Коммутируемое напряжение/сила тока/мощность, не более – 125В/2А/30Вт(30В*А)	Кабельные линии (УТри аналоги) компьютерной сети стандарта Ethernet10/100

Размыкатели "Соната-ВК4.1", "Соната-ВК4.2", "Соната-ВК4.3" могут применяться с блоком питания и управления "Соната-ИП4.х" совместно с пультом управления и в составе комплексов ТСЗИ.

Вопросы:

1. Описать систему защиты от утечек за счет АЭП.
2. Подобрать устройства локализации микрофонного эффекта.
3. Нарисовать схему расстановки средств защиты от утечек за счет АЭП.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.
2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НПЦ «Аналитика», 2017.

Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Элек-тронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:<http://biblioclub.ru/index.php?page=book&id=93349>.

2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/
А. Ф. Чипига- М.: Гелиос АРВ, 2013.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению лабораторных работ
по дисциплине
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Комплексная защита объектов информатизации**

Пятигорск, 2024 г.

СОДЕРЖАНИЕ

	Стр.
Введение	5
Лабораторная работа № 1. «Обнаружение скрытых видеокамер с помощью поискового прибора «Оптик»»	8
Лабораторная работа № 2. «Качественная оценка утечки речевой информации по акустическим каналам с помощью многофункционального поискового прибора «Спайдер»»	14
Лабораторная работа № 3. «Качественная оценка утечки речевой информации по виброакустическому каналу с помощью многофункционального поискового прибора «Спайдер»»	27
Лабораторная работа № 4. Тема: «Количественная оценка защищенности речевой информации по акустическому каналу через двери с использованием ПАК «Шёпот»»	35

Введение.

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Существует множество причин и мотивов, по которым одни люди хотят шпионить за другими. Имея немного денег и старание, злоумышленники могут организовать ряд каналов утечки сведений, используя собственную изобретательность и (или) халатность владельца информации. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Для построения системы надежной защиты информации необходимо выявить все возможные угрозы безопасности, оценить их последствия, определить необходимые меры и средства защиты, оценить их эффективность. Оценка рисков производится квалифицированными специалистами с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации. На основании результатов анализа выявляются наиболее высокие риски, переводящих потенциальную угрозу в разряд реально опасных и, следовательно, требующих принятия дополнительных мер обеспечения безопасности.

Информация может иметь несколько уровней значимости, важности, ценности, что предусматривает соответственно наличие нескольких уровней ее конфиденциальности. Наличие разных уровней доступа к информации предполагает различную степень обеспечения каждого из свойств безопасности информации – конфиденциальность, целостность и доступность.

Анализ системы защиты информации, моделирование вероятных угроз позволяет определить необходимые меры защиты. При построении системы защиты информации необходимо строго соблюдать пропорцию между стоимостью системы защиты и степенью ценности информации. И только

располагая сведениями о рынке открытых отечественных и зарубежных технических средств несанкционированного съема информации, возможно определить необходимые меры и способы защиты информации. Это одна из самых сложных задач в проектировании системы защиты коммерческих секретов.

При возникновении различных угроз от них приходится защищаться. Для того чтобы оценить вероятные угрозы, следует перечислить и основные категории источников конфиденциальной информации – это могут быть люди, документы, публикации, технические носители, технические средства обеспечения производственной и трудовой деятельности, продукция, промышленные и производственные отходы и т. д. Кроме того, к возможным каналам утечки информации следует отнести совместную деятельность с другими фирмами; участие в переговорах; фиктивные запросы со стороны о возможности работать в фирме на различных должностях; посещения гостей фирмы; знания торговых представителей фирмы о характеристиках изделия; излишнюю рекламу; поставки смежников; консультации специалистов со стороны; публикации в печати и выступления, конференции, симпозиумы и т. д.; разговоры в нерабочих помещениях; правоохранительные органы; «обиженных» сотрудников предприятия и т. п.

Все возможные способы защиты информации сводятся к нескольким основным методикам:

- воспрепятствование непосредственному проникновению к источнику информации с помощью инженерных конструкций технических средств охраны;
- скрывание достоверной информации;
- предоставление ложной информации.

Упрощенно принято выделять две формы восприятия информации – акустическую и зрительную (сигнальную). Акустическая информация в потоках сообщений носит преобладающий характер. Понятие зрительной информации весьма обширно, поэтому ее следует подразделять на объемно-

видовую и аналогово-цифровую.

Самыми распространенными способами несанкционированного получения конфиденциальной информации являются:

- прослушивание помещений с помощью технических средств;
- наблюдение (в т. ч. фотографирование и видеосъемка);
- перехват информации с использованием средств радиомониторинга информативных побочных излучений технических средств;
- хищение носителей информации и производственных отходов;
- чтение остаточной информации в запоминающих устройствах системы после выполнения санкционированного запроса, копирование носителей информации;
- несанкционированное использование терминалов зарегистрированных пользователей с помощью хищения паролей;
- внесение изменений, дезинформация, физические и программные методы разрушения (уничтожения) информации.

Современная концепция защиты информации, циркулирующей в помещениях или технических системах коммерческого объекта, требует не периодического, а постоянного контроля в зоне расположения объекта. Защита информации включает в себя целый комплекс организационных и технических мер по обеспечению информационной безопасности техническими средствами. Она должна решать такие задачи, как:

- предотвращение доступа злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения;
- защита носителей информации от уничтожения в результате различных воздействий;
- предотвращение утечки информации по различным техническим каналам.

Способы и средства решения первых двух задач не отличаются от способов и средств защиты любых материальных ценностей, третья задача решается исключительно способами и средствами инженерно-технической

защиты информации.

Лабораторная работа № 1

Тема: «Обнаружение скрытых видеокамер с помощью поискового прибора «Оптик»»

Цель работы: изучить методику поиска объективов скрытых видеокамер.

1. Теоретическая часть

Описание прибора «Оптик»

Профессиональный обнаружитель скрытых видеокамер «Оптик» предназначен для поиска и локализация скрытых (камуфлированных в интерьер) видеокамер типа «пинхол» независимо от их состояния (включено/выключено) и типа передачи видеосигнала.

Поиск объектива видеокамеры методом световой локации.

При обнаружении объектива скрытой камеры в объективе прибора «Оптик» будет наблюдаться точечное пятно зелёного или красного цвета – результат отражения подсветки от видеокамеры. Технические характеристики прибора представлены в таблице 1.

Таблица 1.

№ п/п	Параметр	Значение
1.	Дальность обнаружения: (зависит от световой обстановки (освещённости помещения))	от 0,5 до 50 метров
2.	Угол обзора:	7,5 градусов
3.	Кратность	6,5х

4.	Диапазон фокусировки:	от 0,5 метра до ∞
5.	Режим работы:	- непрерывный зелёный - непрерывный красный - импульсный зелёный - импульсный красный - импульсный красно-зелёный
6.	Тип питания:	Li-ion аккумулятор 3,7 В
7.	Вид подсветки:	светодиодная
8.	Количество светодиодов	22 шт.
9.	Цвет подсветки	зелёная, красная, красно/зелёная
10.	Масса прибора (грамм)	450 гр.
11.	Масса прибора в транспортной сумке, с зарядным устройством	800 гр.
12.	Время работы (при полностью заряженном аккумуляторе)	- в импульсном режиме при работе красно/зелёной подсветки: не менее 4-х часов - в непрерывном режиме: не менее 6-ти часов

ВНИМАНИЕ: прибор работает от встроенного аккумулятора, установленного на предприятии изготовителе. Заряд аккумулятора прибора осуществляется от зарядного устройства (5 В, 0,6 А) из комплекта поставки. Заряд осуществляется при выключенном приборе. Полностью разряженный прибор заряжается в течение 4 часов.

Вставьте зарядное устройство в сеть 220 В (50 Гц). Светодиод на зарядном устройстве должен загореться красным цветом при подключении к сети 220 В.

Подключите штекер зарядного устройства в разъем прибора с надписью +5v. При подключении загорится индикатор CNG на приборе, подтверждающий начало заряда. Светодиод на зарядном устройстве при заряде горит красным цветом.

По окончании заряда на приборе погаснет индикатор CNG.

Отключите зарядное устройство от прибора, затем, от сети 220 В.



Рис. 1

Прибор готов к работе.

Порядок работы с прибором

Работа с прибором заключается в равномерном осмотре с его помощью проверяемого помещения.

Для обнаружения видеокамеры необходимо находиться в том месте, которое предположительно является объектом скрытого видеонаблюдения. Если ходить по помещению и просто осматривать интерьер через «Оптик-2», камера может быть не обнаружена.

Например, если предполагается ведение скрытого видеоконтроля стола руководителя, необходимо сесть в кресло руководителя и вести поиск именно с этой точки.

При обнаружении бликующего точечного пятна необходимо осмотреть это место с близкого расстояния и определить источник блика.

Основной режим работы прибора – непрерывный. Импульсный режим является дополнительным и используется при проверке в обычной световой обстановке. В затемнённом помещении рекомендуется использовать непрерывный режим.

На рис. 2 показан пример выявленной видеокамеры

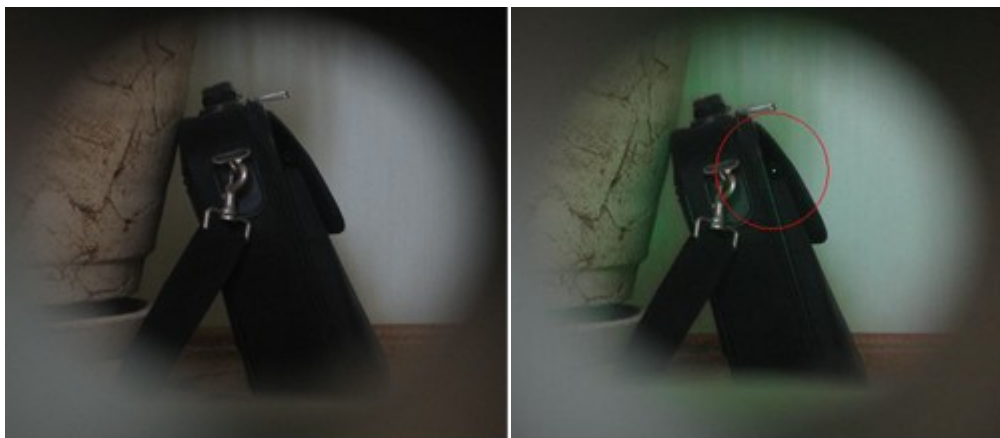


Рис. 2 - Пример выявления видеокамеры

Рекомендации по поиску скрытых камер

Основным правилом при обнаружении скрытых камер является необходимость находиться в месте, которое вероятнее всего интересует лиц, установивших камеру (или между предполагаемым местом установки видеокамеры и местом съёмки).

Вероятнее всего такими местами являются: места работы (столы с сидящими за ними людьми), места отдыха (кресла, диваны, кровати). В случае если интерес может представлять, посещало ли то или иное лицо помещение – камера может быть направленно на дверной проём.

Необходимо учитывать, что видеокамер может быть несколько. Обнаружение одной или двух видеокамер не даёт право сделать вывод, что помещение проверено. Для этого необходимо проверить все места, из которых возможен видеоконтроль.

Наиболее сложен поиск в помещениях с большим количеством бликующих объектов – большое количество зеркал, стекла и т.д. В случае обнаружения блика, мешающего осмотру какой-либо поверхности, необходимо сменить угол под которым осматривается поверхность. Зачастую достаточно переместиться на шаг и блик исчезнет. При этом блик от объектива останется.

Необходимо при проверке помещений стараться не стоять под прямым углом к бликующей поверхности.

Видеокамеры могут быть установлены в любую деталь интерьера, подходящую для такой установки. Это может быть подвесной потолок, видео- и аудиоаппаратура, картины, декоративные украшения и т.д.

Поиск значительно облегчается и яркость видимого пятна от засветки объектива возрастает, если в помещении нет прямых солнечных лучей. Нет необходимости «делать темноту» - достаточно создать нормальную для работы световую обстановку. При необходимости можно работать и практически в сторону Солнца, но при этом глаз оператора способен различить пятно объектива с 1-2 метров.

Данные рекомендации справедливы при работе с любым обнаружителем скрытых видеокамер, работающим по принципу обнаружения бликующих объектов.

Правила техники безопасности

Внимание! В приборе установлены стеклянные оптические элементы. В случае разбития любого из них запрещается эксплуатация прибора во избежание получения травм.

Не наводить включенную подсветку на глаза людей. Кратковременная засветка глаз безопасна.

Избегать попадания прямых солнечных лучей и нагрева прибора.

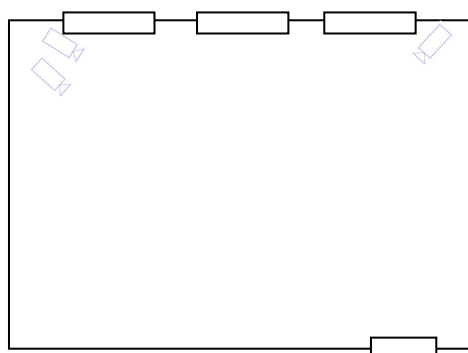
Не разбирать и не бросать прибор.

Не оставлять на длительное время под воздействием низких температур – прибор предназначен для работы в обычных помещениях при температуре от +5 до +40 градусов Цельсия

Для чистки загрязненной оптики используйте только салфетки, предназначенные для протирки оптических устройств.

2. Задание.

- 1) Произвести визуальный осмотр защищаемого помещения.
- результат (кол-во в/камер);
- 2) Произвести осмотр помещения с помощью профессионального обнаружителя скрытых видеокамер «Оптик».
- результат (кол-во в/камер);
- 3) Отобразить результаты осмотра на схеме исследуемого помещения.



- 4) Сделать выводы.
- 5) Ответить на вопросы.

5. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, студента, курс, группа, проверил: преподаватель ФИО.

6. Вопросы для самоконтроля:

- 1) по какому принципу работает обнаружитель?
- 2) какова дальность обнаружения прибора?
- 3) при каких условиях облегчается поиск скрытых видеокамер?

Лабораторная работа № 2

Тема: Качественная оценка утечки речевой информации по акустическому каналу с помощью многофункционального поискового прибора «Спайдер»

Цель лабораторного практикума: отработка навыков проведения исследований по выявлению утечки речевой информации по акустическому каналу.

Задачи лабораторного практикума:

- изучить поисковое оборудование и приобрести навыки работы с ним;
- закрепить знание существующей методики проведения качественной оценки утечки речевой информации по акустическим каналам;
- отработать навыки практического применения методики качественной оценки утечки речевой информации по акустическим каналам.

1. Теория.

Для качественного решения задач аттестационных испытаний необходимо обладать теоретическими знаниями в разных областях науки – акустики и виброакустики, спектрального анализа, антенно-фидерных устройств, законов распространения электромагнитных колебаний, нормативно-правовых актов и руководящих документов по защите выделенных помещений и средств вычислительной техники, метрологии и т.д. Кроме того, специалист по аттестации объектов информатизации должен обладать умениями и практическими навыками применения инструментальных средств контроля защищенности информации, навыками использования специализированных средств сетевого и системного сканирования, установки, настройки и администрирования средств защиты информации, навыками работы с контрольно измерительной аппаратурой, навыками проведения измерений и т.п.

К основным угрозам безопасности защищаемой информации относятся: несанкционированное распространение сведений (утечка информации) и несанкционированное целенаправленное или непреднамеренное воздействие на информацию или ее носитель.

Доступ к защищаемой информации с применением технических средств разведки часто называют техническим каналом утечки информации, под которым понимают совокупность объекта разведки, на котором обрабатывается защищаемая информация, среды распространения информационных сигналов и технического средства разведки (ТСР), с помощью которого регистрируются, измеряются и анализируются перехватываемые сигналы.

Под акустической информацией обычно понимается информация, носителями которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой. Первичными источниками акустических сигналов являются механические колебательные системы, например органы

речи человека, а вторичными - преобразователи различного типа, например, громкоговорители.

В акустических измерениях в качестве измеряемой величины наиболее часто используется звуковое давление L . Звуковое давление - это избыточное давление, возникающее в упругой среде при прохождении через нее звуковой волны. Если в качестве упругой среды рассматривать воздушную среду, то звуковое давление - это среднеквадратическое отклонение давления относительно атмосферного давления (рис. 2.1).

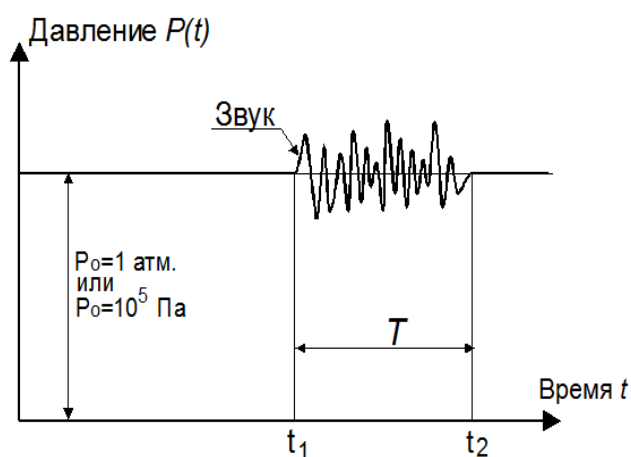


Рис. 2.1. Изменение давление в воздушной среде при возникновении звука

$$L = \sqrt{\frac{1}{T} \int_{t_1}^{t_2} (P(t) - P_0)^2 dt}$$

Обычно при проведении измерений время интегрирования T составляет 30-60с и более.

Для обсуждения информации ограниченного доступа (совещаний, обсуждений, конференций, переговоров и т.п.) используются специальные помещения (служебные кабинеты, актовые залы, конференц-залы и т.д.), которые называются *защищаемыми помещениями (ЗП)*.

Перехват речевой информации из ЗП возможен по акустическому, каналу с применением различных технических средств акустической разведки, к которым относятся направленные микрофоны (см. табл. 2.1).

Таблица 2.1.

Потенциальные технические каналы утечки речевой информации

Технические каналы утечки информации	Специальные технические средства речевой разведки, используемые для перехвата информации
Акустический (через щели, окна, двери, технологические проемы, вентиляционные каналы и т.д.)	• направленные микрофоны, установленные в близлежащих строениях и транспортных средствах, находящихся за границей КЗ; • специальные высокочувствительные микрофоны установленные в воздуховодах или в смежных помещениях, принадлежащих другим организациям (<u>несанкционированное целенаправленное прослушивание</u>).
	• прослушивание разговоров, ведущихся в ЗП, без применения технических средств посторонними лицами (посетителями, техническим персоналом), при их нахождении в коридорах и смежных с ЗП (<u>непреднамеренное прослушивание</u>).

Из практических соображений может быть установлена некоторая шкала оценок качества перехваченного речевого сообщения:

1) Перехваченное речевое сообщение содержит количество правильно понятых слов, достаточное для составления подробной справки о содержании перехваченного разговора.

2) Перехваченное речевое сообщение содержит количество правильно понятых слов, достаточное только для составления краткой справки-аннотации, отражающей предмет, проблему, цель и общий смысл перехваченного разговора.

3) Перехваченное речевое сообщение содержит отдельные правильно понятые слова, позволяющие установить предмет разговора.

4) При прослушивании фонограммы перехваченного речевого сообщения возможно установить факт наличия речи, но нельзя установить предмет разговора.

5) При прослушивании фонограммы перехваченного речевого сообщения невозможно установить факт наличия речи.

Практический опыт показывает, что составление подробной справки о содержании перехваченного разговора невозможно при словесной разборчивости менее 70 – 80 %, а краткой справки-аннотации – при словесной разборчивости менее 40 – 60 %. При словесной разборчивости менее 20 – 40 % значительно затруднено установление даже предмета ведущегося разговора, а при словесной разборчивости менее 10 – 20 % - это практически невозможно. При словесной разборчивости менее 10 % значительно затруднено определение в перехваченном сообщении признаков речи.

2. Методика выбора контрольных точек

Методики выбора контрольных точек для проведения измерений не существует, однако по многолетнему опыту организации, выполняющей специальные исследования, можно сформулировать следующие общие рекомендации. Будем считать, что средства активной защиты отсутствуют.

На вертикальных ограждающих конструкциях (стены, окна, двери) контрольные точки (КТ) размещаются на высоте $H=1,5\text{м}$. На каждые два погонных метра стены намечается одна контрольная точка, на дверь - одна контрольная точка, на каждую фрамугу окна - одна контрольная точка.

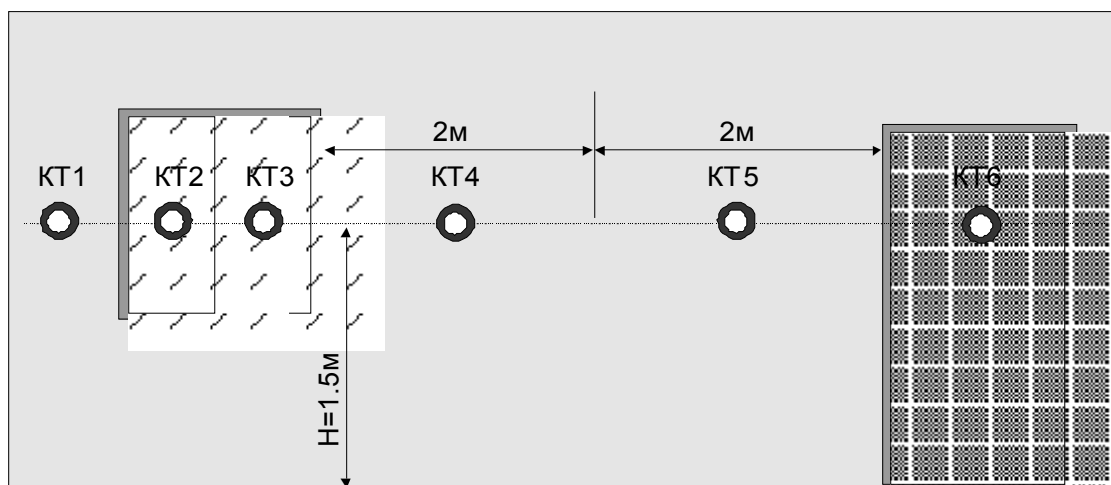


Рисунок 2.2 - Размещение КТ на вертикальных ограждающих конструкциях

Примечание: При наличии трещин и изгибов стен, выставляются дополнительные контрольные точки для устранения утечки.

Контрольные точки для проведения акустических измерений намечаются в центре каждой поверхности оконного остекления.

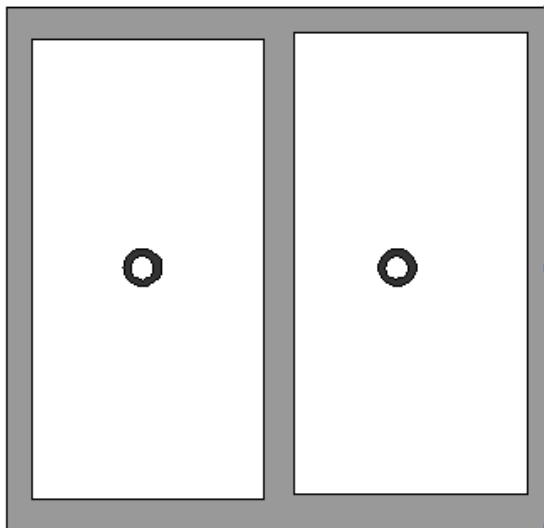


Рисунок 2.3 - Размещение контрольных точек на поверхности оконного остекления для акустических измерений

При проведении акустических исследований в воздуховоде, микрофон для устанавливается в непосредственной близости от ближайшего выхода воздуховода из защищаемого помещения.

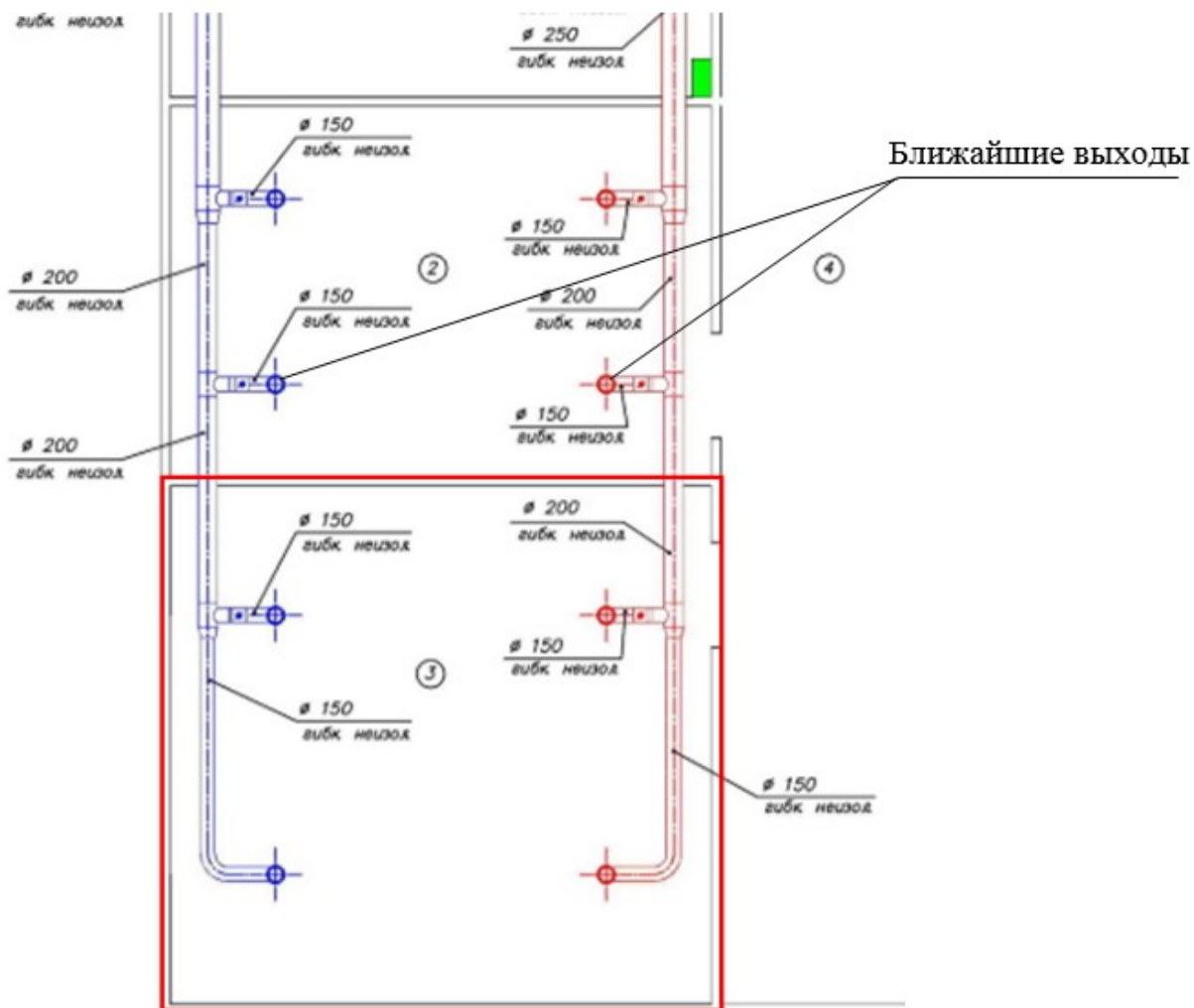


Рисунок 2.4 - Размещение точек выхода для акустических измерений на воздуховодах

На горизонтальных ограждающих конструкциях (перекрытиях) на каждые 2м намечается одна контрольная точка. Если перекрытие состоит из плит, то места размещения КТ определяются на примыканиях плит.

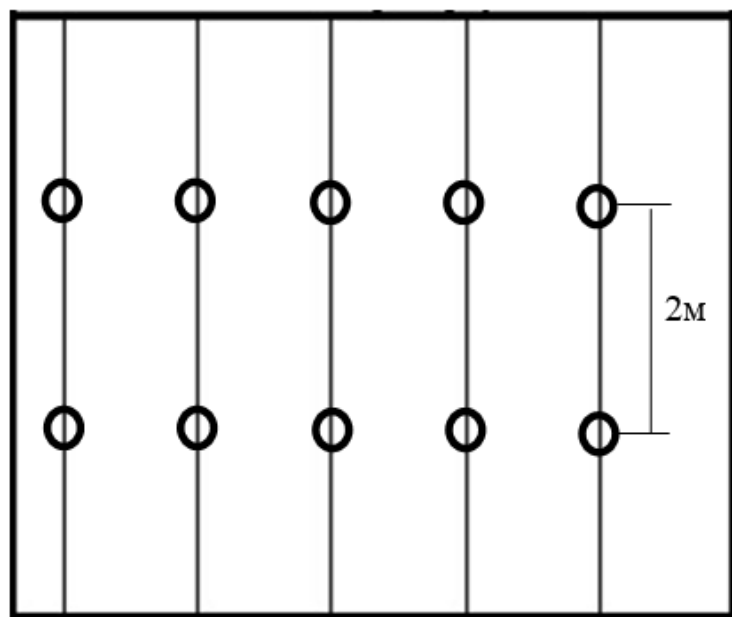


Рисунок 2.5 - Размещение контрольных точек на горизонтальных конструкциях для акустических измерений

Местоположение контрольных точек отображается на план-схеме исследуемого помещения. Утвержденной системы обозначения контрольных точек не существует. Рекомендуется следующий вариант обозначения:

- Первые две-три буквы (цифры) – объект измерений (ограждающая конструкция, инженерно-техническое средство);
- _А – акустические измерения, _В - вибрационные измерения;
- _цифра – номер контрольной точки.

Например, Ст4_А_4 означает – контрольная точка на стене №4 в которой проводятся акустические измерения, номер контрольной точки «4».

2.3 Инструментальное исследование

Качественную оценку утечки речевой информации по акустическим каналам будем осуществлять с помощью multifunctional поискового прибора «Спайдер».

Описание поискового прибора «Спайдер».

Органы управления и индикации.



Рисунок 2.6 – Многофункциональный поисковой прибор «Спайдер» (лицевая часть).

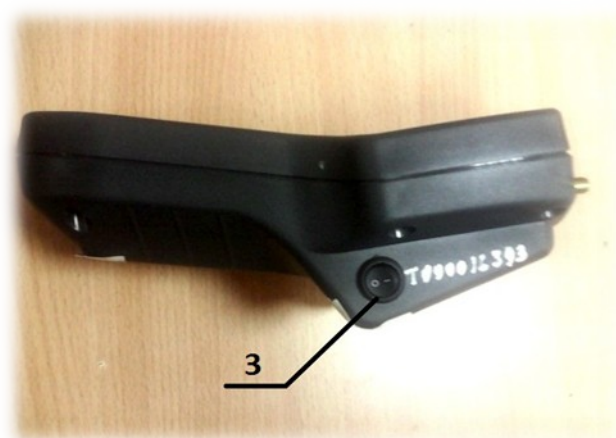


Рисунок 2.7 – многофункциональный поисковой прибор «Спайдер» (вид с правого бока).

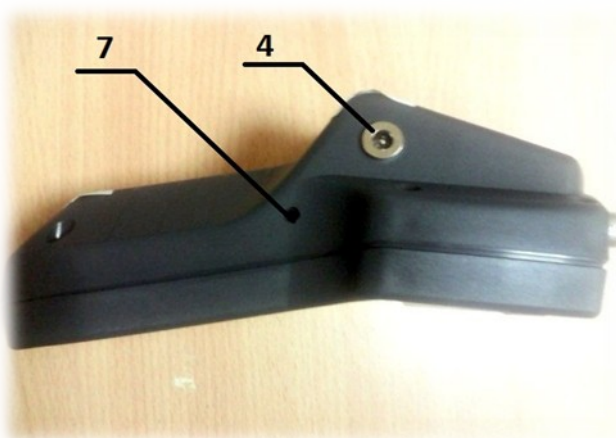


Рисунок 2.8 – многофункциональный поисковой прибор «Спайдер» (вид с левого бока).



Рисунок 2.9 – многофункциональный поисковой прибор «Спайдер» (вид сверху).

Описание обозначений:

- 1 – Дисплей.
- 2 - Многофункциональная клавиатура.
- 3 - Тумблер включения/выключения прибора.
- 4 - Разъем для подключения зарядного устройства.
- 5 - Разъем для подключения ВЧ антенны.
- 6 - Многофункциональный разъем для подключения датчиков.
- 7 - Разъем для подключения наушников.

В режиме акустического приемника прибор позволяет оценить вероятность утечки информации по акустическому каналу.

При подключении акустического датчика к соответствующему разъему прибора и включении прибора, устройство автоматически переходит в данный режим работы.

В данном режиме есть возможность использовать один из двух режимов отображения сигнала - осциллограф или спектроанализатор.

В режиме отображения «осциллограф» реализована возможность установки значений чувствительности и установки длительности развертки.

3. Выявление утечек информации по акустическому каналу, с помощью многофункционального поискового прибора «Спайдер». Порядок выполнения работы.

В аудитории установлена медиа система, поэтому будет производится качественная оценка утечек для источника звука со звукоусилением (84 Дб).

- 1) Присоединить к прибору акустический датчик;



Рисунок 2.10 – акустический датчик.

- 2) Включить источник звука внутри проверяемого помещения.
- 3) Включить прибор кнопкой 2, переключив кнопку питания с 0 на 1. Прибор автоматически перейдет в соответствующий датчику режим работы;
- 4) При необходимости выбрать режим спектрального отображения улавливаемого сигнала кнопкой Fm/Am;
- 5) Микрофон направить на выбранную точку как показано на схеме рис. 2.11.

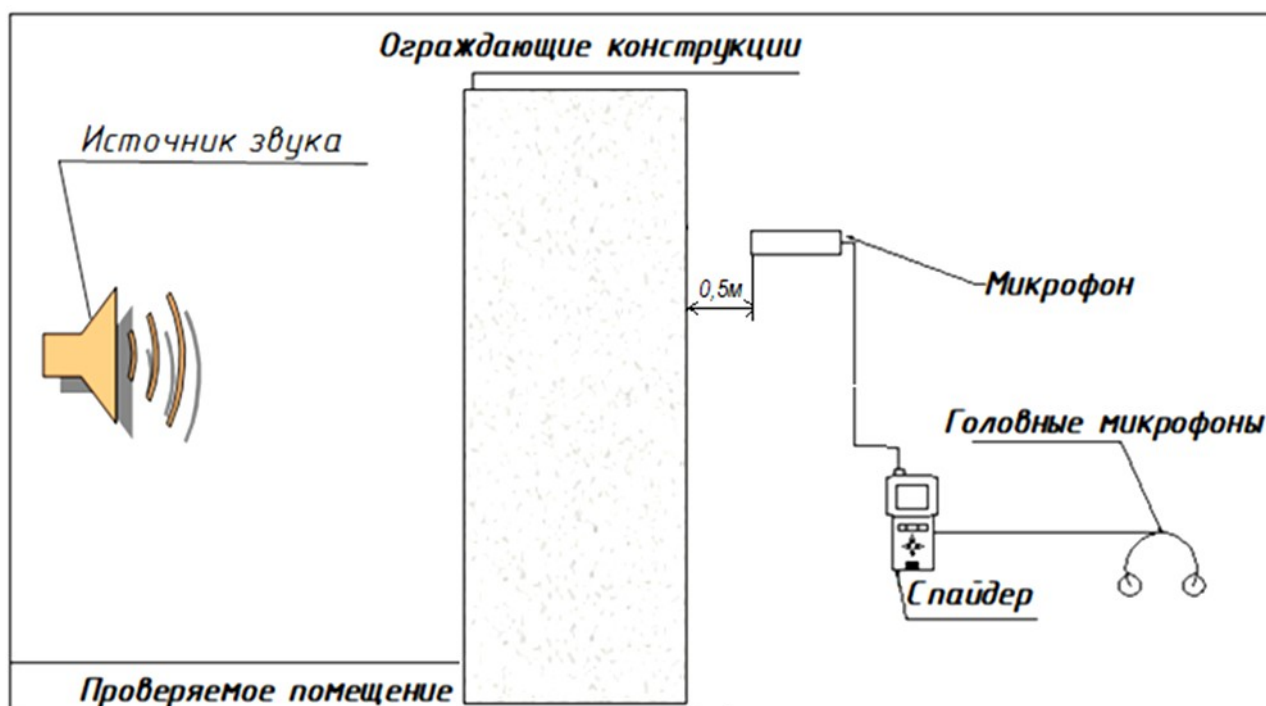


Рисунок 2.11 - Выявление акустических утечек информации с помощью многофункционального поискового прибора «Спайдер»

6) на расстоянии в полуметре для каждой контрольной точки оценить прохождение речевого сигнала.

4. Задания по работе:

- 1) Изучить теоретический материал, данный в работе.
- 2) Определить количество контрольных точек и показать на развёртке помещения места их установки по методике преднамеренного прослушивания.
- 3) Произвести качественную оценку утечки информации для помещения в контрольных точках с помощью поискового прибора «Спайдер».
- 4) Результаты акустического исследования, полученные в ходе обследования занести в таблицу 2.2. Для всех контрольных точек отметить «+» прохождение сигнала $L_{C+Ш}$ и разборчивости речи (W).

Таблица 2.2 Результаты акустических исследований без САЗ (пример)

Объект	КТ	Сигнал L_{C+III}	Разборчивость речи W
Окно 1_1ф	1		
Окно 1_2ф	2		
Окно 1_3ф	3		
Окно 2_1ф	4		
Окно2_2ф	5		
Окно2_3ф	6		
Дверь 1	7		
Дверь 2	8		
Стена 1	9		
Стена 1	10		
Стена 1	11		
Стена 1	12		
Стена 2	13		
Стена 2	14		
Стена 2	15		
Стена 2	16		
Стена 2	17		
Перекрытие потолка	18		
Перекрытие пола	19		

5) Оценить результаты обследования путём выявления мест утечки информации по акустическому каналу и определения мест наилучшего прохождения акустического сигнала.

6) Сделать выводы.

7) Ответить на вопросы.

Вопросы для самоконтроля:

- 1) Какие технические средства могут использоваться злоумышленником для ведения акустической речевой разведки по акустическому каналу утечки?
- 2) Какой показатель определен в качестве нормируемого:
 - a) Слоговая разборчивость речи?
 - b) Словесная разборчивость речи?
 - c) Формантная разборчивость речи?
- 3) Дайте определение словесной разборчивости речи.

Лабораторная работа № 3.

**Тема: «Качественная оценка утечки речевой информации по
виброакустическому каналу с помощью многофункционального
поискового прибора «Спайдер»»**

Цель лабораторного практикума: отработка навыков проведения измерений по выявлению виброакустических каналов утечки речевой информации.

Задачи лабораторного практикума:

- изучить поисковое оборудование и приобрести навыки работы с ним;
- закрепить знание существующей методики проведения качественной оценки утечки речевой информации по виброакустическим каналам;
- отработать навыки практического применения методики качественной оценки утечки речевой информации по виброакустическим каналам.

1. Теория.

Перехват речевой информации из ЗП возможен по вибрационному, оптикоэлектронному (лазерному) и другим каналам с применением различных технических средств акустической разведки, к которым относятся лазерные акустические средства разведки, акселерометры т.д. (см. табл. 3.1.).

Особенностью акустической разведки является то, что анализ перехваченной с помощью технических средств разведки информации производит человек. Поэтому в качестве нормативного показателя оценки эффективности защиты ЗП от утечки речевой информации по техническим каналам часто (но не всегда) используется словесная разборчивость речи W , под которой понимается относительное количество (в процентах) правильно понятых человеком слов, перехваченных (зарегистрированных) средством разведки.

Критерии эффективности защиты речевой информации во многом зависят от целей, преследуемых при организации защиты, например: скрыть смысловое содержание ведущегося разговора, скрыть тематику ведущегося разговора или скрыть сам факт ведения переговоров.

Таблица 3.1.

Потенциальные технические каналы утечки речевой информации

Технические каналы утечки информации	Специальные технические средства речевой разведки, используемые для перехвата информации
Вибрационный (через ограждающие конструкции, трубы инженерных коммуникаций и т.д.)	• <u>Электронные стетоскопы</u>, установленные в смежных помещениях, принадлежащих другим организациям; • <u>электронные устройства перехвата речевой информации с датчиками контактного типа</u>, установленные на инженерно-технические коммуникациях (трубы водоснабжения, отопления, канализации, воздуховоды и т.п.) и внешних ограждающих конструкциях (стены, потолки, полы, двери, оконные рамы и т.п.) ЗП, при условии неконтролируемого доступа к ним

Технические каналы утечки информации	Специальные технические средства речевой разведки, используемые для перехвата информации
	посторонних лиц.
Оптикоэлектронный (через оконные стекла)	• <u>Лазерные акустические системы</u>, установленные в близлежащих строениях, находящихся за границей КЗ.

2. Методика выбора контрольных точек

Методики выбора контрольных точек для проведения измерений не существует, однако по многолетнему опыту организации, выполняющей специальные исследования, можно сформулировать следующие общие рекомендации. Будем считать, что средств активной защиты отсутствуют.

На горизонтальных и вертикальных однородных ограждающих конструкциях (кирпич, бетон) на каждый квадрат 2х2м намечается одна контрольная точка для проведения вибрационных измерений как показано на рисунке 3.1.

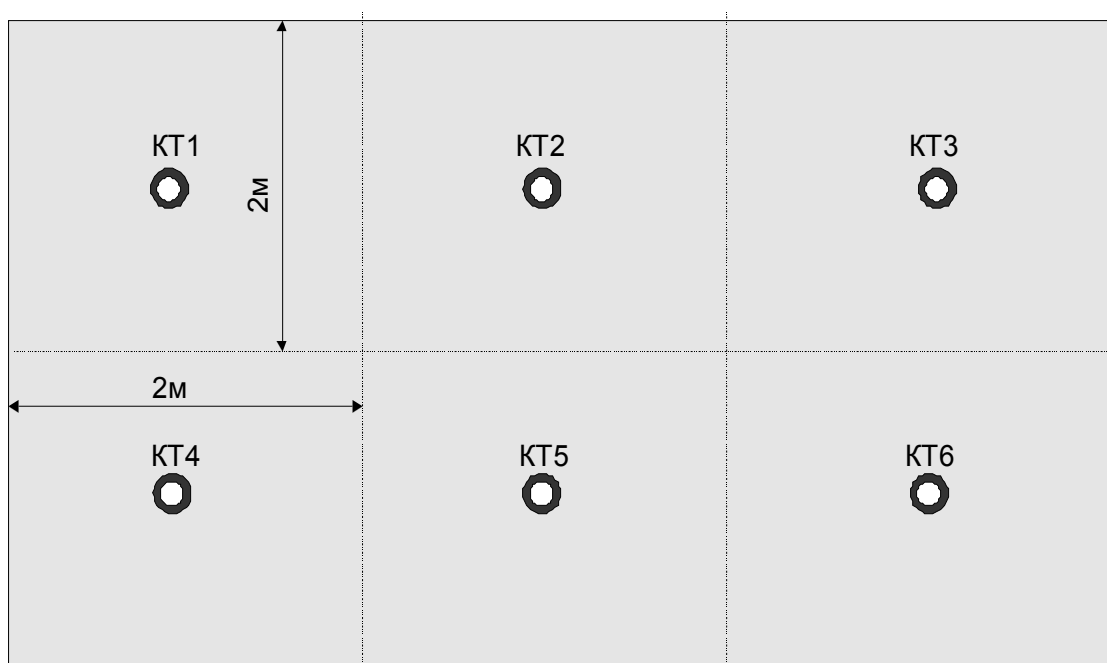


Рисунок 3.1 - Размещение КТ на однородных горизонтальных и вертикальных ограждающих конструкциях

Если конструкция неоднородная (например, плиты перекрытия) то на каждые два погонных метра неоднородности намечается одна контрольная точка.

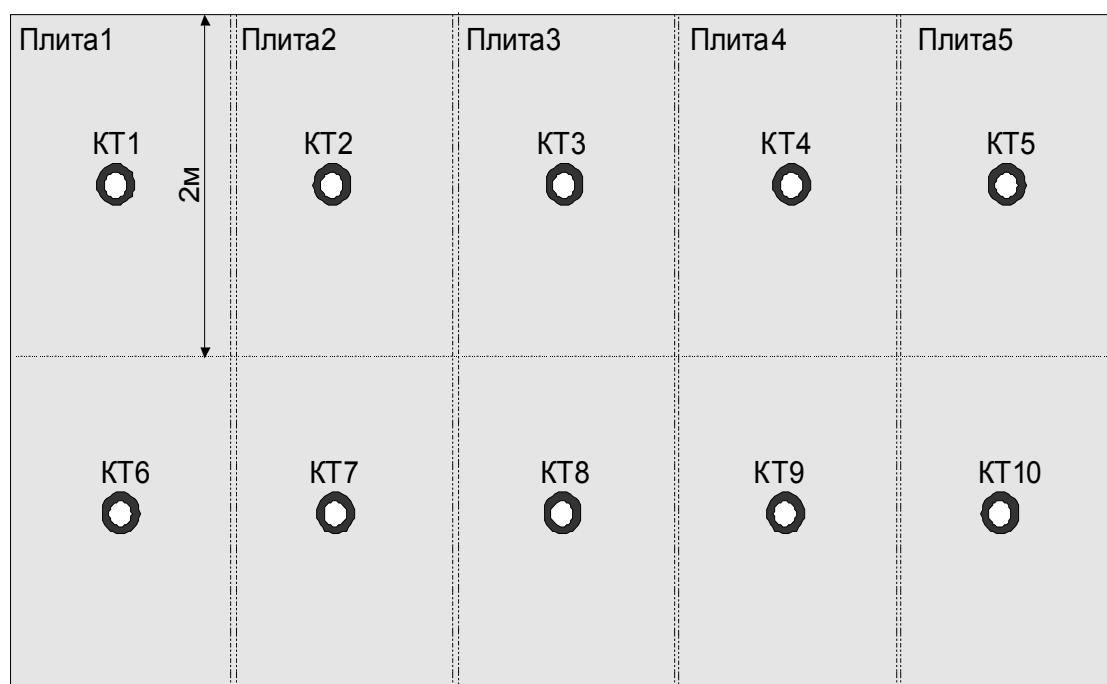


Рисунок 3.2 - Размещение контрольных точек на неоднородной поверхности

Примечание:

- а) Если имеется дверь в стене, то разметка начинается от двери.
- б) При смежных перекрытиях (окна, двери) если не хватает расстояния 2х2м, разметка рассчитывается из оставшегося расстояния. Должна быть охвачена вся площадь поверхности.
- в) При наличии трещин и изгибов стен, выставляются дополнительные контрольные точки для выявления утечки.

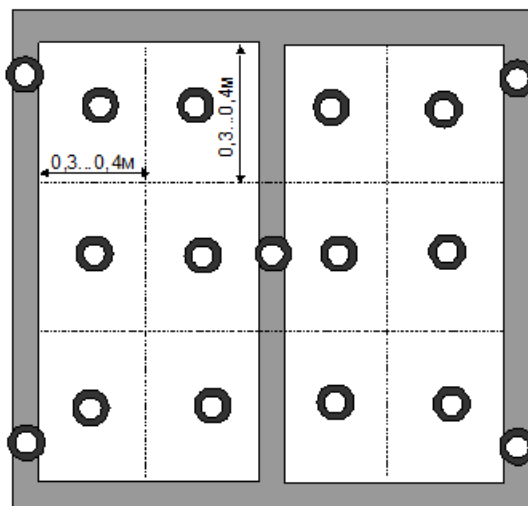


Рисунок 3.3 - Размещение контрольных точек на поверхности оконного остекления для вибрационных измерений

Размещение контрольных точек на поверхности оконного остекления осуществляется на основе правила - поверхность делится на участки размером $(0,3...0,4) \times (0,3...0,4)$ м и в центре каждого участка намечается контрольная точка для проведения вибрационных измерений. Контрольные точки для проведения вибрационных исследований на раме намечаются вблизи узлов крепления.

Объектом исследований так же являются трубопроводы системы отопления и другие инженерные конструкции. Контрольные точки располагать за пределами выделенного помещения на конструкции в полуметре от границы контролируемой зоны.

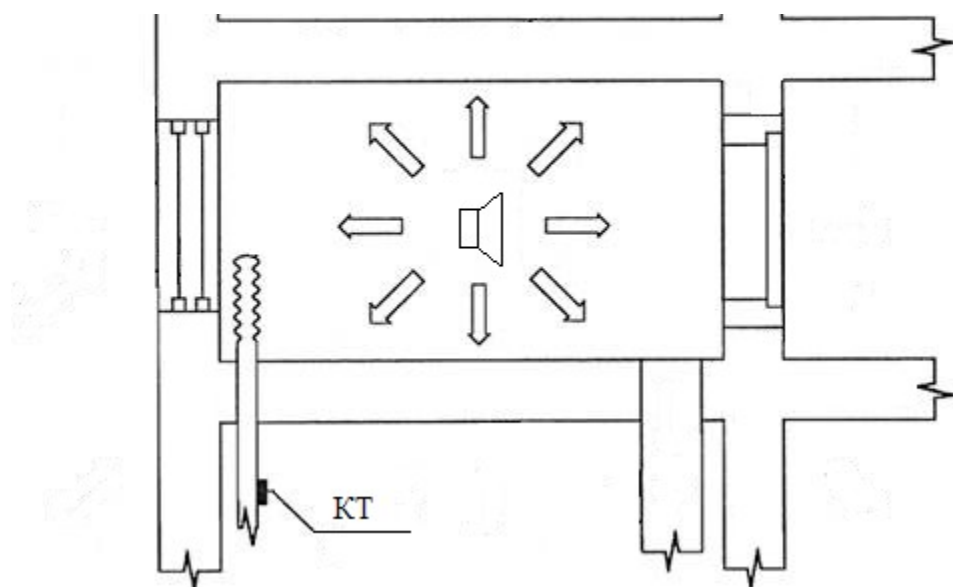


Рисунок 3.4 - Размещение контрольных точек на системе отопления для вибрационных измерений

3. Порядок выполнения работы.

Качественная оценка утечки информации по виброакустическому каналу, с помощью multifunctional search device «Spider»

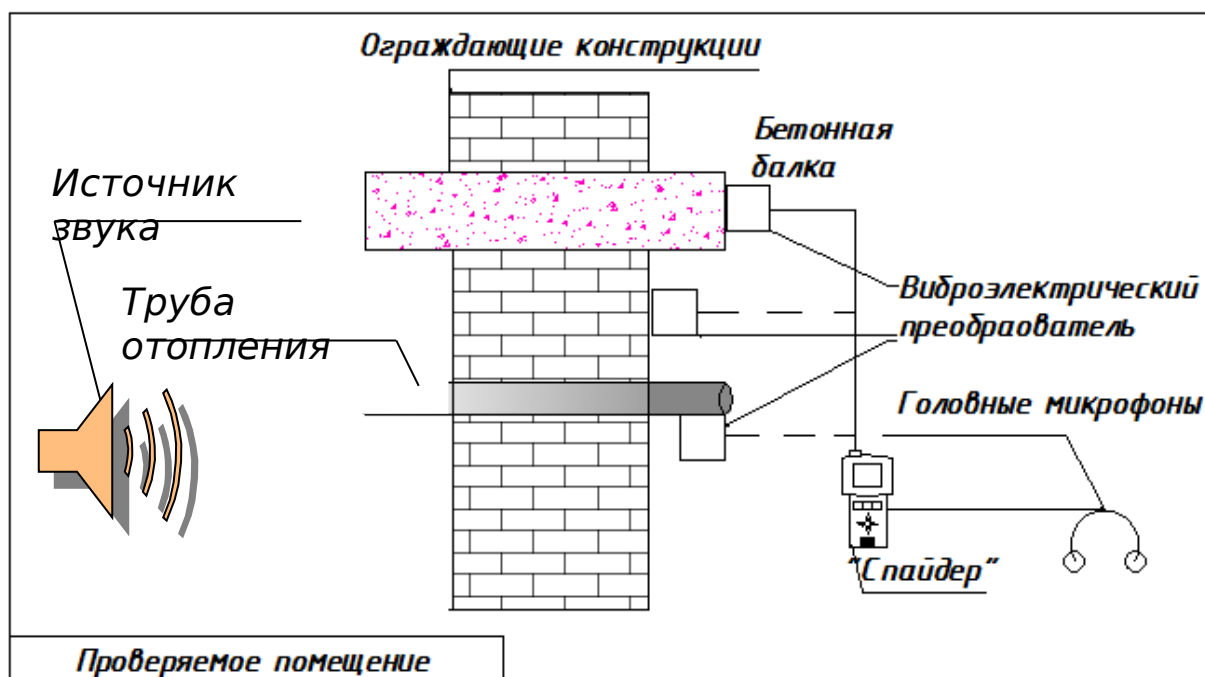


Рисунок 3.5 - Выявление виброакустических утечек информации с помощью многофункционального поискового прибора «Спайдер».

- 1) Поместите источник звука внутри проверяемого помещения на расстоянии одного метра от проверяемых конструкций.
- 2) Возьмите поисковый прибор «Спайдер».
- 3) подключите к прибору виброакустический датчик (рисунок – 3.6).



Рисунок 3.6 – Виброакустический датчик.

4. Включите головные микрофоны в соответствующий разъем.
5. Включите прибор, переключив кнопку питания с 0 на 1. Прибор автоматически перейдет в соответствующий датчику режим работы.

Задания по работе:

- 1) Изучить теоретический материал, данный в лабораторной работе.
- 2) На развёртке плана исследуемого помещения отметить все контрольные точки для качественной оценки утечки речевой информации по виброакустическому каналу.
- 3) Произвести качественную оценку утечки информации для помещения в виброакустических контрольных точках. Занести результаты виброакустического исследования, полученные в ходе обследования в таблицу

1. Для всех контрольных точек отметить «+» прохождение сигнала $L_{C+Шi}$ и разборчивости речи (W).

Таблица 3.1. Результаты виброакустических исследований без САЗ (вариант)

Объект	КТ	Сигнал $L_{C+Шi}$	Разборчивость речи W
Окно 1_1ф	1		
Окно 1_2ф	2		
Окно 1_3ф	3		
Окно 2_1ф	4		
Окно2_2ф	5		
Окно2_3ф	6		
Дверь 1	7		
Дверь 2	8		
Стена 1	9		
Стена 1	10		
Стена 1	11		
Стена 1	12		
Стена 2	13		
Стена 2	14		
Стена 2	15		
Стена 2	16		
Стена 2	17		
Перекрытие потолка	18		
Перекрытие пола	19		
Трубы отопления	20		

- 3) Оценить результаты обследования путём выявления мест утечки информации по виброакустическому каналу и определения мест наилучшего прохождения сигнала.
- 4) Сделать выводы.

3. Вопросы для самоконтроля:

- 1) Что такое вибрационный канал утечки информации?
- 2) Какие технические средства могут использоваться злоумышленником для ведения акустической речевой разведки по виброакустическому каналу утечки?
- 3) Каков показатель разборчивости речи для скрывтия факта переговоров?

Лабораторная работа № 4.

Тема: «Количественная оценка защищенности речевой информации по акустическому каналу через двери с использованием ПАК «Шёпот»»

Цель работы: Отработка навыков проведения измерений по выявлению виброакустических каналов утечки речевой информации с использованием системы оценки защищенности выделенных помещений по виброакустическому каналу «Шепот»

Основными задачами работы являются:

- изучение порядка работы с системой «Шепот» при проведении измерений;
- приобретение навыков проведения измерений по оценке защищенности ограждающих конструкций – дверей – от утечки информации по акустическому каналу;

- закрепление навыков проведения измерений по оценке защищенности ограждающих конструкций – дверей – от утечки информации по акустическому каналу;
- закрепление навыков автоматизированного составления отчета;
- закрепление навыков калибровки системы.

1. Теоретическая часть

1.1 Специальные документы РФ по защите информации:

- Специальные требования и рекомендации по технической защите конфиденциальной информации. (Утверждены приказом Гостехкомиссии России от 30 августа 2002г).
- Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам, Москва, 2002г.

1.2. Аудит информационной безопасности по акустическому каналу.

Аудит информационной безопасности позволяет получить наиболее полную и объективную оценку защищенности информационных ресурсов объекта защиты, локализовать имеющиеся каналы утечки, разработать наиболее эффективную политику защиты информации.

Среди важнейших каналов утечки информации являются акустический и виброакустический каналы.

Частотный диапазон речи лежит в пределах 70...7000 Гц. Энергия акустических колебаний в пределах указанного диапазона распределена неравномерно. На рисунке 1 кривой *I* представлен вид среднестатистического спектра русской речи. Следует отметить, что порядка 95% энергии речевого сигнала лежит в диапазоне 175...5600 Гц.

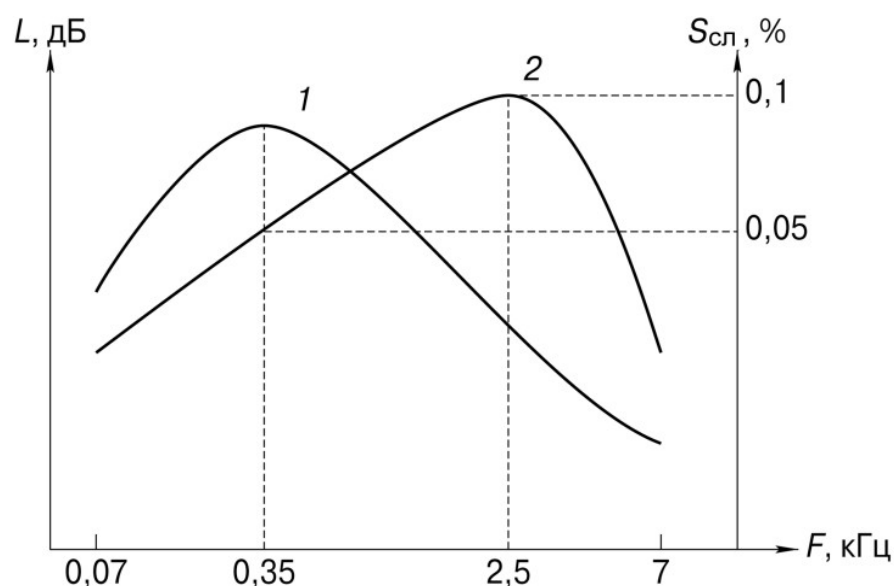


Рисунок 1. Среднестатистический спектр русской речи.

Важно отметить и то, что информативная насыщенность отдельных участков спектра речи неравномерна. Кривой 2 на рисунке 1 представлен вклад отдельных участков спектра речи в суммарную разборчивость.

При своем распространении звуковая волна, доходя до какой-либо преграды (границы двух сред, фазовый переход) и взаимодействуя с ней, частично отражается от нее, а частично продолжает распространяться внутри преграды. Внутренняя поверхность преграды начинает колебаться, создавая вибрационные волны внутри нее. Вибрационные волны дойдя до внешней поверхности преграды вызывают колебания внешней поверхности. И внешняя и внутренняя поверхности при колебаниях движутся с ускорениями, которые можно измерить.

Измерив звуковое давление до и после преграды L_1 и L_2 можно оценить звукоизоляцию Q :

$$Q = L_1 - L_2, \quad (1)$$

Измерив уровень вибрационного ускорения на внутренней и внешней сторонах преграды V_1 и V_2 можно оценить виброизоляцию:

$$Q = V_1 - V_2, \quad (2)$$

Данные выражения верны, если уровни звукового давления и вибрационные ускорения измерены в децибеллах.

В настоящее время все оценки технических каналов утечки речевой информации осуществляются путём измерений отношений сигнал/шум в тех или иных полосах частот речевого диапазона. Типовые уровни речевого сигнала в октавных полосах частотного диапазона речи приведены в таблице 1.

Таблица 1.

Типовые уровни речевого сигнала в октавных полосах частотного диапазона речи $L_{с.і}$

Номер полосы	Частотные границы полосы, f_H-f_B , Гц	Среднегеометрическая частота полосы, f_i , Гц	Типовые интегральные уровни речи L_s , измеренные на расстоянии 1 м от источника сигнала, дБ	
			$L_s = 70$	$L_s = 84$
1	175 - 355	250	66	80
2	355 - 710	500	66	80
3	710 - 1400	1000	61	75
4	1400 - 2800	2000	56	70
5	2800 - 5600	4000	53	67

Определив отношение сигнал/шум можно количественно оценить словесную разборчивость речи. Зависимость словесной разборчивости речи от отношения сигнал/шум представлены на рисунке 2.

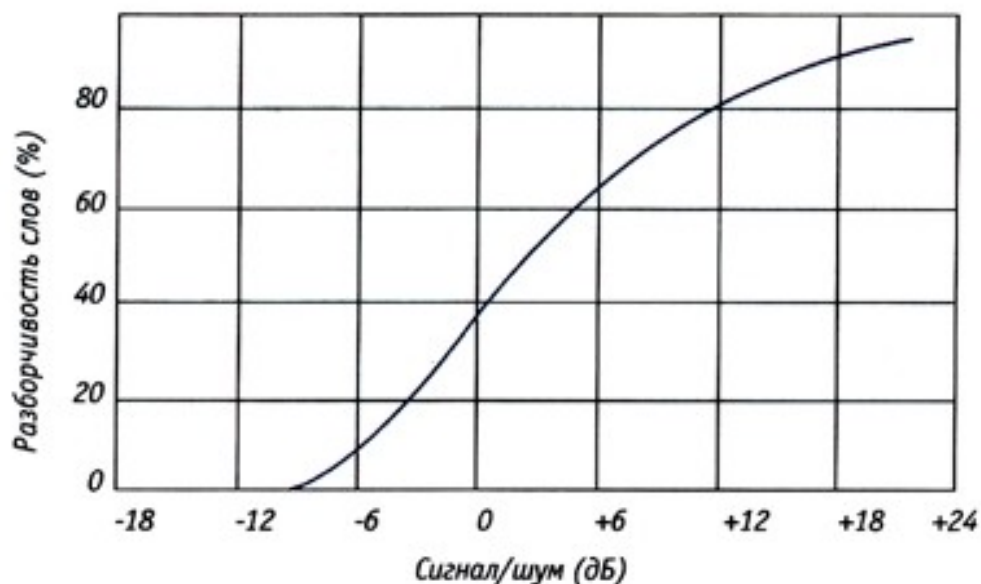


Рисунок 2. Зависимость словесной разборчивости речи от отношения сигнал/шум.

Учитывая то, что характеристики речи каждого человека индивидуальны, при проведении измерений речь реального человека заменяется тестовым

сигналом. Практически во всех измерительных комплексах в качестве тестового сигнала используется шум. Нормированный уровень тестового сигнала (модель русской речи) представлен на рисунке.

На верхней части рисунка 3 представлена модель русской речи для помещения без средств звукоусиления, на нижней части - модель русской речи для помещений со средствами звукоусиления.

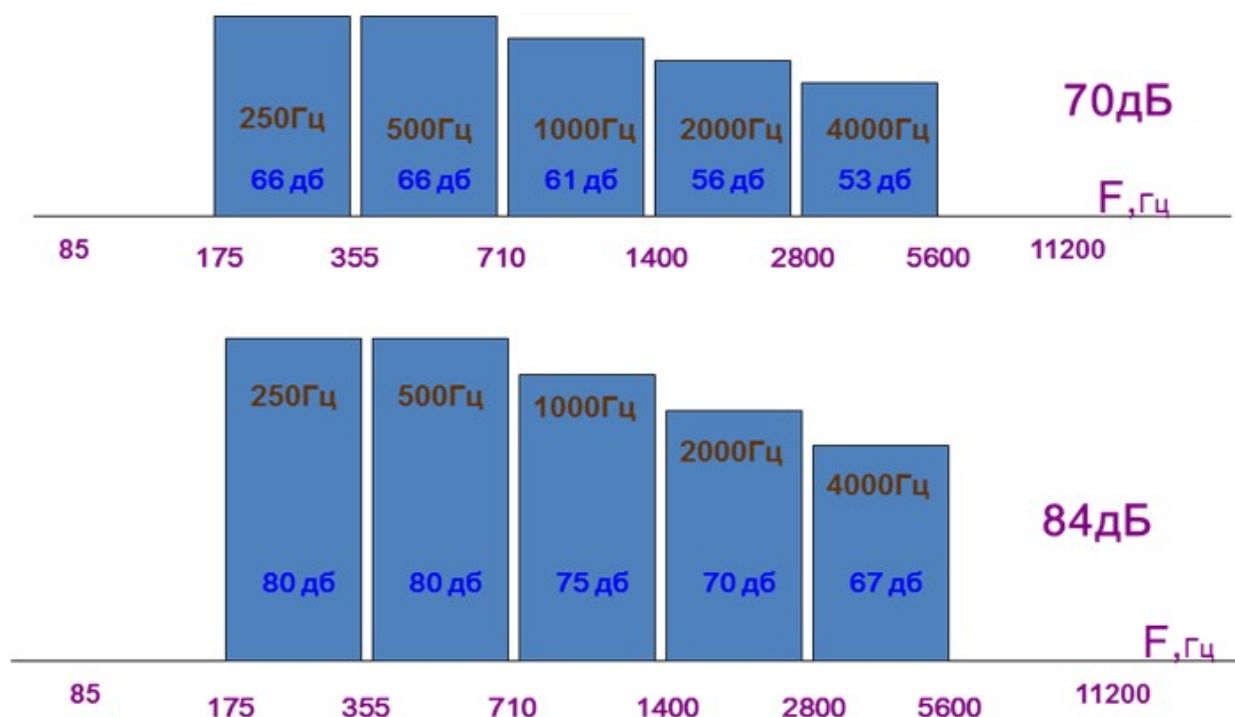


Рисунок 3. Модель русской речи.

Интегральный уровень звукового давления по пяти октавам рассчитывается по формуле:

$$L_{\Sigma} = 10 \lg \left(10^{\frac{L_{c1}}{10}} + 10^{\frac{L_{c2}}{10}} + 10^{\frac{L_{c3}}{10}} + 10^{\frac{L_{c4}}{10}} + 10^{\frac{L_{c5}}{10}} \right). \quad (3)$$

Для оценки защищенности речевой информации в качестве критерия используется такой показатель, как словесная разборчивость речи.

Разборчивость речи оценивается инструментально-расчетным методом. Для этого оценивается октавное отношение сигнал/шум E_i за пределами ограждающей конструкции, а разборчивость речи W рассчитывается в соответствии с выражением:

$$W = \begin{cases} 1,54 * R^{0,25} [1 - \exp(-11 * R)], & \text{если } R < 0,15, \\ 1 - \exp\left[-\frac{11 * R}{1 + 0,7 * R}\right], & \text{если } R \geq 0,15, \end{cases} \quad (4)$$

где: R – интегральный индекс артикуляции речи,

$$R = \sum_{i=1}^5 r_i, \quad (5)$$

$$r_i = \begin{cases} \left(\frac{0,78 + 5,46 * \exp[-4,3 * 10^{-3} * (27,3 - |Q_i|)^2]}{1 + 10^{0,1 * |Q_i|}} \right) * K_i, & \text{если } Q_i \leq 0; \\ \left(1 - \frac{0,78 + 5,46 * \exp[-4,3 * 10^{-3} * (27,3 - |Q_i|)^2]}{1 + 10^{0,1 * |Q_i|}} \right) * K_i, & \text{если } Q_i > 0; \end{cases} \quad (6)$$

K_i – значение весового коэффициента в i -й октавной полосе;

$$Q_i = E_i - A_i;$$

$E_i = L_{с,i} - L_{ш,i}$ – отношение "уровень сигнала/уровень шума" в месте измерения в i -й октавной полосе, дБ;

$L_{с,i}$ – уровень сигнала в месте измерения в i -й октавной полосе, дБ;

$L_{ш,i}$ – минимальный уровень шума (помехи) в месте измерения в i -й октавной полосе, дБ.

В зависимости от поставленной цели защиты требуемую разборчивость речи можно определить исходя из таблицы 2.

Таблица 2. Показатели разборчивости.

Цель защиты	Показатель разборчивости, W%
Скрыть факт переговоров	<10
Скрыть предмет переговоров	<20
Скрыть содержание переговоров	<30
Непреднамеренное прослушивание	<40

--	--

2. Описание системы оценки защищенности выделенных помещений по виброакустическому каналу «Шепот»

2.1 Назначение, технические характеристики и состав системы

Система оценки защищенности выделенных помещений по виброакустическому каналу «Шепот» (далее система «Шепот») предназначена для проведения специальных акустических и вибрационных измерений в выделенных помещениях с целью оценки их защищенности от утечки речевой информации по акустическому и вибрационному каналам.

Система «Шепот» обеспечивает:

- автоматические измерения уровня звукового давления в 5-ти октавных полосах с центральными частотами 250, 500, 1000, 2000 и 4000 Гц;
- автоматические измерения уровня виброускорения в 5-ти октавных полосах с центральными частотами 250, 500, 1000, 2000 и 4000 Гц;
- возможность перехода на ручное управление аппаратурой системы;
- автоматизированный расчет показателей защищенности выделенных помещений по акустическому и виброакустическому каналу утечки речевой информации;
- возможность настройки системы защиты выделенных помещений объекта от утечки речевой информации по акустическому и виброакустическому каналу;
- формирование и ведение базы данных о месте и результатах выполненных измерений;
- составление отчета по результатам измерений в форме, отвечающей требованиям НМД АРР;

Состав основных элементов базового комплекта системы «Шепот» представлен на рисунке 4.

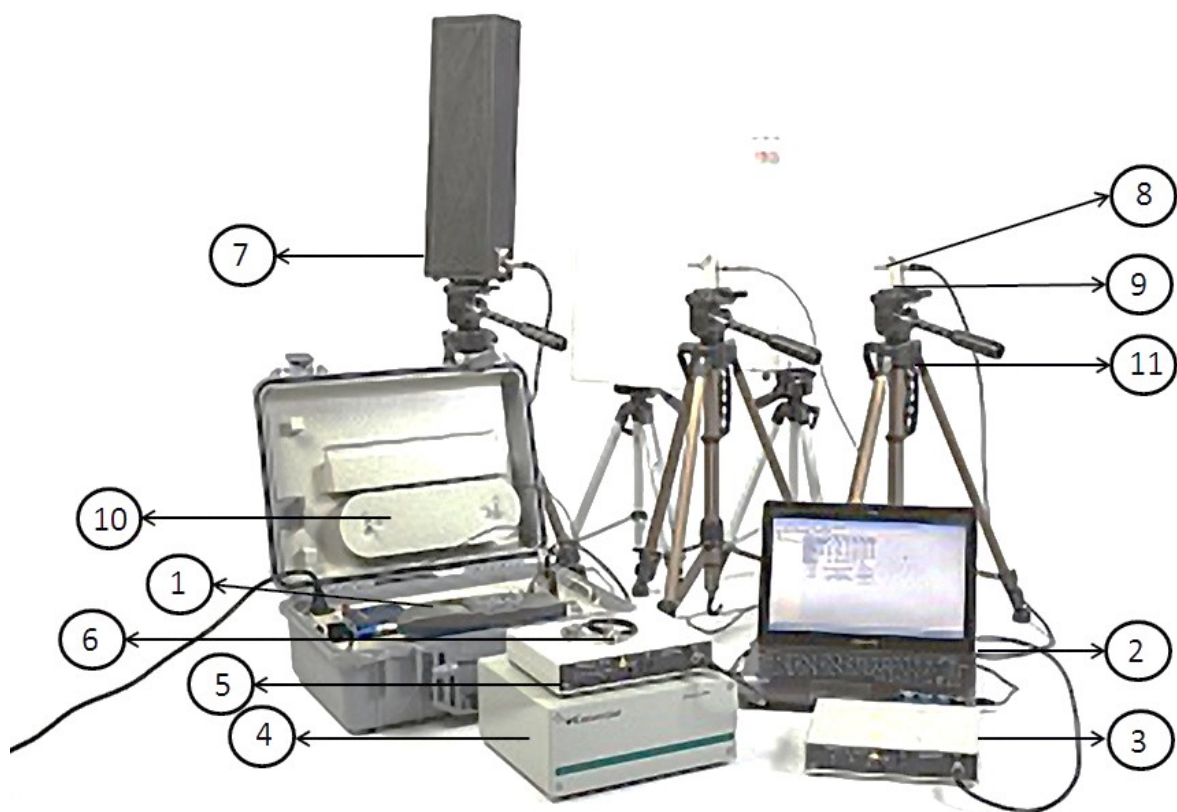


Рисунок 4. Основные элементы комплекта системы «Шепот»

Система «Шепот» включает в себя:

- 1) Шумомер.
- 2) Персональная ЭВМ (ноутбук).
- 3) Комплект приемник/передатчик информации по радиоканалу «Тип А».
- 4) Генератор тестового акустического сигнала.
- 5) Комплект приемник/передатчик информации по радиоканалу «Тип В».
- 6) Акселерометр.
- 7) Громкоговоритель (колонка).
- 8) Микрофон.
- 9) Держатель микрофона.
- 10) Кабель измерительный 20 м.
- 11) Штатив для микрофона.

Генератор шума «Шорох-2МИ» предназначен для генерации электрического сигнала с возможностью регулировки его уровня на центральных октавных частотах 250, 500, 1000, 2000, 4000Гц.

На задней панели генератора имеется разъем «Выход» для подключения звукового излучателя, кнопка «Упр» для ручного отключения генератора, разъем «Упр» для подключения генератора к рабочей укладке, разъем «Вход» для подключения внешнего источника шума, переключатель «Внутр-Внеш» для подключения выхода к внутреннему или внешнему источнику шума, регулятор уровня сигнала.

На передней панели под крышкой расположены органы управления 5-ти полосным эквалайзером.

Акустический излучатель (звуковая колонка) предназначен для преобразования электрического сигнала в акустические колебания воздушной среды.

Микрофон предназначен для преобразования звукового давления в воздушной среде в электрический сигнал.

Акселерометр предназначен для преобразования виброускорений в твердых средах в электрический сигнал.

Шумомер предназначен для измерения уровня электрического сигнала от микрофонов или акселерометра и обработки результатов измерений.

Компьютер с соответствующим программным обеспечением предназначен для управления компонентами системы, ведения базы данных об исследуемых объектах и результатах измерений, выполнения необходимых расчетов и подготовки отчета.

2.2. Принцип работы системы

Порядок работы данной системы можно разделить на несколько этапов:

1) Генератор тестового сигнала «Шорох-2МИ» по командам от компьютера формирует с помощью акустического излучателя (звуковой колонки) шумовой тест-сигнал в пяти октавных полосах, который принимается микрофоном 1 (рис.5).

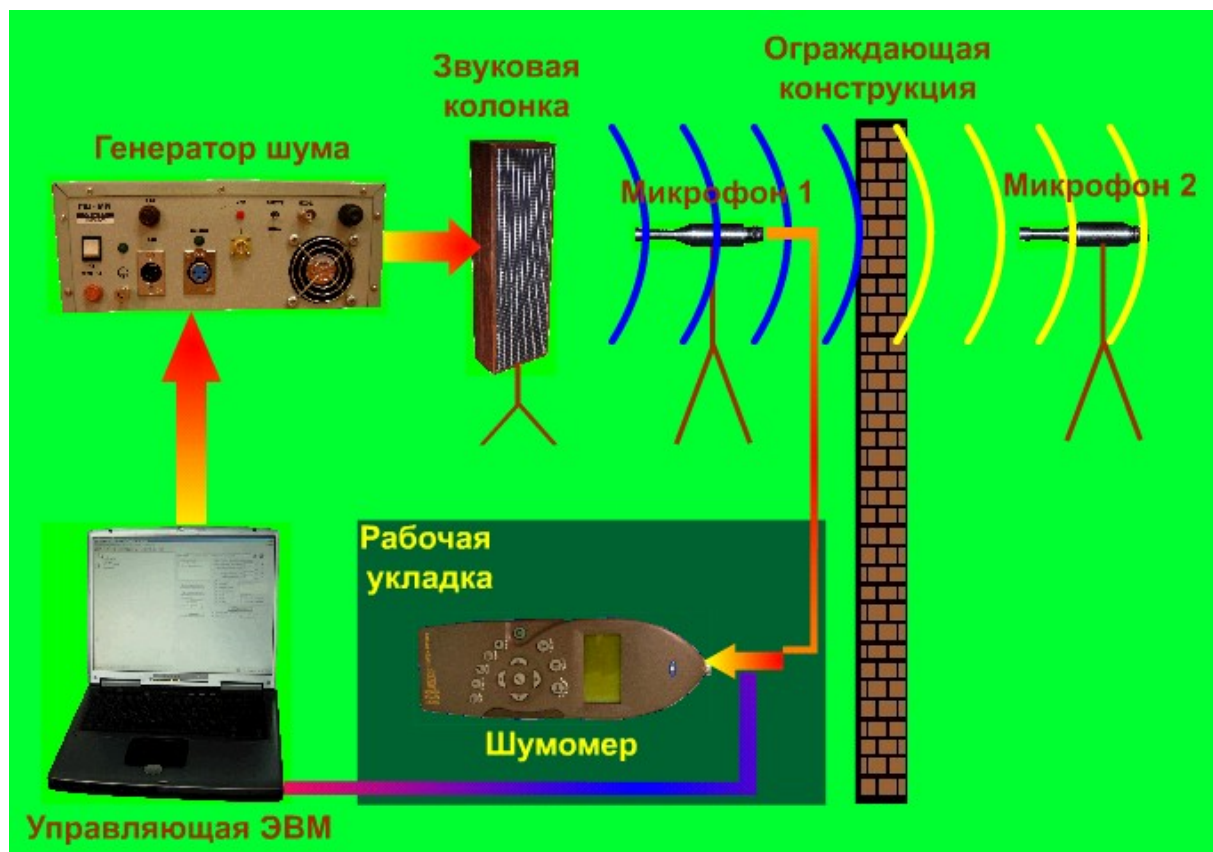


Рис. 5. Структура системы «Шепот» на этапе измерения уровня тест-сигнала

Электрический сигнал от микрофона через управляемый коммутатор поступает в шумомер, где происходит измерение его уровня. Значения измеренных шумомером уровней информативного (тестового) сигнала в пяти октавных полосах записываются в базу данных компьютера.

2) Во второго этапа в коммутаторе микрофон 1 и включается микрофон 2 таким образом, измерение уровня сигнала и фона ограждающей конструкцией измерению тест сигнала.

3) На этапе, по компьютера, излучение сигнала прекращается и микрофон 2 производится уровня только фона.

4) В заключительном результаты измерений компьютером (2) и в табличном и графическом виде.

Если оценка эффективности создаваемых средствами защиты (САЗ), проводится четвертый измерения. При система предлагает САЗ, после начинается измерение и фона.

Защита речевой информации обеспечена в случае, если на границе контролируемой зоны расчётные величины отношения синла/шум и разборчивость речи не превышают необходимого значения.

2.3 Описание работы программного обеспечения «Шепот-Интерфейс»

Программное обеспечение «Шепот-Интерфейс» уже должно быть загружено в ПЭВМ.

Запуск программы «Шепот-Интерфейс» (файл «**asct.exe**») выполняется аналогично запуску любого приложению Windows. В случае корректного запуска программы «Шепот-Интерфейс» на экран выводится ее главное рабочее окно.

Проверяются параметры соединения ПЭВМ с шумомером. Для этого в поле «**Соединение**» (рис. 7) в окне «**Порт**» указать номер СОМ-порта ПЭВМ, к которому подсоединен шумомер. Номер порта ПЭВМ, используемого для подключения шумомера, может быть введен с клавиатуры заглавными латинскими буквами. Уточнить номер порта можно в диспетчере устройств ПЭВМ. В окне «**Скорость**» из списка должно быть выбрано значение установленной на шумомере скорости передачи его данных. Рекомендованное значение скорости передачи данных для установки на шумомере и в окне «**Скорость**» - 19200 бит/с. Для вступления введенных в этом окне параметров в силу необходимо кликнуть на кнопке «**Применить**».

Уточнить/изменить скорость передачи данных шумомера «Larson&DavisSystem 824». Для этого необходимо на шумомере нажать «**Tolls/Communications/Bound**» и выставить рекомендованное скорость передачи «**19200**».

Убедиться, что флаг «**ICP-питание**» в окне «**Начальные установки**» установлен. При наличии этого флага производится программное включение встроенного источника ICP-питания измерительных датчиков системы «Шепот».

В меню «**Параметры**» главного рабочего окна выбирается позиция «**Настройки уровней и отчета**». В открывшемся окне «**Настройки уровней и отчета**» оператор может ввести нормированные значения отношений «сигнал/шум» в октавных полосах с центральными частотами 250, 500, 1000, 2000 и 4000 Гц для уровней **A**, **B** и **C**. Нормированные значения определены НМД APP и используются программой при обработке результатов измерений. Значения заданных отношений «сигнал/шум» в октавных полосах с центральными частотами 250, 500, 1000, 2000 и 4000 Гц для уровней **A**, **B** и **C** «по умолчанию» приняты равными нулю.

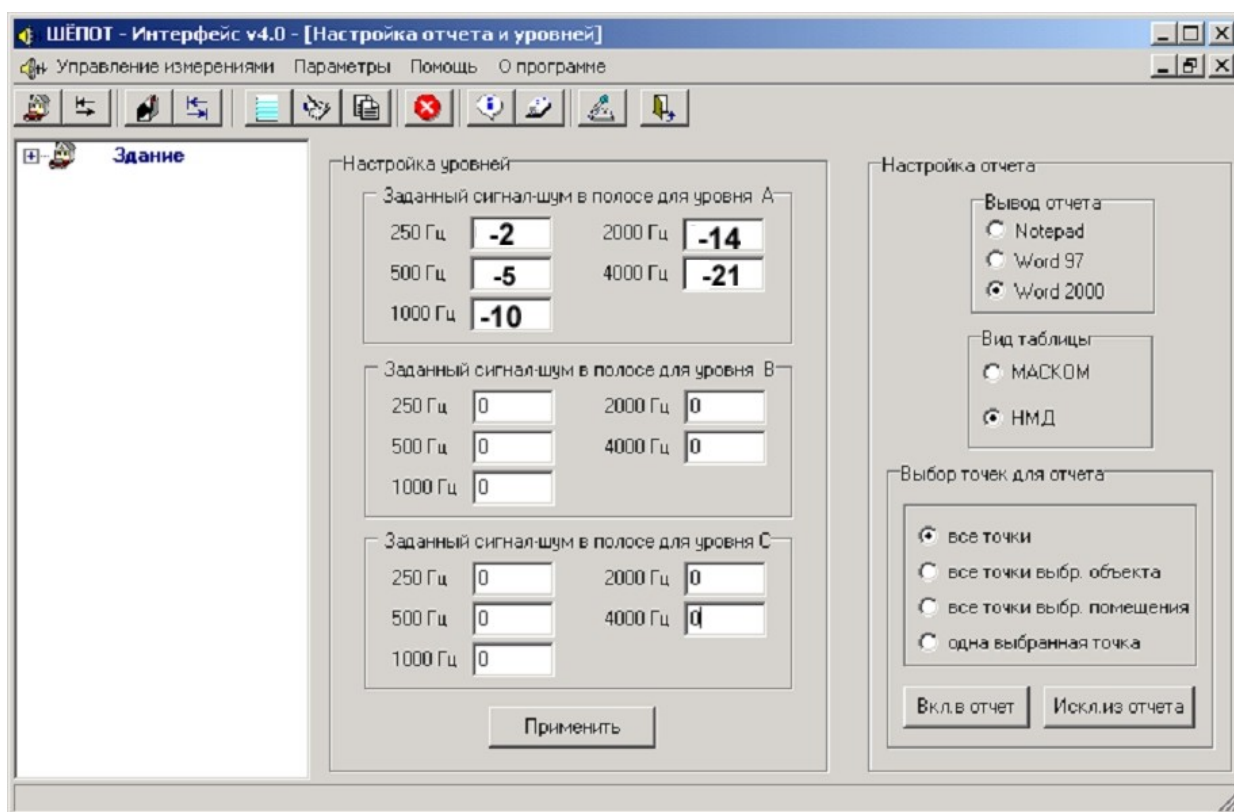


Рис. 6. Окно настройки уровней

Для проведения измерений и расчетов рекомендуется ввести гипотетические значения отношений «сигнал/шум», изображенные на рис. 6.

Для вступления введенных в этом окне параметров в силу необходимо нажать кнопку «**Применить**».

На панели «**Настройка отчета**» необходимо выбрать текстовый редактор, с помощью которого будет готовиться отчет, вид таблиц и контрольные точки, выводимые в отчете.

В левой части главного окна программы находятся окно, в которое вводятся наборы мест проведения исследований. В правой части окна расположено поле для размещения собственных окон программы и их вкладок. Места проведения исследований представляются в виде дерева с тремя уровнями иерархии: на первом уровне показываются объекты, на втором – помещения, на третьем – контрольные точки. Развертывание и свертывание уровней осуществляется «щелчком» левой клавиши «мыши» по символу .

Выбранный объект, помещение или контрольная точка выделяются синей заливкой.

Контрольные точки, в которых имеются результаты измерений, отмечены знаком . Знаком  отмечены контрольные точки, включенные в отчет по результатам исследования, а знаком  - контрольные точки, исключенные из этого отчета.

Для проведения измерений и расчетов объект обязательно должно содержать в себе хотя бы одно помещение, а помещение – хотя бы одну контрольную точку. Объектам рекомендуется присваивать уникальные имена.

Основными элементами управления главного окна программы являются три кнопки вызова меню - «**Управление измерениями**», «**Параметры**», «**Помощь**», кнопка вызова сведений «**О программе**» и двенадцать кнопок выбора режимов работы, каждая из которых переводит программу в одноименный режим работы:

- кнопка «**Добавление объекта**» (Ctrl + Alt + O) ;
- кнопка «**Просмотреть/Изменить параметры объекта**» (Ctrl + Alt + V) ;
- кнопка «**Добавление помещения**» (Ctrl + Alt + R) ;
- кнопка «**Просмотреть/Изменить параметры помещения**» (Ctrl + Alt + P) ;
- кнопка «**Добавить контрольную точку**» (Ctrl + Alt + Q) ;
- кнопка «**Просмотр контрольной точки**» (Ctrl + Alt + M) ;
- кнопка «**Копирование контрольной точки**» (Ctrl + Alt + C) ;
- кнопка «**Удаление элемента**» (Ctrl + Alt + D) .

- кнопка **«Отчет по объектам»** (Shift + Ctrl + F11) ;
- кнопка **«Параметры соединения с шумомером и контрольной точки»** ;
- кнопка **«Тест коммутатора»** (Ctrl + Alt + K) ;
- кнопка **«Выход из программы»** (F10) .

Позиции меню **«Управление измерениями»** дублируют одиннадцать из перечисленных выше кнопок (в этом меню отсутствует позиция **«Параметры соединения с шумомером и контрольной точки»**). Щелчок правой клавиши мыши на элементе в левой части главного окна программы открывает окно меню, позиции которого дублируют десять из перечисленных выше кнопок (в этом меню отсутствуют позиции **«Параметры соединения с шумомером и контрольной точки»** и **«Выход из программы»**).

Меню **«Параметры»** содержит две позиции:

- **«Настройки БД, шумомера и по умолчанию»**, дублирующую кнопку **«Параметры соединения с шумомером и контрольной точки»**;
- **«Настройка уровней и отчета»**.

Меню **«Помощь»** организовано аналогично стандартному меню **«Справка»** приложения «Windows».

Доступные оператору в процессе работы кнопки управления и позиции меню отображаются как активные, недоступные – блокируются и отображаются как неактивные. Практически все кнопки и позиции меню дублируются «горячими клавишами».

Работа в главном окне программы аналогична работе в многооконном режиме ОС «Windows». Единственной особенностью является ограничение зоны перемещения и разворачивания собственных окон программы границами

правого поля главного окна программы, предназначенного для их размещения. Все остальные операции – изменение границ окон, перемещения открытых окон с помощью «мыши», применение кнопок работы с окнами - «Свернуть», «Развернуть/Свернуть окно» и «Заккрыть», работа с позициями меню, выбор элементов в окне мест проведения работ – совпадают с аналогичными операциями в окнах ОС «Windows».

Окно «**Начальные установки**» предназначено для выбора оператором требуемого для работы файла базы данных, установки используемого типа шумомера и параметров соединения с ним, а также для установки параметров и условий проведения измерений для вновь создаваемых контрольных точек. Кроме того, окно служит для ввода результатов калибровки системы «Шепот» и поверочных характеристик средств измерения перед проведением измерений. Вид окна «**Начальные установки**» в правом поле главного окна программы показан на рис. 7.

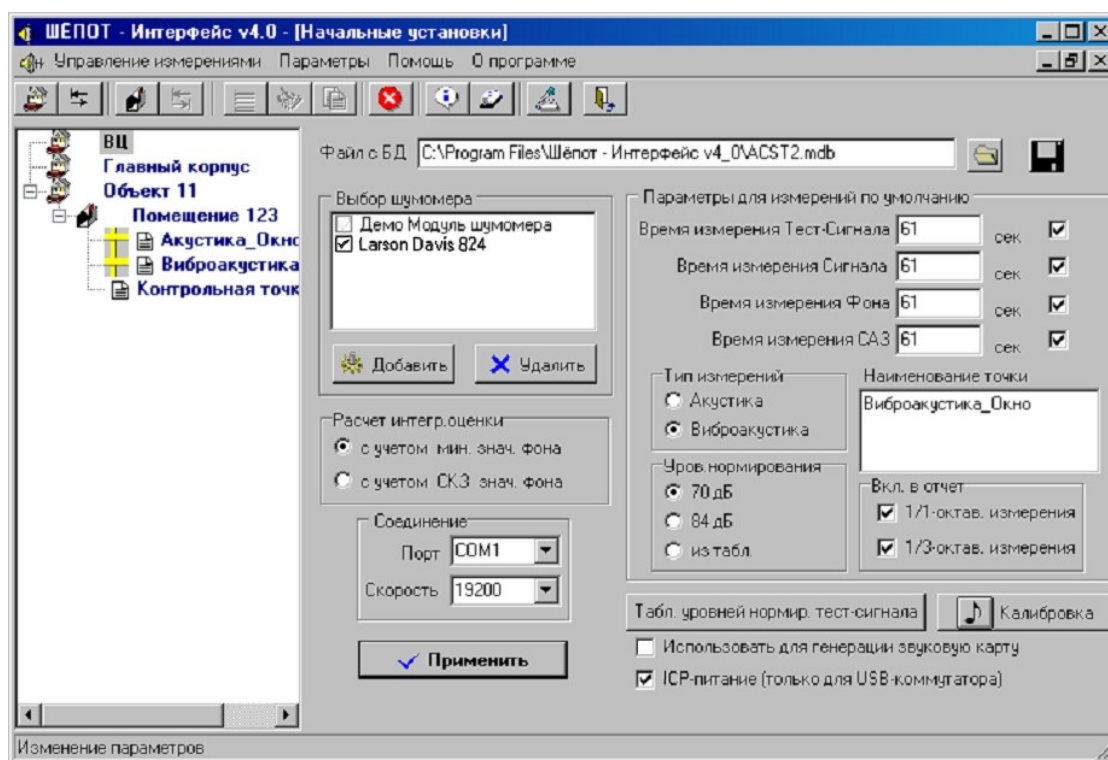


Рисунок 7. Окно «Начальные установки»

Вызов окна «Начальные установки» производится нажатием кнопки «Параметры соединения с шумомером и контрольной точки»  или выбором в меню «Параметры» позицию «Настройки БД, шумомера и по умолчанию».

Поле «**Параметры для измерений по умолчанию**» расположено в правой части окна начальных установок.

В верхней части поля расположены четыре окна установки временных параметров измерения - «**Время измерения тест-сигнала**», «**Время измерения сигнала**», «**Время измерения фона**» и «**Время измерения САЗ**». Указанные окна заполняются оператором с клавиатуры. Наименования временных параметров измерения приведены в табл. 3.

Справа от каждого из окон установки временных параметров измерения находится окно флага включения данного вида измерений в общий цикл при автоматическом режиме измерений. Общая продолжительность цикла измерений будет равна сумме времен, занесенных в окна, отмеченные флагами. По умолчанию все временные параметры цикла измерения приняты равными 61 секунде. Чем больше временные циклы измерения, тем точнее результаты.

В поле «**Тип измерений**» находятся кнопки установки типа проводимых измерений. Выбор типа измерений должен соответствовать типу исследуемого канала утечки информации и используемому средству измерения, расположенному на расстоянии от источника тестового акустического сигнала.

Таблица 3

Окно установки временных параметров измерения	Временные параметры измерения, установленные в окне, в секундах	
	Тип измерений «Акустика»	Тип измерений «Виброакустика»
«Время измерения тест-сигнала»	Продолжительность измерения уровня звукового давления шумомером, расположенным вблизи работающего источника тестового акустического сигнала	
«Время измерения сигнала»	Продолжительность измерения уровня звукового давления микрофоном, расположенным на расстоянии от работающего источника тестового акустического сигнала	Продолжительность измерения уровня наведенного виброускорения акселерометром, расположенным на расстоянии от работающего источника тестового акустического сигнала

«Время измерения фона»	Продолжительность измерения уровня фонового звукового давления микрофоном, расположенным на расстоянии от выключенного источника тестового акустического сигнала	Продолжительность измерения фонового уровня наведенного виброускорения акселерометром, расположенным на расстоянии от выключенного источника тестового акустического сигнала
«Время измерения САЗ»	Продолжительность измерения уровня звукового давления микрофоном, расположенным на расстоянии от выключенного источника тестового акустического сигнала, при работающих средствах защиты	Продолжительность измерения уровня наведенного виброускорения акселерометром, расположенным на расстоянии от выключенного источника тестового акустического сигнала, при работающих средствах защиты

Окно **«Наименование точки»** служит для присвоения имен новым записям результатов выполненных измерений при занесении их в базу данных (имя записи по умолчанию – **«Контрольная точка»**). Для новых записей в базу данных рекомендуется использовать имена с указанием типа выполняемого измерения и конструктивного элемента выделенного помещения (например, **«Акустика_Окно»**, **«Виброакустика_Окно»** вместо записи по умолчанию).

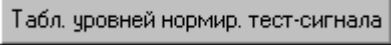
Поле **«Включить в отчет»** служит для определения номенклатуры результатов измерений, используемых для формирования отчета.

В поле **«Уровень нормирования»** находятся кнопки установки уровня нормирования (интегрального уровня речевого сигнала для различных видов русской речи), используемого при обработке результатов измерений.

Уровень нормирования может быть задан единым во всем диапазоне частот с привязкой к типу исследуемого помещения, либо заданным оператором для каждой из пяти октавных полос с центральными частотами 250, 500, 1000, 2000 и 4000 Гц:

«70 дБ» - для помещений без средств звукоусиления;

«84 дБ» - для помещений с установленными в них средствами звукоусиления;

«из таблицы» - уровни нормирования задаются оператором в таблице, показанной слева, открывающейся при нажатии кнопки  этого окна.

Различным видам речи соответствуют типовые интегральные уровни речевых сигналов, измеренные на расстоянии 1 м от источника речи (говорящий человек, звуковоспроизводящее устройство): $L_c = 70$ дБ - речь средней громкости; $L_c = 84$ дБ - очень громкая речь, усиленная техническими средствами. Уровень речевого сигнала в октавных полосах не является равномерным. Предлагается следующий вариант распределения уровня речевых сигналов в октавных полосах (табл.2).

Таким образом, выбором уровня нормирования определяется модель источника речевой информации.

Состояние установок в поле «**Расчет интегральной оценки**» определяет какой из результатов обработки измерений за время наблюдения будет использовано в дальнейших расчетах – минимальное из измеренных значений или, эквивалентное значение за время наблюдения, результатам измерений уровня фона. В соответствии с НМД в расчетах необходимо использовать минимальное значение уровня фона.

Поле «**Файл с БД**» для работы с файлами базы данных с кнопками открытия  и сохранения  расположено в верхней части окна. Оно предназначено для выбора оператором требуемого для работы файла базы данных. Шаблон файла базы данных «**ACST.mdb**» устанавливается при установке программы.

Загрузка, сохранение и переименование файла базы данных производится в порядке, аналогичном выполнению указанных процедур в ОС «Microsoft Windows».

Окна «Загрузка» и «Сохранить как», открываются при нажатии кнопок  и  соответственно. Вид окна «Сохранить как» показан на рис. 8.

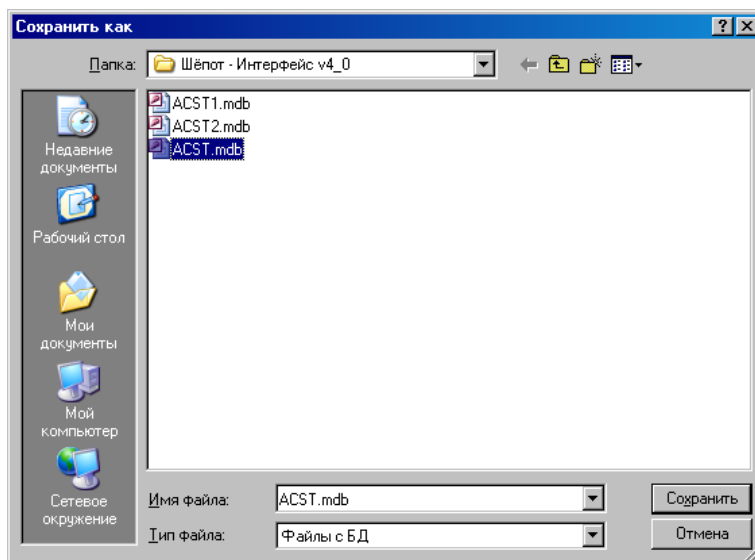


Рис. 8. Окно сохранения файла базы данных

При начале работы в окне **«Начальные установки»** необходимо загрузить файл базы данных с расширением **«*.mdb»**. После появления имени выбранного файла базы данных в окне поля **«Файл с БД»** для его открытия нажать кнопку **«Применить»** . При необходимости сохранить открытый файл базы данных под новым именем (например, **«Арсенал.mdb»**). Подготовленную базу данных можно использовать для обработки на другом компьютере. Для этого базу данных необходимо скопировать на другой компьютер, загрузить на этот компьютер программное обеспечение **«Шепот-Интерфейс»** и вставить HASP-ключ. Данный прием может использоваться тогда, когда при проведении измерений нельзя использовать ПЭВМ, сертифицированную для обработки закрытой информации, а протокол измерений должен быть закрытым. Кроме этого, база данных может быть заполнена информацией, полученной с использованием средств измерений, не входящих в комплект системы **«Шепот»**. Однако получение результатов расчетов возможно только при наличии HASP-ключа.

База данных выполненных измерений предназначена для хранения информации о месте проведения измерений (объект, помещение, контрольная точка) и о результатах измерений и расчетов в каждой контрольной точке. База

данных выполненных измерений имеет иерархическую структуру с тремя уровнями иерархии – «Объект», «Помещение», «Контрольная точка». На каждом из уровней иерархии возможно выполнение операций добавления и удаления элементов и редактирования информации, относящейся к конкретному объекту, помещению или контрольной точке.

Загрузка файла базы данных по умолчанию «Acst.mdb» происходит автоматически при запуске программы. Изменение подключенной базы данных и открытие требуемого файла с расширением «*.mdb» производится в поле «Файл с БД» «Окна начальных установок». Отображение элементов базы данных осуществляется в виде дерева в левой области главного окна работы программы. Каждый элемент древовидной базы данных должен иметь уникальное для своей ветки имя. Переход между элементами осуществляется щелчком левой клавиши «мыши».

Элементами управления базой данных в главном окне программы являются:

- кнопка «Добавление объекта» (Ctrl + Alt + O) ;
- кнопка «Просмотреть/Изменить параметры объекта» (Ctrl + Alt + V) ;
- кнопка «Добавление помещения» (Ctrl + Alt + R) ;
- кнопка «Просмотреть/Изменить параметры помещения» (Ctrl + Alt + P) ;
- кнопка «Добавить контрольную точку» (Ctrl + Alt + Q) ;
- кнопка «Просмотр контрольной точки» (Ctrl + Alt + M) ;
- кнопка «Копирование контрольной точки» (Ctrl + Alt + C) ;
- кнопка «Удаление элемента» (Ctrl + Alt + D) .

Переход в режим редактирования элемента базы данных осуществляется двойным щелчком левой клавиши «мыши» на нем. При этом будет открыто соответствующее данному элементу и его уровню иерархии диалоговое окно редактирования **«Просмотреть/Изменить параметры объекта (помещения, контрольной точки)»**.

При нажатии кнопки **«Добавление объекта»** (Ctrl + Alt + O)  открывается окно **«Добавление объекта»**, показанное на рис. 8. При нажатии кнопки **«Просмотреть/Изменить параметры объекта»** (Ctrl + Alt + V)  или при двойном щелчке левой клавиши «мыши» по выделенному объекту – окно **«Объект»**, показанное на рис. 9.

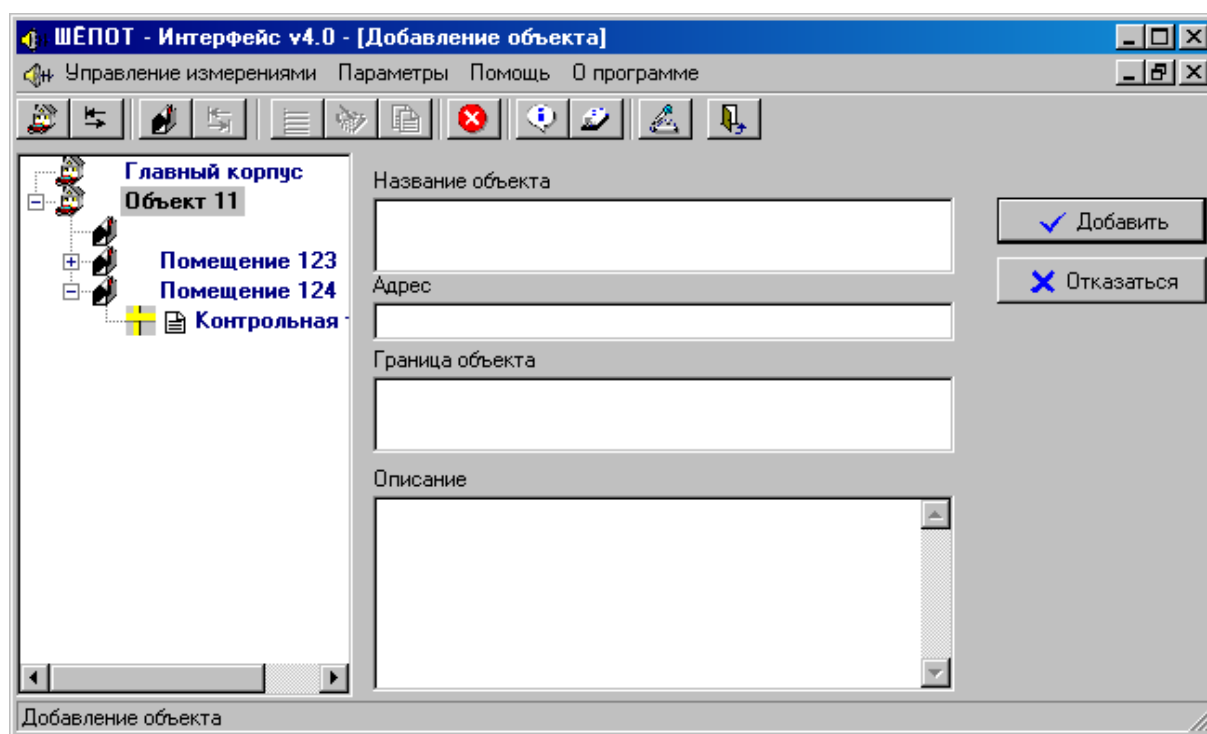


Рис. 9. Окно «Добавление объекта»

Вид окон **«Добавление объекта»** и **«Объект»** (рис. 10) практически идентичен, за исключением вида кнопок ввода результатов редактирования ( и ) и наличия ранее введенной информации об объекте в окне **«Объект»**.

При нажатии кнопки **«Добавление помещения»** (Ctrl + Alt + R)  открывается окно **«Добавление помещения»**, показанное на рис. 11. При

нажатии кнопки «**Просмотреть/Изменить параметры помещения**» (Ctrl + Alt + P)  или при двойном щелчке левой клавиши «мыши» по выделенному помещению – окно «**Помещение**», показанное на рис. 11.

Вид окон «**Добавление помещения**» и «**Помещение**» (рис.11, 12) также практически идентичен, за исключением вида кнопок ввода результатов редактирования ( и ) и наличия ранее введенной информации о помещении в окне «**Помещение**».

Указанные окна содержат требующие заполнения вкладки описания помещения – «**Ограждающие конструкции**», «**Инженерные конструкции**», «**Окна**», «**Двери**» и «**Параметры САЗ**». Информации этих вкладок используется при формировании отчета по результатам проведенных исследований и сохраняется в базе данных программы.

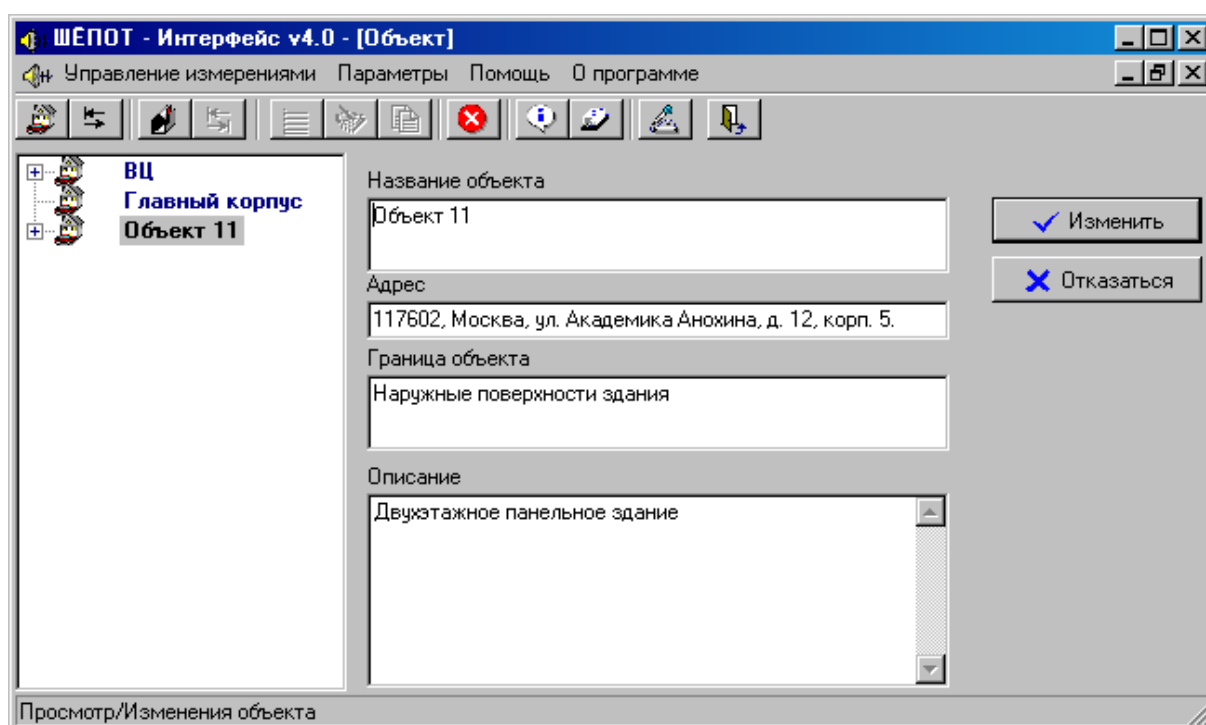


Рис. 10. Окно «Объект»

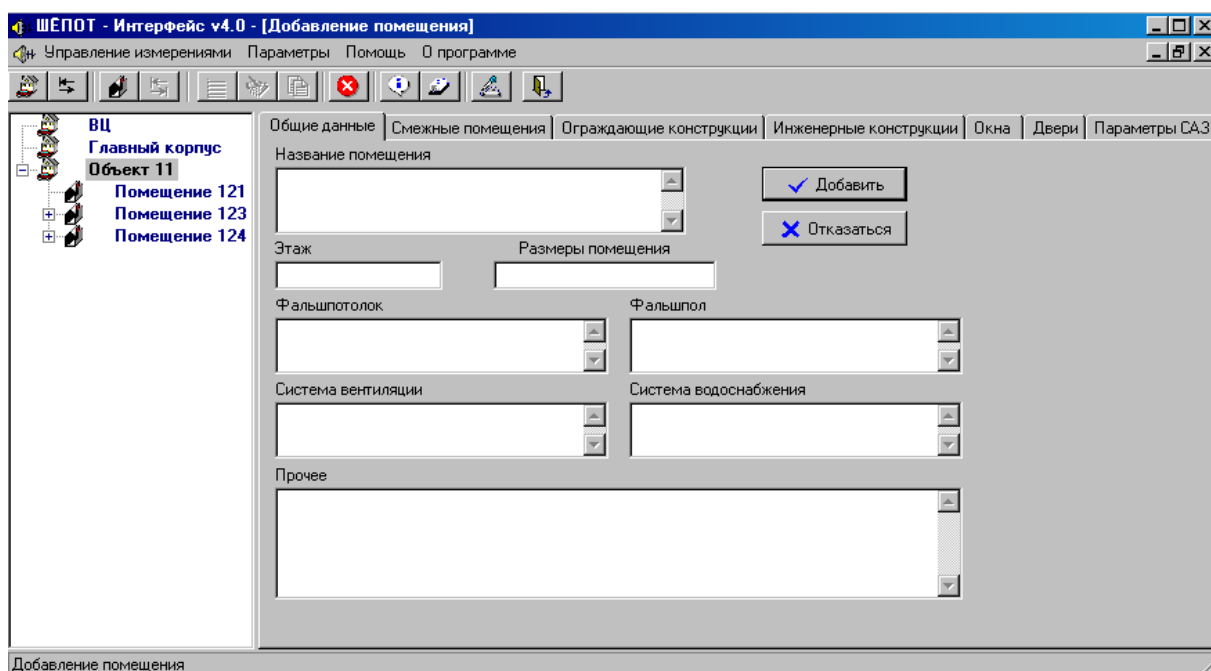


Рис. 11. Окно «Добавление помещений»

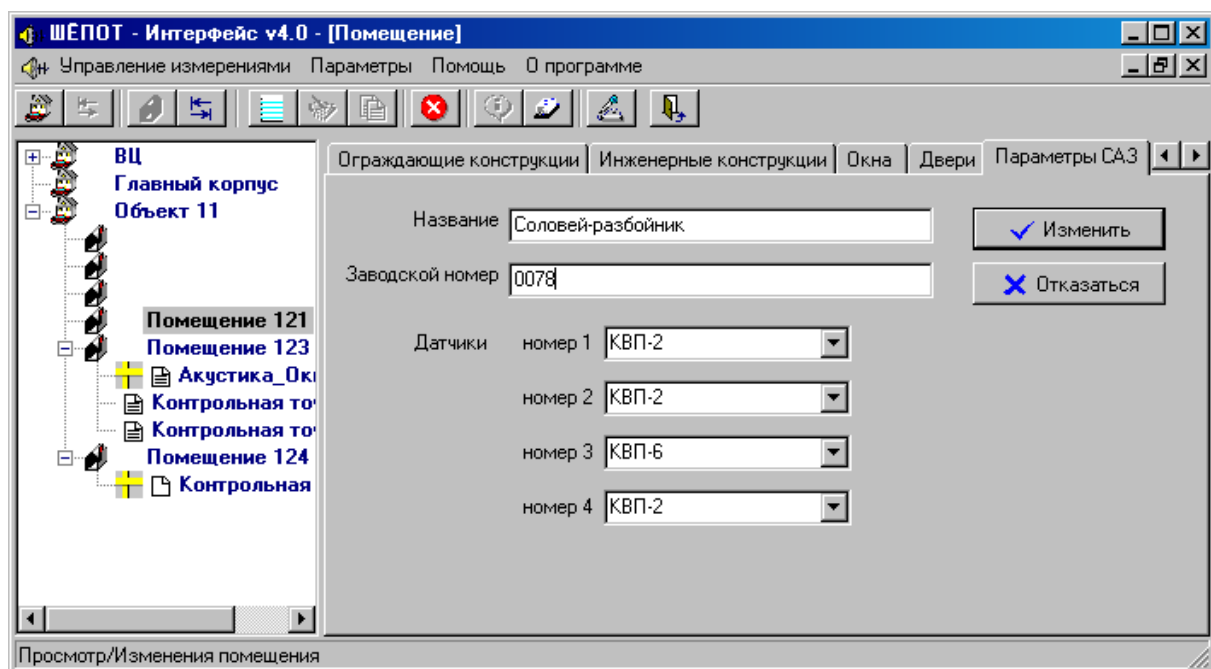


Рис. 12. Окно «Помещение»

После завершения ввода данных в поля окон необходимо нажатие кнопок «Добавить» или «Изменить» для их ввода в базу данных.

При заполнении полей окон на уровнях «Объект» и «Помещение» необходимо соблюдать определенные правила.

«Объект» - элемент верхнего уровня иерархии базы данных – имеет следующие атрибуты:

- **«Название объекта»** - обязательное поле ввода уникального имени объекта в файле базы данных. Оно может быть полем данных до 254 знаков ($2^8 - 2$ служебных символа). В окне с набором уже введенных мест проведения исследований в левой части главного окна программы будет отображаться только первая строка данного поля;
- **«Адрес»** - поле ввода почтового адреса здания, в котором размещен объект защиты, длиной до 254 знаков;
- **«Границы объекта»** - многострочное поле описания границ, за пределы которых не должна вскрываться защищаемая речевая информация (объем до 64000 знаков);
- **«Описание»** - многострочное поле ввода дополнительных сведений по объекту (объем до 64000 знаков).

«Помещение» - элемент среднего уровня иерархии базы данных – имеет следующие атрибуты:

- **«Название помещения»** - обязательное поле ввода уникального имени выделенного помещения данного объекта (формат поля – текстовый 254 символа). В окне с набором уже введенных мест проведения исследований в левой части главного окна программы будет также отображаться только первая строка данного поля.
- **«Этаж»** - номер этажа, на котором расположено помещение (формат поля – числовой, до 254 символов);
- **«Размеры помещения»** - размеры помещения в метрах (формат поля – текстовый, до 254 символов);
- **«Фальшпол», «Фальшпотолок», «Система вентиляции», «Система водоснабжения»** - информация о соответствующих

системах, смонтированных в помещении (формат полей – текстовый, до 254 символов);

- **«Прочее»** - многострочное поле ввода дополнительных сведений помещению (объем до 64000 знаков);

- **Вкладка «Смежные помещения».** В поля данной вкладки вводятся названия (и/или номера) и краткие характеристики смежных помещений по всем шести направлениям от выделенного помещения (формат полей – текстовый, до 254 символов);

- **Вкладка «Ограждающие конструкции».** В поля данной вкладки вводятся характеристики стен, перегородок, перекрытий потолка и пола выделенного помещения. (формат полей – текстовый, до 254 символов);

- **Вкладка «Инженерные конструкции».** В поля данной вкладки вводятся характеристики различных систем, размещенных в выделенном помещении. Формат полей левого столбца – текстовый до 254 символов, правого – числовой до 254 символов;

- **Вкладка «Окна».** В поля данной вкладки заносятся характеристики всех окон в выделенном помещении. Формат полей **«Количество»**, **«Толщина стекла»** и **«Фрамуг в окне»** - числовой до 254 символов, остальных полей – текстовый до 254 символов;

- **Вкладка «Двери».** В поля данной вкладки вводятся характеристики всех дверей в выделенном помещении. Форматы полей заданы в соответствии с заносимыми данными (текстовые или числовые);

- **Вкладка «Параметры САЗ».** В полях данной вкладки вводятся данные об установленных в помещении средствах активной акустической и вибрационной защиты (при их наличии). В поле

«**Название**» рекомендуется заносить тип (модель) генератора САЗ. Ввод типов датчиков САЗ производится выбор из выпадающего списка или с клавиатуры.

В каждом помещении должна быть хотя бы одна контрольная точка. Добавление контрольной точки осуществляется нажатием кнопки «**Добавить контрольную точку**» (Ctrl + Alt + Q) . При этом открывается окно «**Новая контрольная точка**», показанное на рис.13.

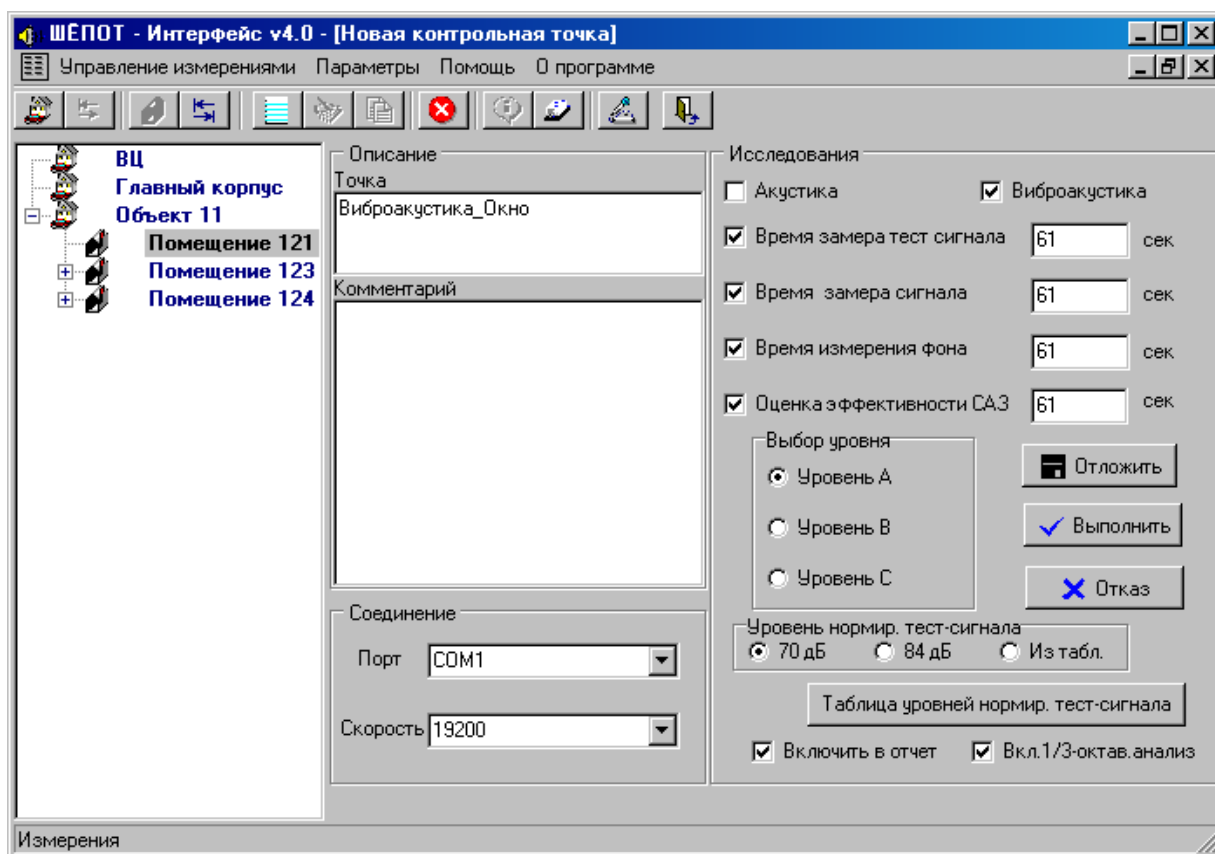


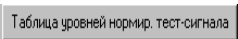
Рис. 13. Окно «Новая контрольная точка»

Окно «**Новая контрольная точка**» открывается с уже записанными в нем условиями проведения измерений и использования их результатов в отчете:

- типом измерений;

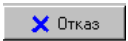
- временными параметрами цикла измерения;
- уровнем нормирования (интегральным уровнем речевого сигнала для различных видов русской речи);
- параметрами соединения с шумомером;
- номенклатурой результатов измерений, используемых для формирования отчета.

Изначально записанные в окне **«Новая контрольная точка»** условия проведения измерений соответствуют заданным программой или оператором как «условия по умолчанию» в окне «Начальные установки». Текст в окне «Точка» поля «Описание» соответствует шаблону имени контрольной точки, также заданному в окне «Начальные установки».

Уровни нормирования в таблице уровней нормированного тест-сигнала  при открытии окна соответствуют заданным оператором как «значения по умолчанию» в таблице окна «Начальные условия». Требуемый уровень оценки – **А**, **В** или **С** должен быть установлен оператором, исходя из цели и условий исследования объекта.

Кнопка **«Выполнить»**  - запуск процедуры измерений. После завершения измерений отображение контрольной точки на ее уровне в дереве базы данных будет отмечено знаком .

Кнопка **«Отложить»**  - сохранить контрольную точку для проведения измерений в более позднее время. Эту кнопку рекомендуется использовать для заблаговременного создания в базе данных набора контрольных точек перед проведением измерений на исследуемом объекте.

Кнопка **«Отказ»**  - отказ от создания новой контрольной точки.

«Контрольная точка» - элемент нижнего уровня иерархии базы данных. При заполнении полей окон на уровне **«Контрольная точка»** необходимо соблюдать определенные правила.

- **«Название точки»** - обязательное поле ввода уникального имени контрольной точки для данного помещения (формат поля – текстовый до 254 символов);
- **«Комментарий»** - многострочное поле ввода дополнительных сведений по контрольной точке объекту (объем до 64000 знаков).
- **«Включить в отчет»** - флаги включения информации об октавных и третьоктавных измерениях в данной контрольной точке в отчет по результатам выполненных работ.
- **«Выбор уровня»** - кнопки выбора оператором нужного ему набора отношений «сигнал/шум» в октавных полосах в зависимости от уровня исследуемого помещения - А, В или С.
- **«Уровень нормирования тест-сигнала»** - кнопки выбора оператором уровня нормирования тест-сигнала:
- **«70 дБ»** - для помещений без средств звукоусиления;
- **«84 дБ»** - для помещений с установленными в них средствами звукоусиления;
- **«из таблицы»** - уровни нормирования проверяются и при необходимости редактируются оператором применительно к данной контрольной точке в таблице уровней нормирования тест-сигнала в пяти октавных полосах, открываемой при нажатии кнопки

Таблица уровней нормир. тест-сигнала

Введение уровня нормирования необходимо для выполнения расчета отношения сигнал/шум.

После завершения ввода данных в поля окон и вкладок работы с контрольной точкой необходимо нажатие кнопок **«Выполнить»**, **«Отложить»** или **«Изменить»** для их ввода в базу данных.

При нажатии кнопки **«Просмотр контрольной точки»** (Ctrl + Alt + M)  или при двойном щелчке левой клавиши «мыши» по выделенной точке контроля открывается окно с именем этой точки, показанное на рис. 14.

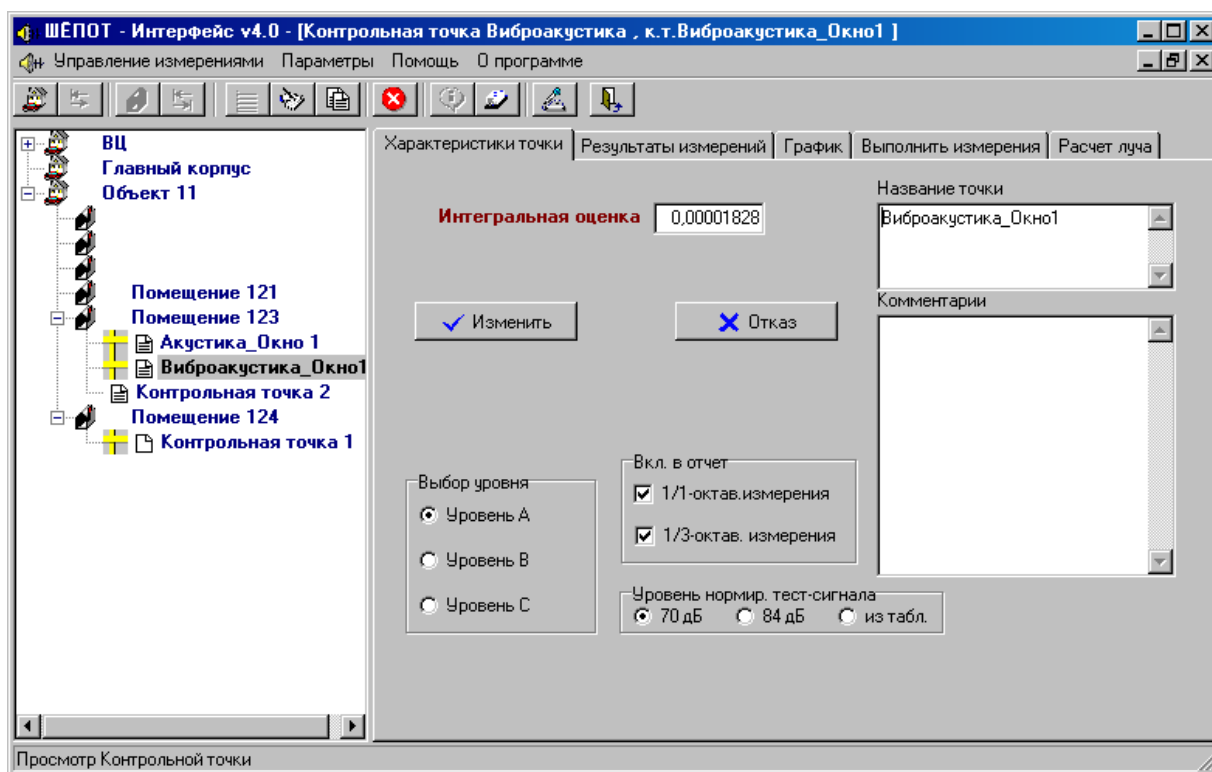


Рис. 14. Окно просмотра результатов измерений в контрольной точке (вкладка «Характеристики»)

Окно просмотра результатов измерений в контрольной точке содержит пять вкладок – **«Характеристики»**, **«Результаты измерений»**, **«График»**, **«Выполнить измерения»** и **«Расчет луча»** (рис.15-17). Вкладки окна допускают возможность редактирования содержащейся в них информации. Поля вкладки **«Характеристики»** дублируют поля окна **«Новая контрольная точка»** (рис. 13).

Значения интегральной оценки на вкладках **«Характеристики»** и **«Результаты измерений»** совпадают.

Вкладка **«Результаты измерений»** (рис.15) содержит следующие данные:

- В строке «Тест-сигнал» отображается среднее за время измерения значение уровня звукового давления от источника тестового акустического сигнала в каждой октавной полосе, измеренное в точке установки 1-го микрофона;
- В строке «Сигнал» - отображается среднее за время измерения значение уровня звукового давления (или виброускорения) от источника акустического тестового сигнала в каждой октавной полосе, измеренное в точке установки 2-го микрофона (акселерометра);

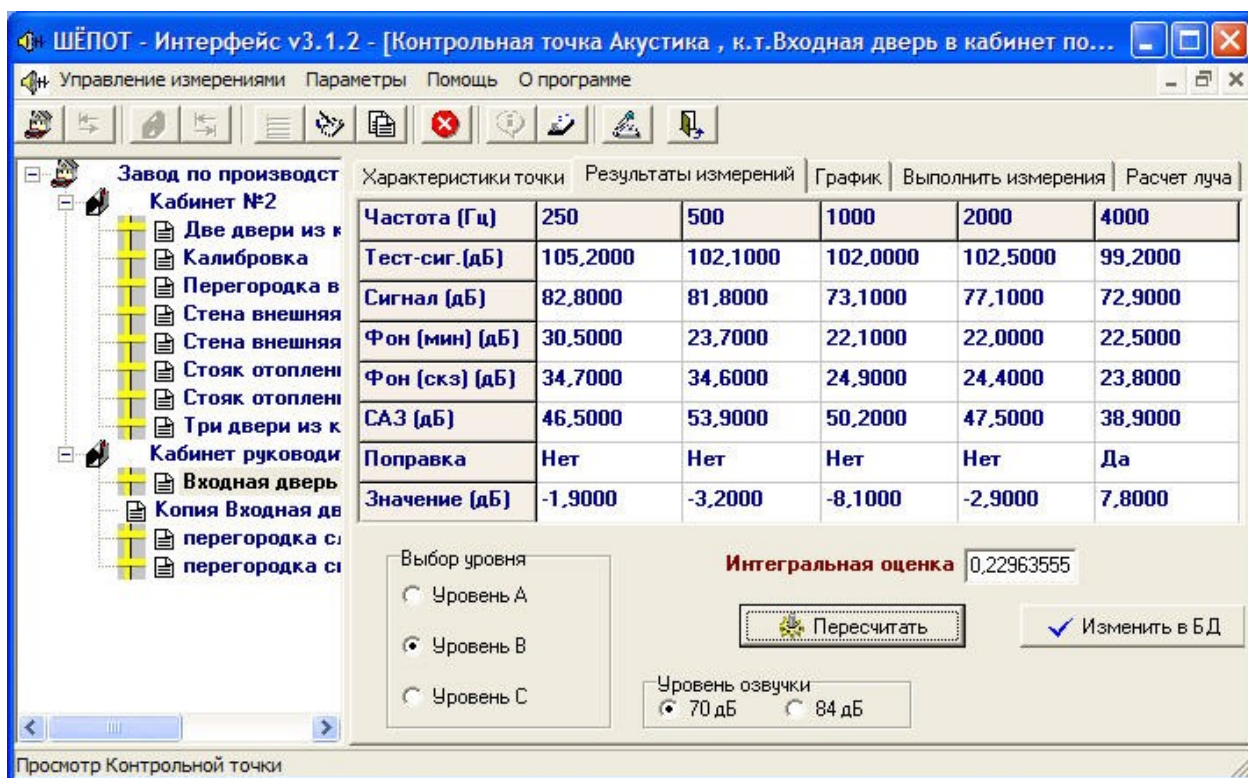


Рис. 15. Окно просмотра результатов измерений в контрольной точке
(вкладка «Результаты измерений»)

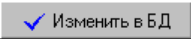
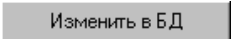
- В строке «Фон (мин)» отображается минимальное значение уровня звукового давления (или виброускорения) в каждой октавной полосе, измеренное в точке установки 2-го микрофона
- В строке «Фон (скз)» - отображается среднее за время измерения значение уровня звукового давления (или виброускорения) фона в каждой октавной полосе, измеренное в точке установки 2-го микрофона (акселерометра). Если разница между уровнем сигнала и

средним значением фона меньше 10 дБ, то система выдает предупреждение о необходимости увеличения уровня тестового сигнала;

- В строке «САЗ» - отображается среднее за время измерения значение уровня звукового давления (или виброускорения) от источника сигнала системы САЗ в каждой октавной полосе, измеренное в точке установки 2-го микрофона (акселерометра), расположенного на расстоянии от источника тестового акустического сигнала;

- В строке «Поправка» - отображается результат логического сравнения вычисленного отношения сигнал/шум с введенными нормированными отношениями. Если показатель равен «ДА», то это означает, что в данной октавной полосе выполняются требования. Если показатель равен «НЕТ» - то требования не выполняются.

- В строке «Значение» - отображается требуемая величина уровня помехи для того, чтобы выполнить требования по защите.

Кнопка «Пересчитать»  служит для запуска процедуры расчета значения интегральной оценки и построения графиков после внесения изменений в таблицу результатов измерений в октавных полосах. Результаты пересчета будут сохранены в базе данных только после нажатия кнопок  или .

На вкладке «График» в графическом виде (рис.16) представлены результаты проведенного измерения.

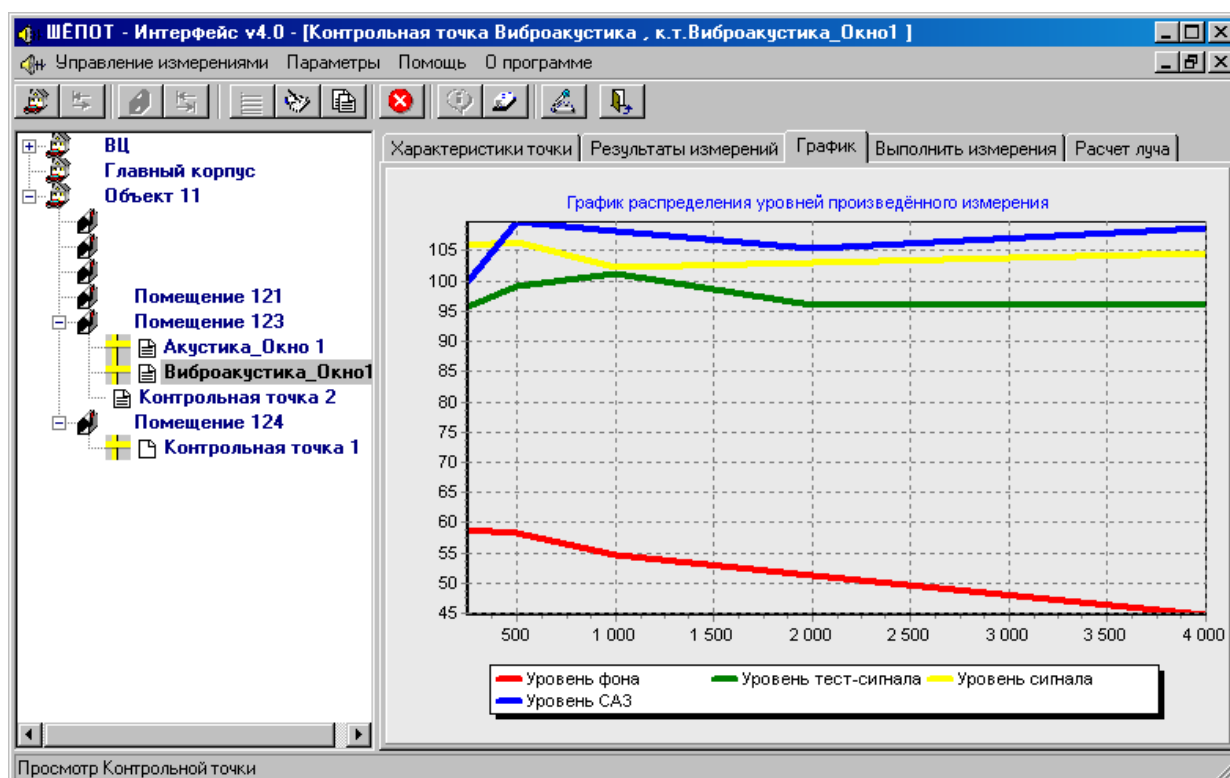


Рис. 16. Окно просмотра результатов измерений в контрольной точке (вкладка «График»)

Вкладка «**Выполнить измерения**» (рис. 17) предназначена для запуска измерения в отложенной контрольной точке или для повторения измерения в данной точке при тех же или измененных в этом окне условиях.

Кнопка «**Выполнить**»  служит для запуска процедуры измерения с установленными на этой вкладке параметрами. По завершении измерения автоматически открывается вкладка «**Результаты измерений**» (рис. 15) с заполненной таблицей результатов.

Для сохранения записи ранее полученных результатов измерения в базе данных перед повторением измерения необходимо предварительно скопировать текущую запись в базе данных с помощью процедуры «**Копирование контрольной точки**» . Данный режим работы программы позволяет создать новую контрольную точку с тем же набором относящейся к ней информации в базе данных, что и у любой предварительно выбранной и выделенной оператором контрольной точки или только с частью такого набора

по выбору оператора. Новая контрольная точка будет создана в том же помещении, что и исходная контрольная точка.

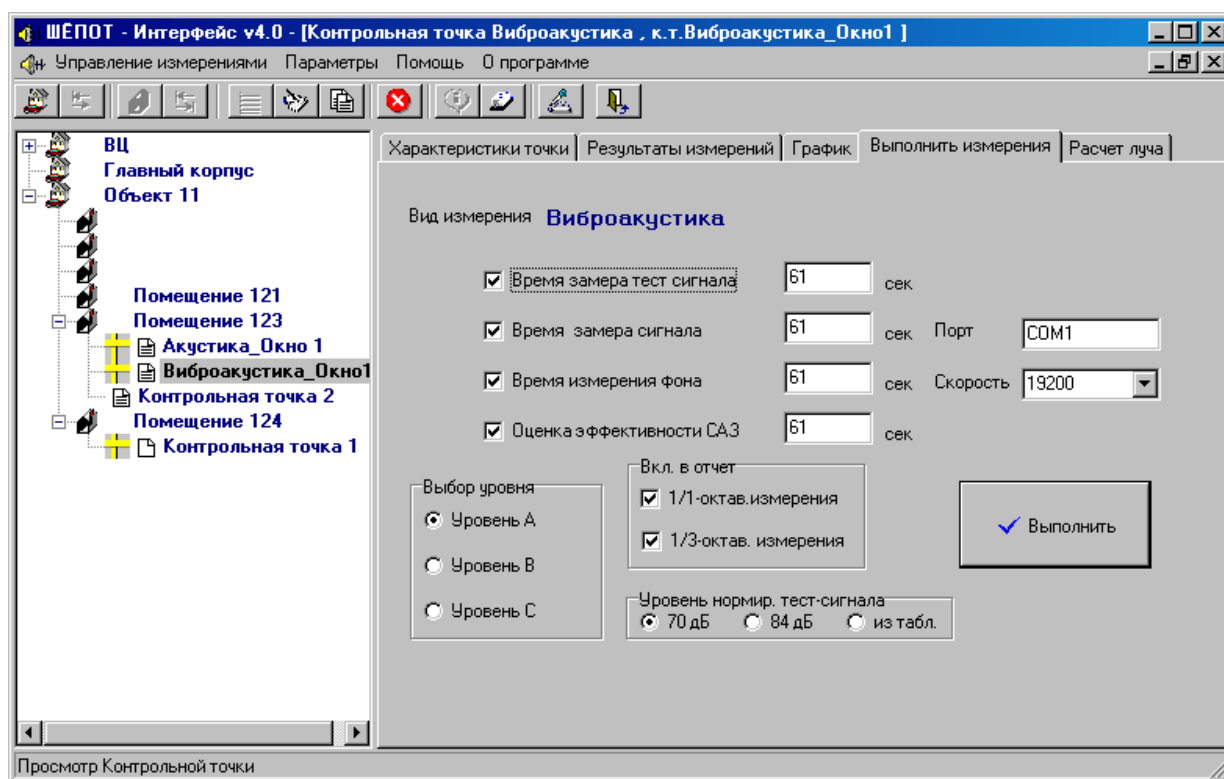


Рис. 17. Вкладка «Выполнить измерения»

При нажатии кнопки **«Копирование контрольной точки»**  открывается окно этого режима работы, показанное на рис. 18, в котором задаются параметры копирования.

В верхней части окна выводится элемент **«Копируемая контрольная точка»**, в котором указано имя копируемой контрольной точки. Информацию в данном элементе изменить нельзя.

Ниже располагается окно **«Новое имя»**, в котором необходимо указать новое имя для создаваемой контрольной точки. По умолчанию в нем указывается имя копируемой контрольной точки с добавлением постфикса **«_копия»**. Если копирование уже производилось, то в этом окне сохраняется последнее имя, присвоенное оператором при копировании.

Ниже располагается поле «**Копировать**», внутри которого расположены окна установки флагов выбора копируемой информации:

- «**Описание**» - копируется описание исходной контрольной точки;
- «**Тип измерений**» - в новую точку копируется тип измерений исходной контрольной точки.

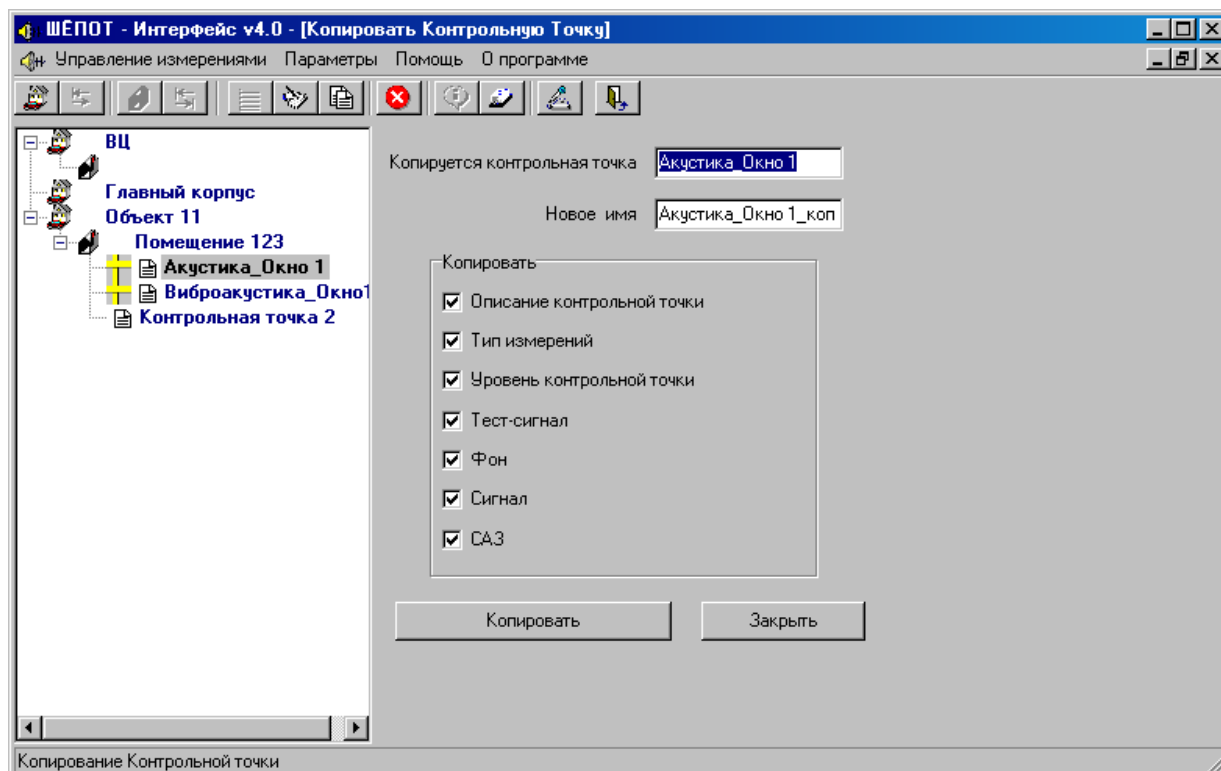


Рис. 18. Окно «Копирование контрольной точки»

Если установлен флаг «**Тип измерений**», у новой точки будут скопированы с исходной:

- тип измерений («**Акустика**» или «**Виброакустика**»);
- комбинация флагов выбора – «**Тест-сигнал**», «**Фон**», «**Сигнал**» и «**САЗ**».

Если флаг «**Тип измерений**» не установлен, программа назначит для новой точки:

- тип измерений – «**Акустика**»

- все флаги видов измерений - «Тест-сигнал», «Фон», «Сигнал» и «САЗ» в выключенном состоянии.

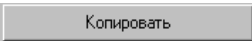
«Уровень контрольной точки» - в новую точку копируется уровень исходной контрольной точки. Если этот флаг не установлен, то новой точке по умолчанию будет назначен уровень контрольной точки - А.

«Тест-сигнал» - в новую точку копируются результаты измерения тест-сигнала в семи октавных полосах и при наличии - и девятнадцати третьоктавных полосах исходной контрольной точки. Если этот флаг не установлен, то в копируемую точку в этот раздел результатов измерений пишутся нули.

«Фон» - в новую точку копируются результаты измерения фона в семи октавных полосах и при наличии - и девятнадцати третьоктавных полосах исходной контрольной точки. Если этот флаг не установлен, то в копируемую точку в этот раздел результатов измерений пишутся нули.

«Сигнал» - в новую точку копируются результаты измерения в семи октавных полосах и при наличии - и девятнадцати третьоктавных полосах исходной контрольной точки. Если этот флаг не установлен, то в копируемую точку в этот раздел результатов измерений пишутся нули.

«САЗ» - в новую точку копируются результаты измерения сигнала САЗ в семи октавных полосах и при наличии - и девятнадцати третьоктавных полосах исходной контрольной точки. Если этот флаг не установлен, то в копируемую точку в этот раздел результатов измерений пишутся нули.

После завершения ввода имени новой точки и копируемых в нее данных необходимо нажатие кнопки «Копировать»  для записи новой точки в базу данных. Окно «Копирование контрольной точки» при этом не закрывается и возможно повторное (многократно) копирование исходной контрольной точки в новые точки. Рядом с этой кнопкой находится кнопка «Заккрыть» по нажатию которой происходит закрытие окна.

Кнопка «**Отчет по объектам**»  включает режим формирования и просмотра протокола по результатам выполненных измерений с возможностью его редактирования и сохранения под новым именем. В протокол будет включена информация по всем отмеченным знаком  контрольным точкам объекта, выделенного цветом в дереве базы данных.

В случае отсутствия выбранного в дереве базы данных объекта, программа выдаст напоминание о необходимости такого выбора.

Вид протокола по результатам проведенных измерений зависит от выбора текстового редактора в поле «**Вывод отчета**» и выбора шаблона вывода в поле «**Вид таблицы**».

При выборе для вывода отчета текстового редактора «**Notepad**» («**Блокнот**») протокол по результатам выполненных измерений выводится в окне просмотра, вид которого показан на рис. 19.

Сохранение отчета в файл осуществляется кнопкой «**Сохранить**»  с помощью стандартной функции Windows. Текст отчета может быть полностью скопирован и перенесен для редактирования в текстовый редактор «**Word**».

При выборе для вывода отчета текстового редактора «**Word-97**» или «**Word-2000**» протокол по результатам выполненных измерений выводится в окне документа такого текстового редактора.

Отчёт

Контрольная точка Акустика_Окно 1

Описание

Уровень В

Частота (Гц)	125	250	500	1000	2000	4000	8000
Тест-сиг. (дБ)	95,1	100,2	95,7	98,2	93,2	99,0	96,8
Уров. сиг. (дБ)	59,4	64,6	68,1	75,6	70,4	63,6	62,3
Уров. фона (дБ)	33,1	31,8	24,8	21,3	17,7	12,7	9,6
Уров.ф.(скз)(дБ)	35,9	33,8	27,0	22,4	19,0	13,6	10,1
Уров. САЗ (дБ)	58,7	76,9	61,3	74,8	72,3	79,0	69,0
Выполнение С/Ш		Да	Да	Да	Да	Да	
Lci[Uci] (дБ)	59,40	64,55	68,07	75,57	70,40	63,56	62,27
Lci[Uci]-d (дБ)		30,36	38,36	38,41	33,21	17,54	
Ei (дБ)		-46,58	-22,93	-36,37	-39,12	-61,43	
z		0	0	0	0	0	
ri		0,0000	0,0001	0,0000	0,0000	0,0000	
R = 0,000141							
Интегральная оценка (W) = 0,000259							

Результаты измерений в 1/3-октавных полосах

Частота (Гц)	125	160	200	250	315	400	500	630	800	1000
Тест-сиг. (дБ)	89,3	91,8	95,9	95,8	94,4	95,1	84,5	82,6	129,0	122,0
Уров. сиг. (дБ)	55,7	51,4	54,5	60,4	61,7	56,5	67,6	53,8	71,7	54,7
Уров.ф.мин.(дБ)	27,1	30,1	29,1	23,0	27,0	24,0	15,1	13,1	18,0	13,0
Уров.ф.скз (дБ)	29,8	33,1	32,0	25,4	29,6	26,4	16,6	14,4	19,8	14,3
Уров. САЗ (дБ)	54,3	53,1	75,9	69,9	56,6	55,7	54,2	58,5	72,6	70,3

Сохранить

Рис. 19. Протокол по результатам измерений в одной точке в окне просмотра текстового редактора «Notepad» (пример).

3. Оборудование и материалы

Лаборатория аудита защиты информации, оснащенная Комплексом оценки защищенности выделенных помещений по виброакустическому каналу «Шепот». Программное обеспечение: Программа управления системой «Шепот» и расчёта показателей защищённости выделенных помещений по виброакустическому каналу «Шепот-Интерфейс» Версия 4.0.0.

4. Порядок выполнения работы.

Порядок выполнения измерений в автоматическом режиме:

осуществить сборку системы в соответствии с рис.20.

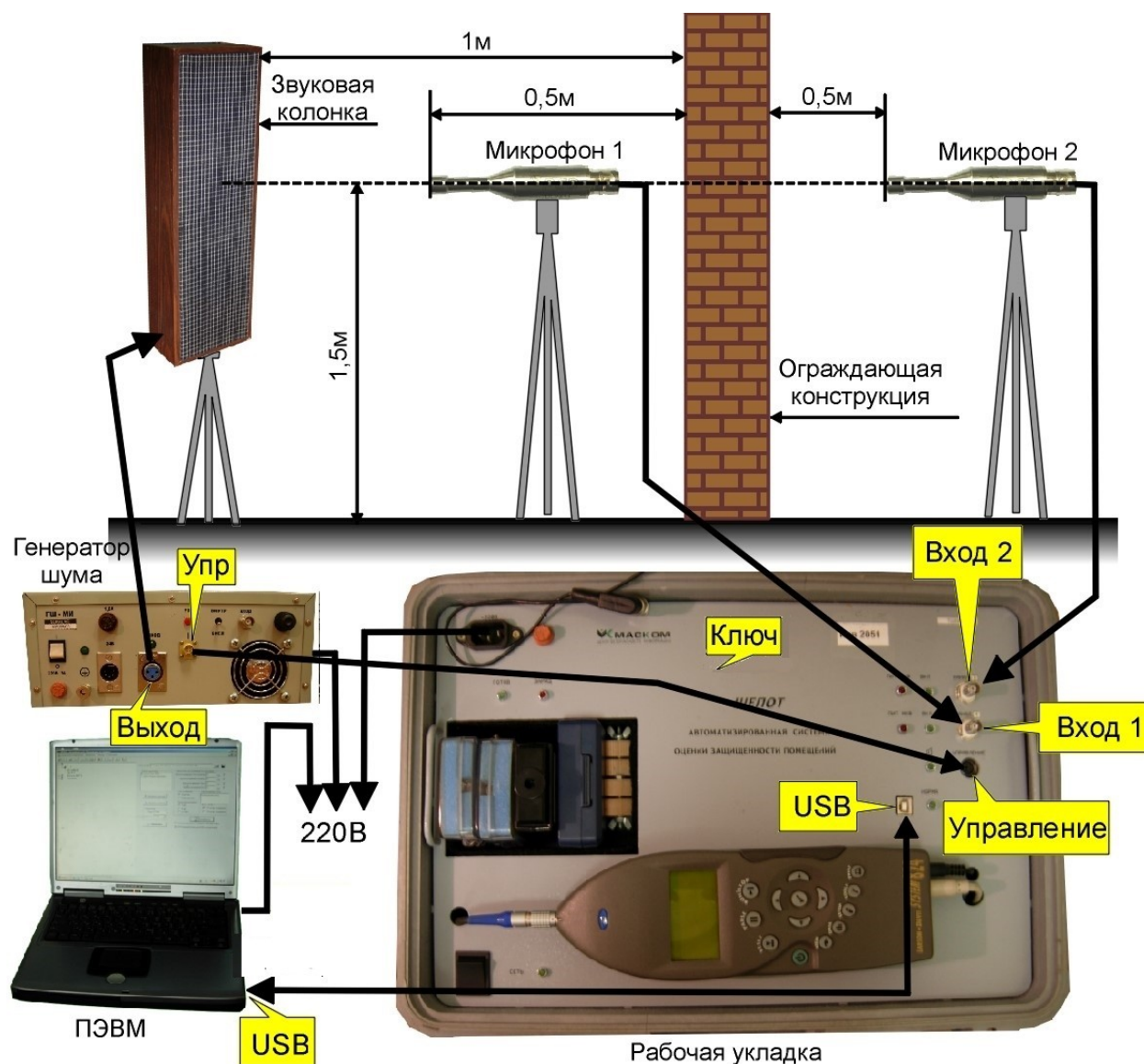


Рисунок 20. Схема соединений системы для проведения акустических измерений

включить электропитание генератора «Шорох-2МИ», ПЭВМ, рабочей укладки, приемника и передатчика.;

запустить на управляющем компьютере программу «Шепот-Интерфейс»;

провести калибровку системы «Шепот» согласно приложению 1;

ввести в окне «**Настройка отчета и уровней**» гипотетические значения показателей сигнал/шум:

- для подгруппы 1 - уровня А,
- для подгруппы 2 – уровня В,

- для подгруппы 3 – уровня С;

Задать «**Уровень нормирования**» для помещений с установленными в них средствами звукоусиления;

проверить правильность установок окна «**Начальные установки**». Параметры поля «**Соединение**», «**Порт**» (могут не совпадать). Убрать флаг «**Время измерения САЗ**», т.к. в данной лабораторной работе не будет оцениваться эффективность САЗ. Выбрать тип измерений «**Акустика**»;

Загрузить ранее созданную, при проведении измерений на двери, базу данных. Сохранить сформированную базу данных в отдельную папку с именем подгруппы. Сформированная база данных будет использоваться в других лабораторных работах.

Создать в базе данных запись «**Объект**» с описанием исследуемого объекта и записи «**Помещение**» с описанием исследуемых выделенных элементов;

Создать в базе данных записи по выбранной контрольной точке;

После заполнения полей ввода параметров и условий проведения измерений нажать кнопку «**Выполнить**»  для запуска процедуры измерений.

По завершении измерения в данной контрольной точке автоматически откроется вкладка «**Результаты измерений**» в окне «**Просмотр контрольной точки**».

Отображение контрольной точки на ее уровне в дереве базы данных будет отмечено знаком ;

Переместить элементы системы в новую контрольную точку;

Повторить пункты 10 и 11. Для сокращения времени при формировании записи новой контрольной точки использовать процедуру «**Копирование контрольной точки**» Новая контрольная точка будет создана в том же помещении, что и исходная контрольная точка;

Подготовить протокол, для чего нажать кнопку «Отчет по объектам»



. Скорректировать представленную в отчете информацию.

Произвести расчет разборчивости речи W с помощью ПО УЛМК_Расчет АВАК (.xls).

Составить отчет.

В конце отчета сформулировать вывод о наличии каналов утечки речевой информации через двери и о необходимости защиты. Критерии оценки:

- 1) отношение сигнал/шум для уровня по заданию преподавателя (см. приложение 2);
- 2) разборчивость речи W (табл. 2– Цель защиты: Скрыть предмет переговоров);

Ответить на контрольные вопросы.

5. Оформление отчета

Отчет по лабораторной работе оформляется в программной оболочке MicrosoftWord в электронном виде в формате .doc. На титульном листе указываются:

- наименование учебного учреждения,
- наименование дисциплины,
- название и номер работы, вариант,
- выполнил: фамилия, имя, отчество, студента, курс, группа,
- проверил: должность, ФИО преподавателя.

Отчет должен содержать:

1. Название, цели и задачи лабораторной работы;
2. Скриншоты о проделанной работе;
3. Заключение и выводы;