

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шебзухова Татьяна Александровна
Должность: Директор Пятигорского института (филиал) Северо-Кавказского
федерального университета
Дата подписания: 23.08.2023 15:53:25
Уникальный программный ключ:
d74ce93cd40e39275c3ba2f58486412a1c8ef96f

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**

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

Пятигорск, 2022 г.



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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 понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИД-1_{ОПК-9} При решении задач профессиональной деятельности использует современные информационные технологии и понимает принципы их работы. ИД-2_{ОПК-9} Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает современные информационные технологии. ИД-3_{ОПК-9} Владеет навыками применения современных информационных технологий для решения задач профессиональной деятельности.	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.
ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ Сертификат: 12000002A633E3D113AD425FB50002000002A6 Владелец: Шебзухова Татьяна Александровна Действителен: с 20.08.2021 по 20.08.2022		ОПК-10: Способен в качестве технического специалиста знать меры по обеспечению информационной безопасности

специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	безопасности и методы 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.	принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты
ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ИД-1 ПК-4 Имеет знания виды комплексного подхода в организации политики информационной безопасности. ИД-2 ПК-4 Умеет формулировать, настраивать политики безопасности. ИД-3 ПК-4 Владеет навыками формулирования и контролирования соблюдения требований политики безопасности.	сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности; проведение предварительного технико-экономического обоснования проектных расчетов.
ПК-5 Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям	ИД-1 ПК-5 Знает нормативную документацию по аттестации объектов информатизации. ИД-2 ПК-5 Способен выполнять требования безопасности хранения и обработки информации. ИД-3 ПК-5 Обладает навыками аттестации объектов информации по средствам требований информатизации.	участие в разработке проекта комплексных систем безопасности объектов информатизации

3. Технологическая карта самостоятельной работы студента

№	Раздел (тема) дисциплины	Реализуемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем, часов	Самостоятельна
Сертификат: 12000002A633E3D113AD425FB50002000002A6 Владелец: Шебзухова Татьяна Александровна Действителен: с 20.08.2021 по 20.08.2022				

			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	я работ а, часов
5 семестр							
1	Введение в цифровые технологии	ОПК-9, ОПК-10, ПК-4, ПК-5	3	6	3		27
2	Интернет-технологии	ОПК-9, ОПК-10, ПК-4, ПК-5	3	6	3		
3	Электронные почтовые сервисы	ОПК-9, ОПК-10, ПК-4, ПК-5	3	6	3		
4	Информационная безопасность и её составляющие	ОПК-9, ОПК-10, ПК-4, ПК-5	4,5	9	4,5		
	Итого за 5 семестр		13,5	27	13,5		27
	Итого		13,5	27	13,5		27

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

Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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 электрооборудования

3. Физические основы возникновения ТК АЭП в ВТСС

4. Средства пассивной защиты информации по каналу АЭП

5. Низкочастотные и высокочастотные излучения технических средств

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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, грубые ошибки в ответах, непонимание сущности излагаемых вопросов, неуверенные и неточные ответы на дополнительные вопросы.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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**

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

Пятигорск, 2022 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».

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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

ДОКУМЕНТ ПОДПИСАН	
ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Другие средства	
Действителен: с 20.08.2021 по 20.08.2022	

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.: НПЦ «Аналитика», 2017.

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>.

2. Чипига, А.А. Информационная безопасность автоматизированных систем: учеб. пособие /

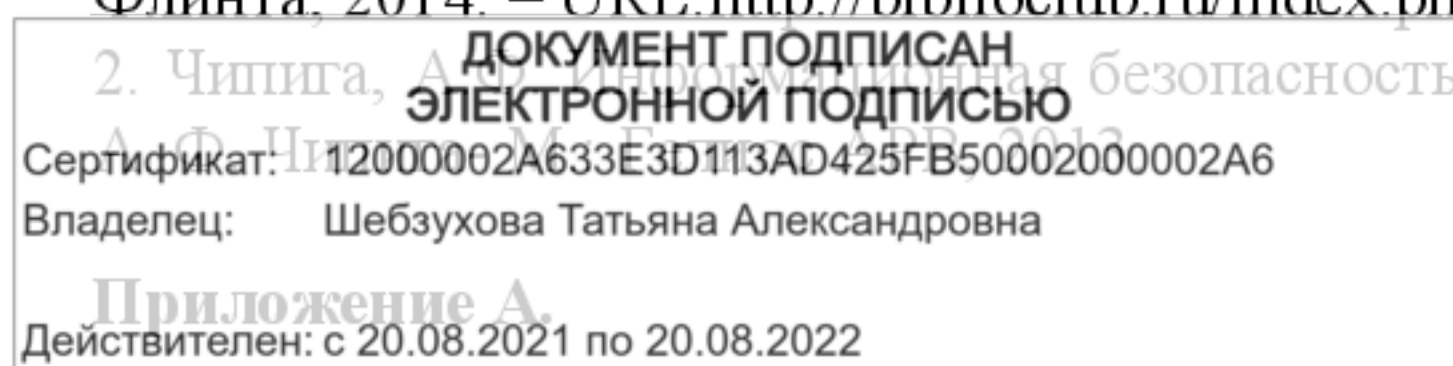


Таблица П.1. Пространственная модель защищаемого объекта

№ 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.
ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ Сертификат: 12000002A633E3D113AD425FB50002000002A6 Владелец: Шебзухова Татьяна Александровна Действителен: с 20.08.2021 по 20.08.2022		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 2 (r1') - минимальный радиус зоны вокруг ОТСС, в пределах которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах** превышает

допустимое (нормированное) значение.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

* - 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 зашумления. В итоге ориентировочно может быть определено общее число каждого типа излучателей, требуемое для зашумления 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

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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, воздуховодов 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.

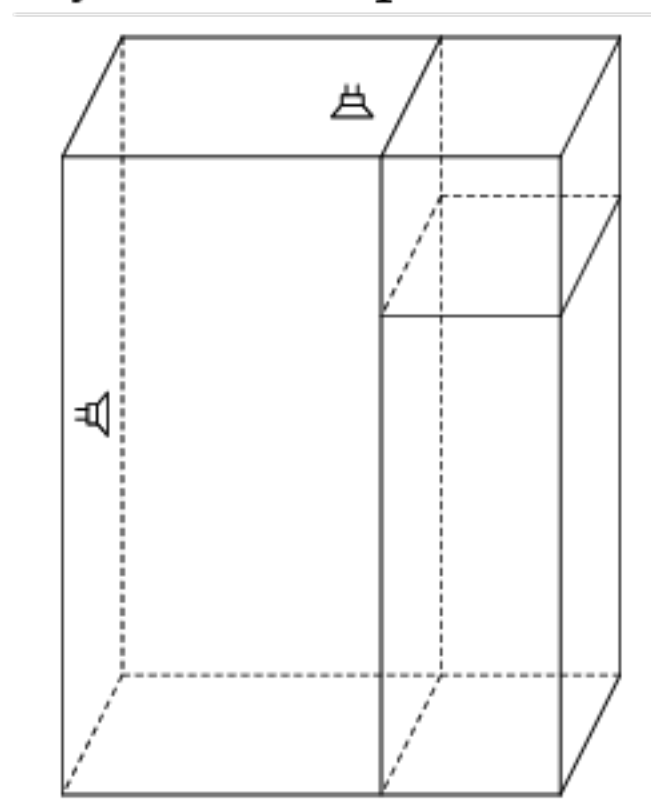
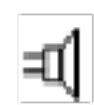


Рисунок 4 - Пример применения аудиоизлучателей для окна

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.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022



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.

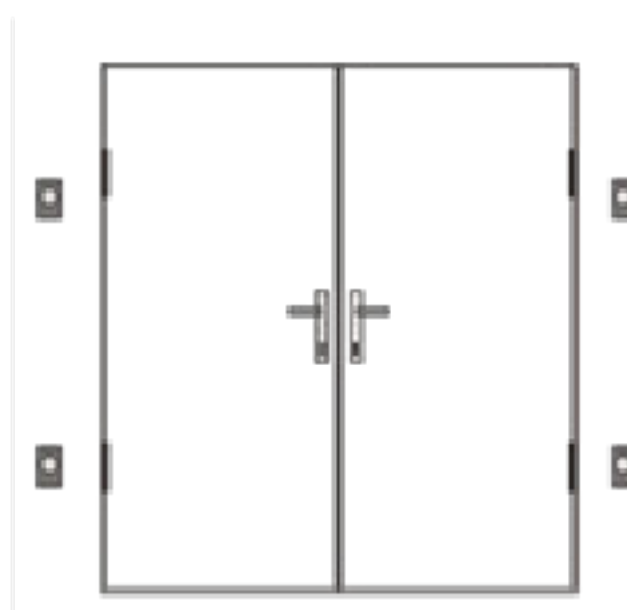


Рисунок 7 - Вариант размещения акустических излучателей для защиты дверного проёма с двумя створами.

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 вентиляции, что обеспечивает нормальный воздухообмен.

Такое размещение обеспечивает защищенность 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".



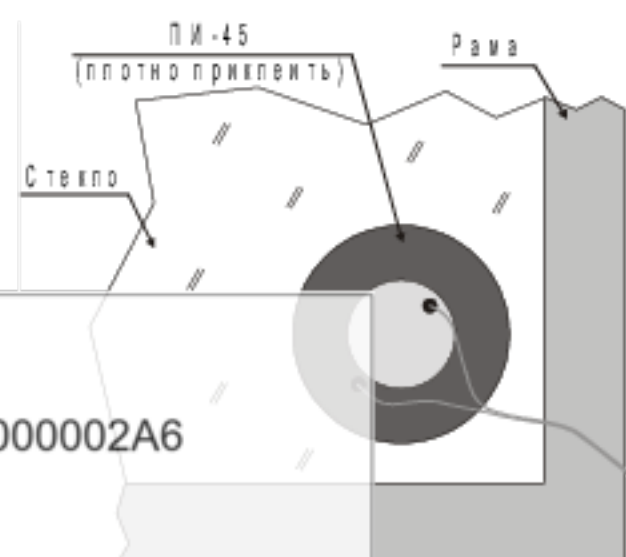
Рисунок 9 - Генераторы-акустоизлучатели "СА-4Б"

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.



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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.

б) 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. Кувыкин, 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. Схема обозначения на схеме		ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат: 12000002A633E3D113AD425FB50002000002A6		Полное наименование (комментарии)	ID
Владелец: Шебзухова Татьяна Александровна			
Действителен: с 20.08.2021 по 20.08.2022			

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:

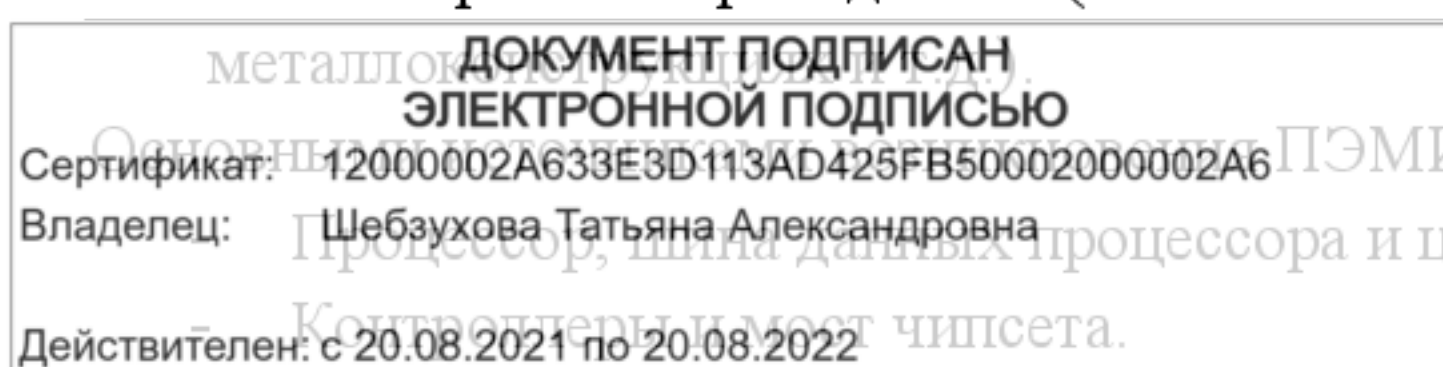
Естественные каналы утечки информации образуются за счёт побочных электромагнитных излучений, возникающих при обработке информации СВТ (электромагнитные каналы утечки информации), а также вследствие наводок информативных сигналов в линиях электропитания и заземления СВТ, соединительных линиях ВТСС и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



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.

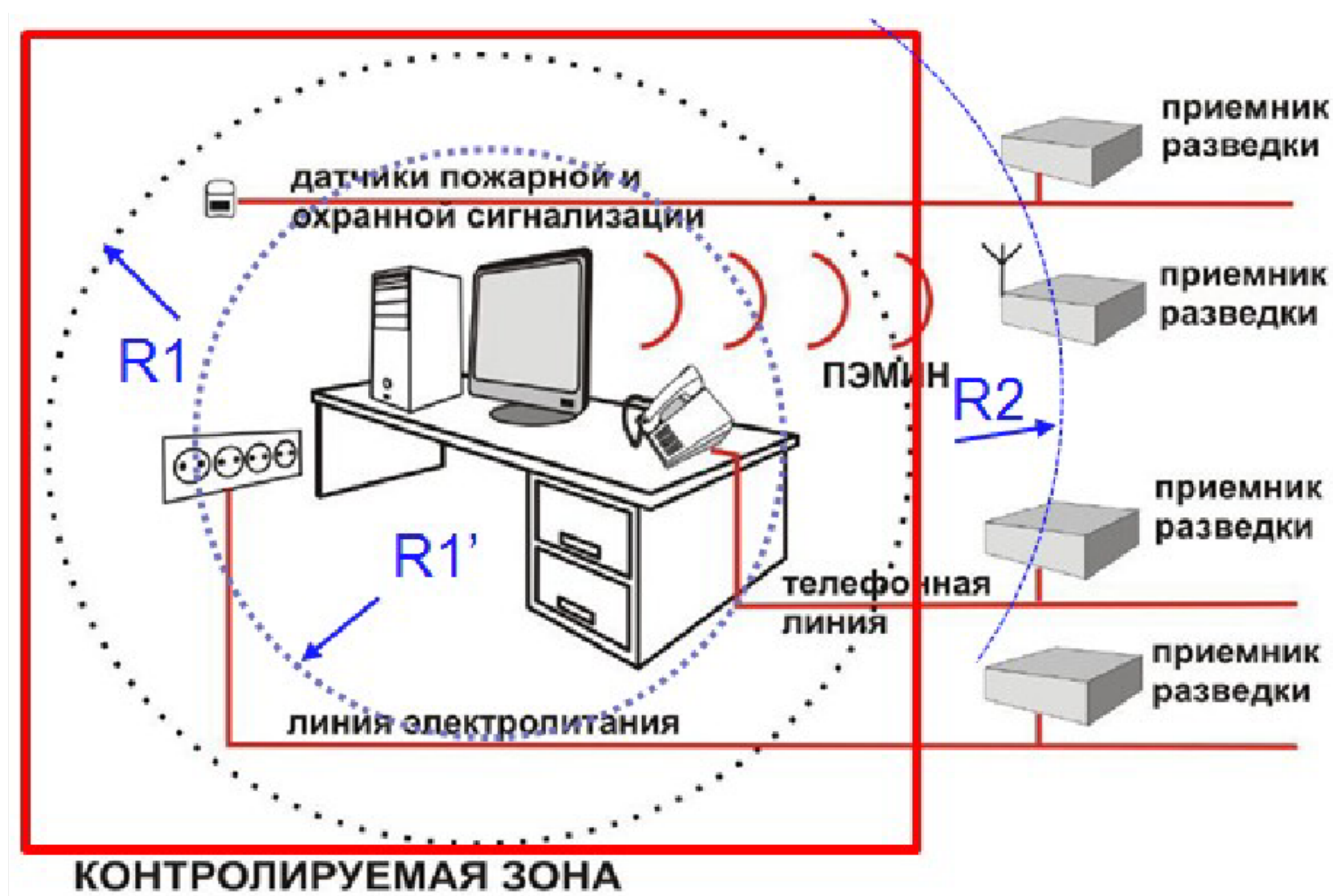


Рис 3.2 Радиусы опасных зон для перехвата информативных сигналов

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 (ПЭМИН) и тем самым к уменьшению отношения с/ш.

Опасный сигнал (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.

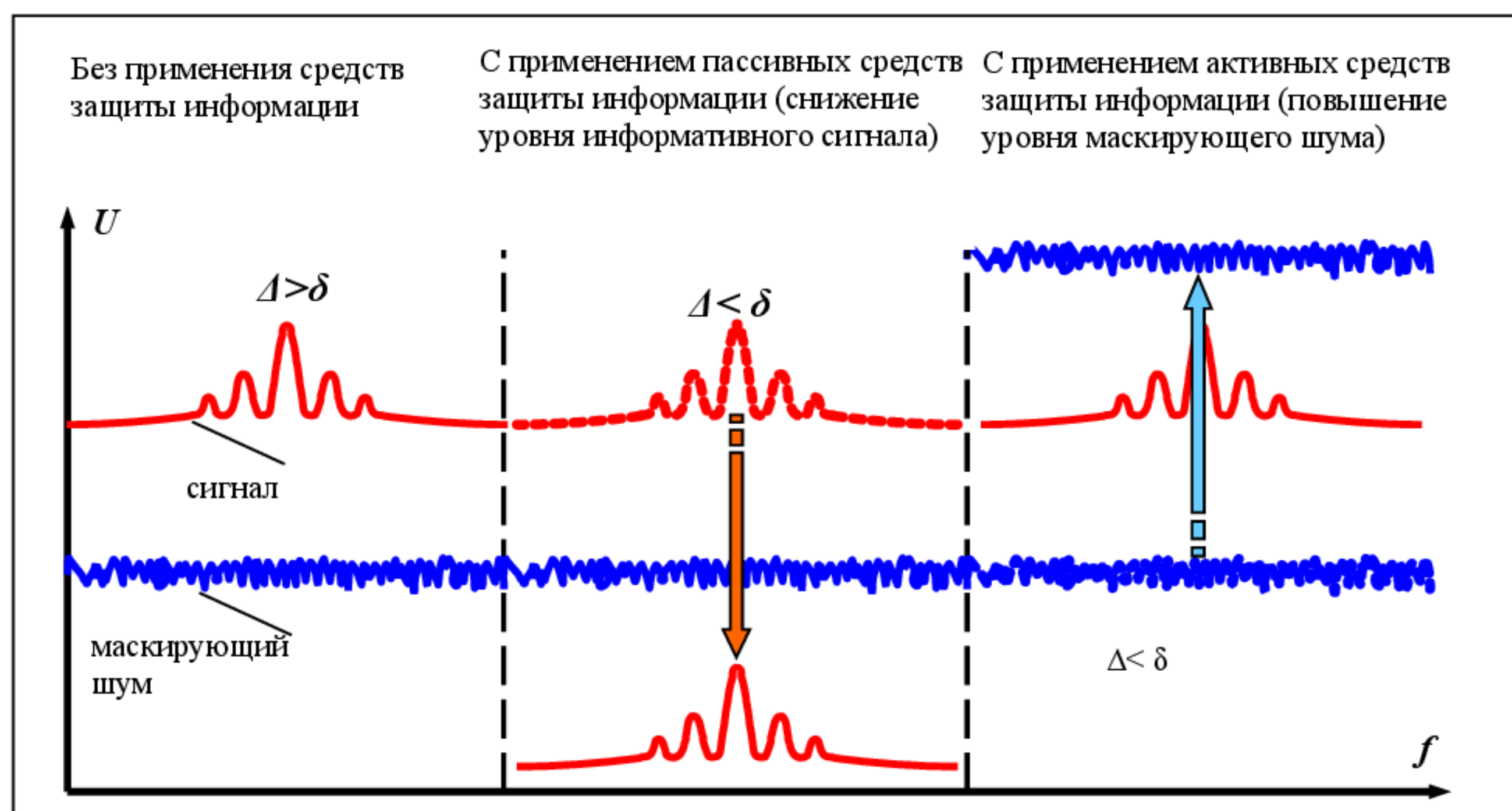


Рисунок 3.3 - Физические основы пассивных и активных методов защиты информации

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

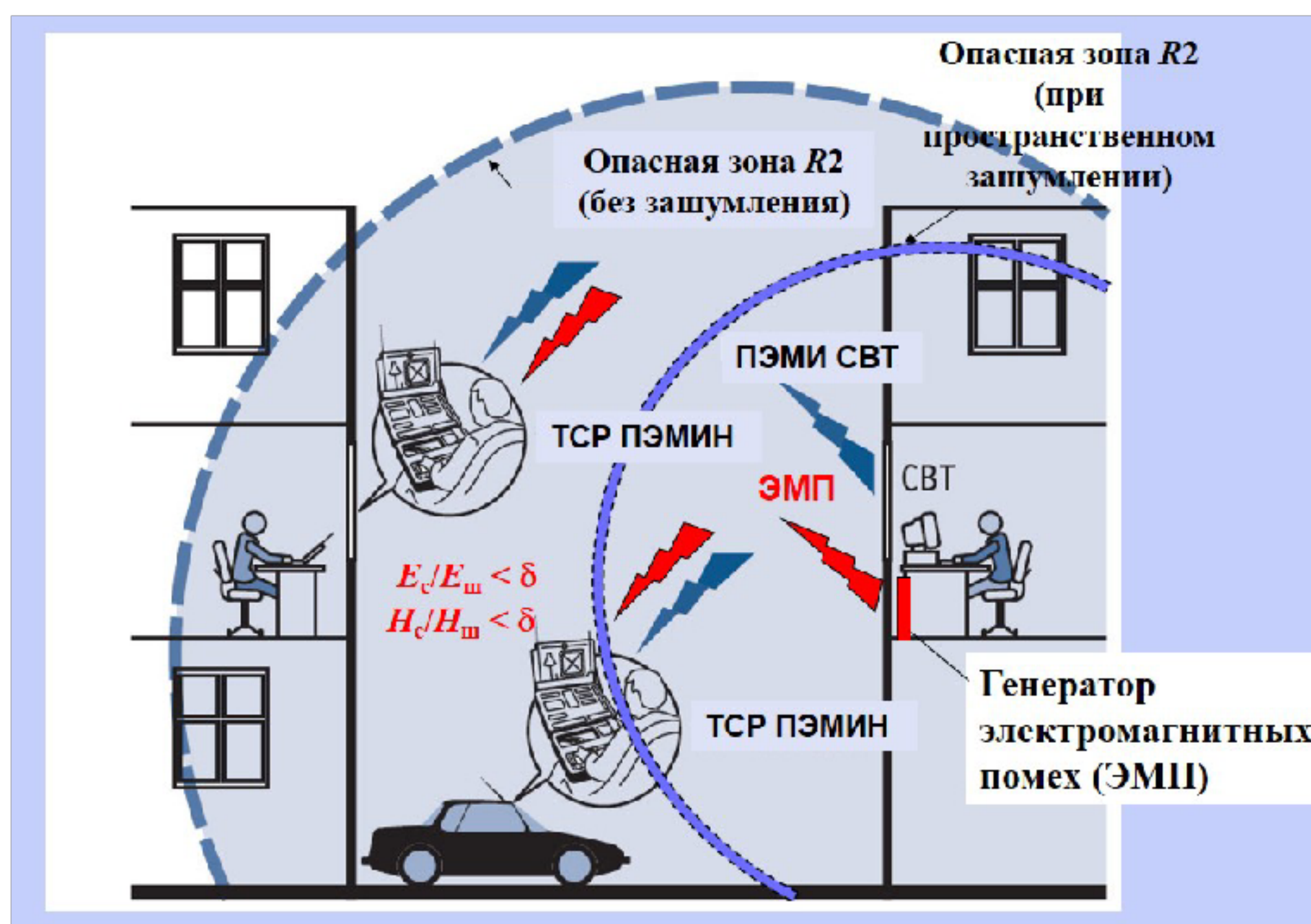


Рис 3.4– схема пространственного электромагнитного зашумления

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**.

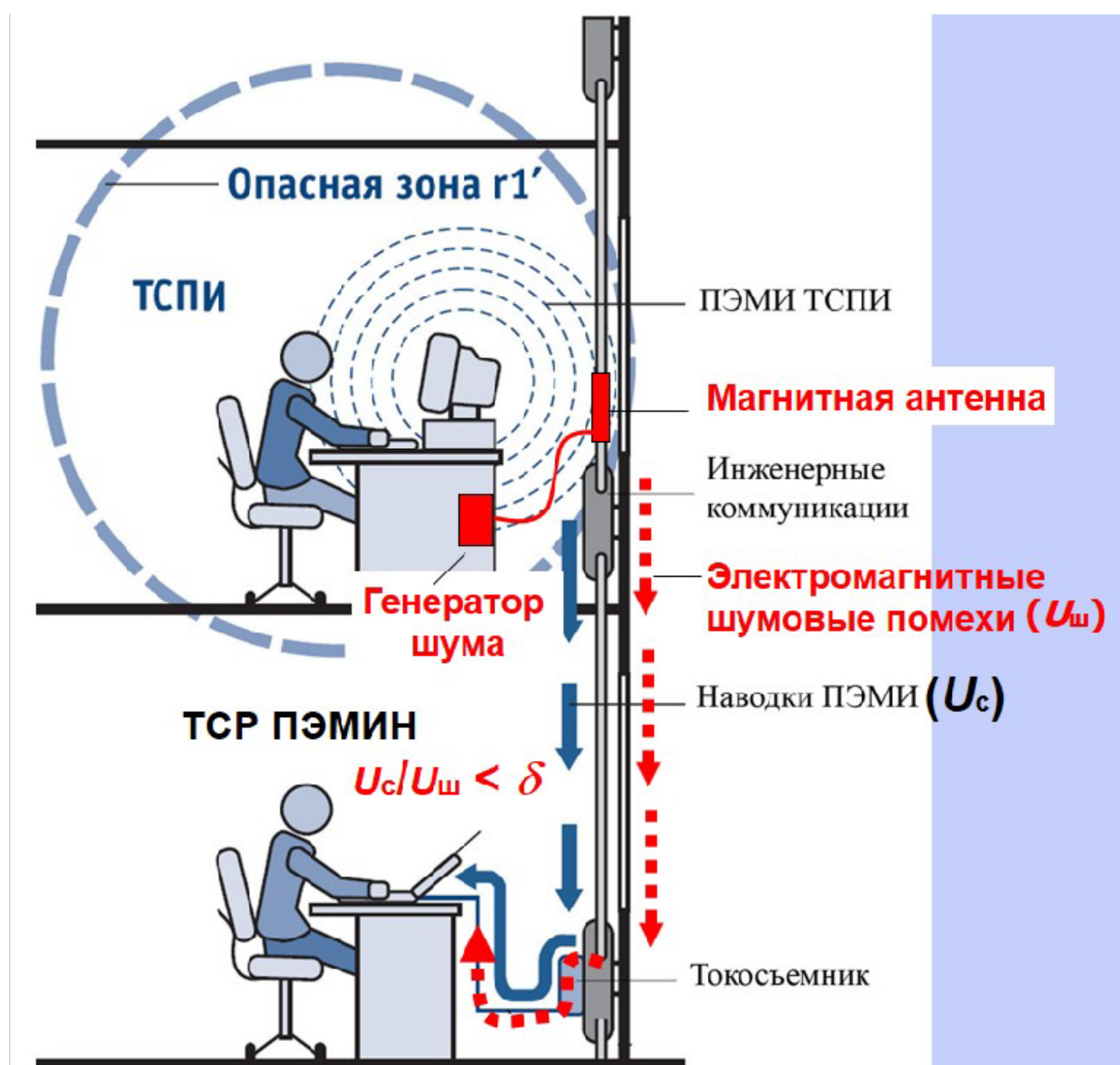


Рис 3.5 – Схема создания шумовых помех в системе отопления

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Рисунок 3.8 – Внешний вид устройства "Соната-Р3.1"



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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.



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6
 Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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.

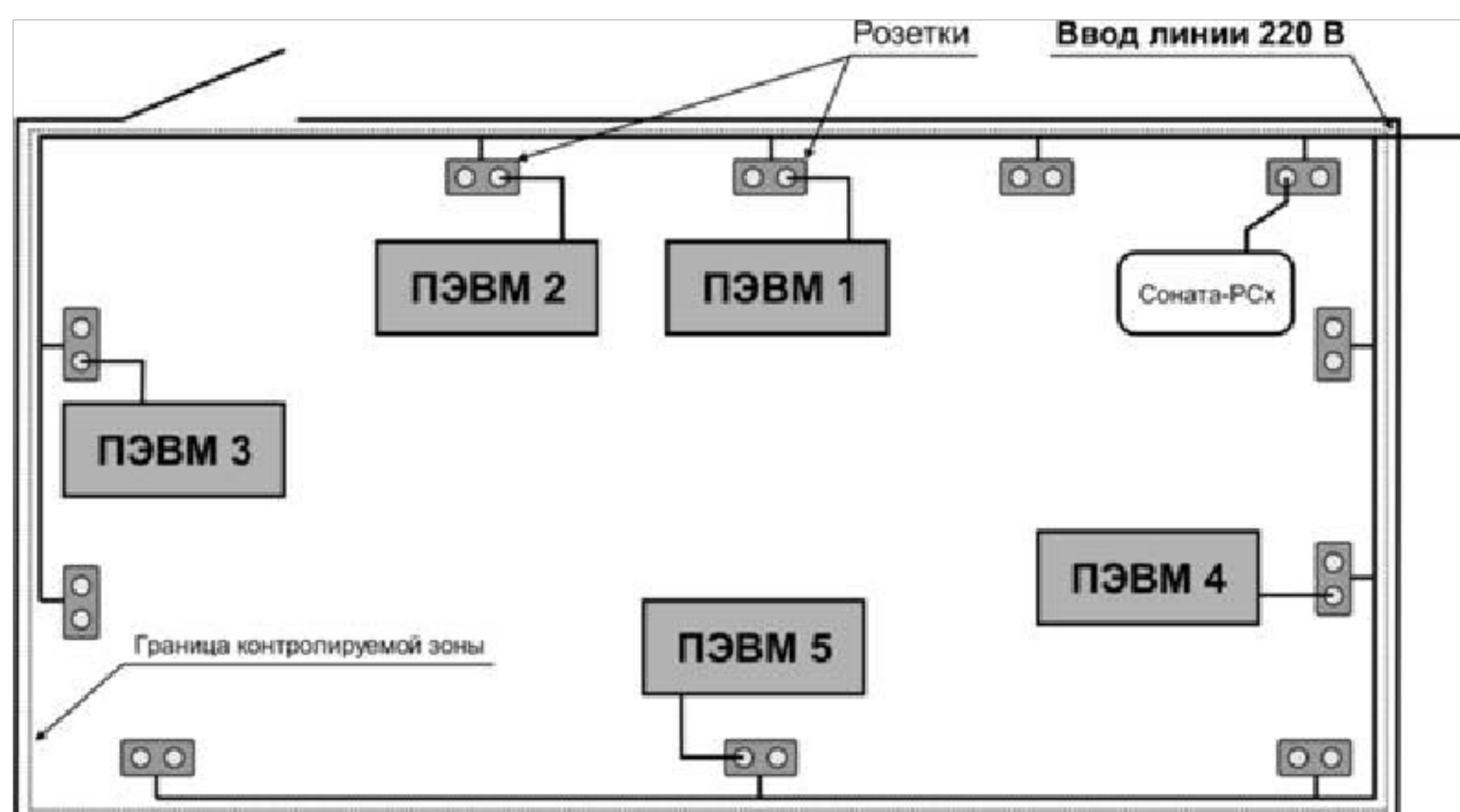


Рисунок 3.11 - Вариант установки устройства «Соната-РС3» на объекте ВП с одним вводом линии 220В

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

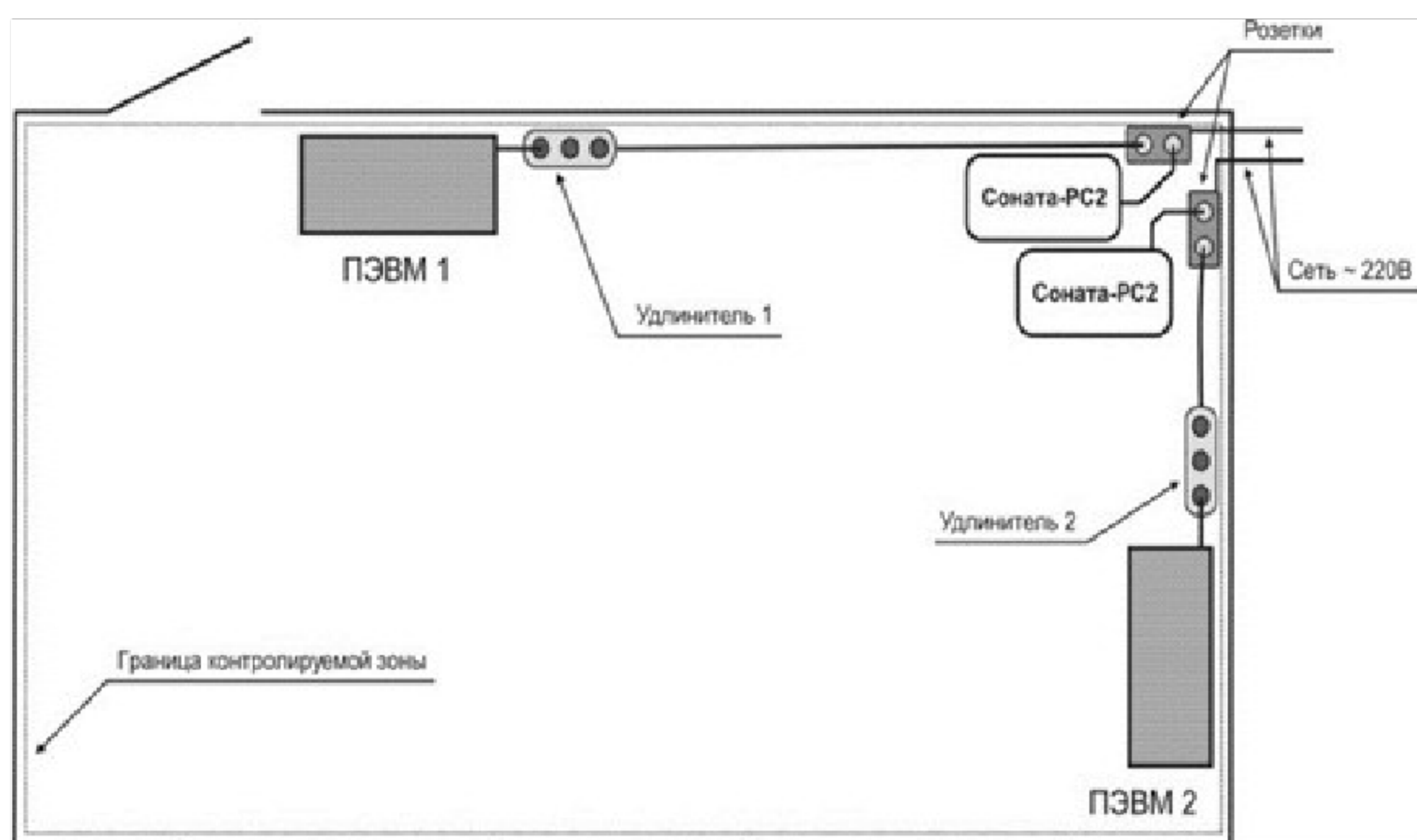


Рисунок 3.12 - Вариант установки устройств «Соната-РС3» на объекте ВП с двумя вводами линий 220В

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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

Практическое занятие № 4.

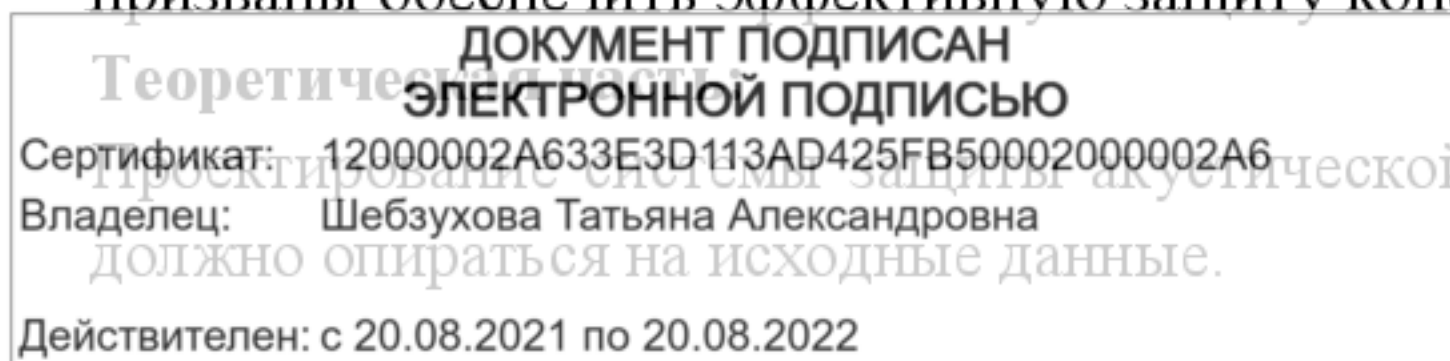
Тема: Разработка системы защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований.

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.





2

(ECC)

```
INCLUDE PICTURE #1" //          /D : H1 1/X          / 1/140: ")*
```



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.: НПП «Аналитика», 2017.

Перечень дополнительной литературы:
Сертификат 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Фланта, 2014. – URL: http://biblioclub.ru/index.php
Действителен: с 20.08.2021 по 20.08.2022

Техническая защита информации: учебное пособие [Элек-тронный
выклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.:
p?page=book&id=93349.

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

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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**

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

Пятигорск, 2022 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

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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.

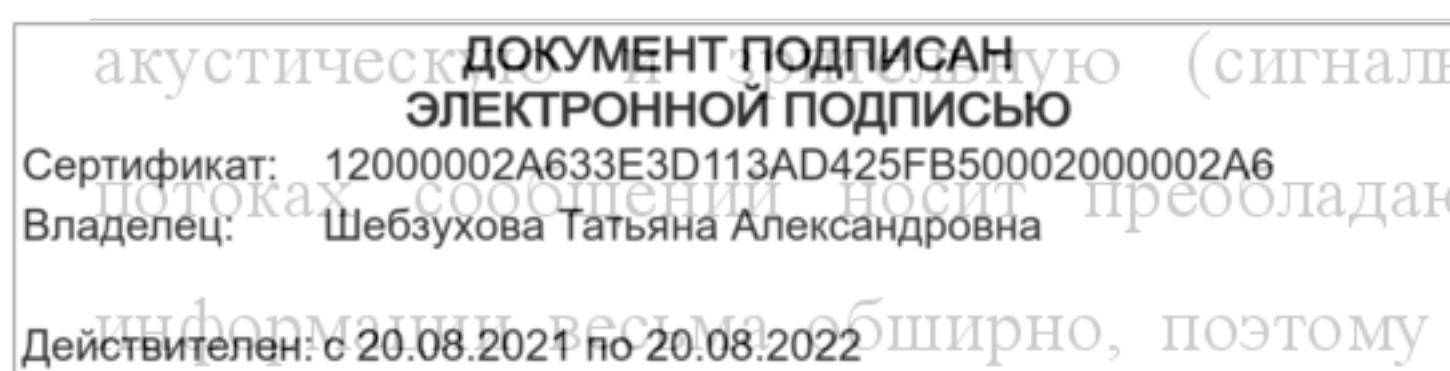
При возникновении различных угроз от них приходится защищаться. Для того чтобы оценить вероятные угрозы, следует перечислить и основные категории источников конфиденциальной информации – это могут быть люди, документы, публикации, технические носители, технические средства обеспечения производственной 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 (сигнальную) и зрительную. Акустическая информация в потоках сообщений носит преобладающий характер. Понятие зрительной информации весьма обширно, поэтому ее следует подразделять на объемно-



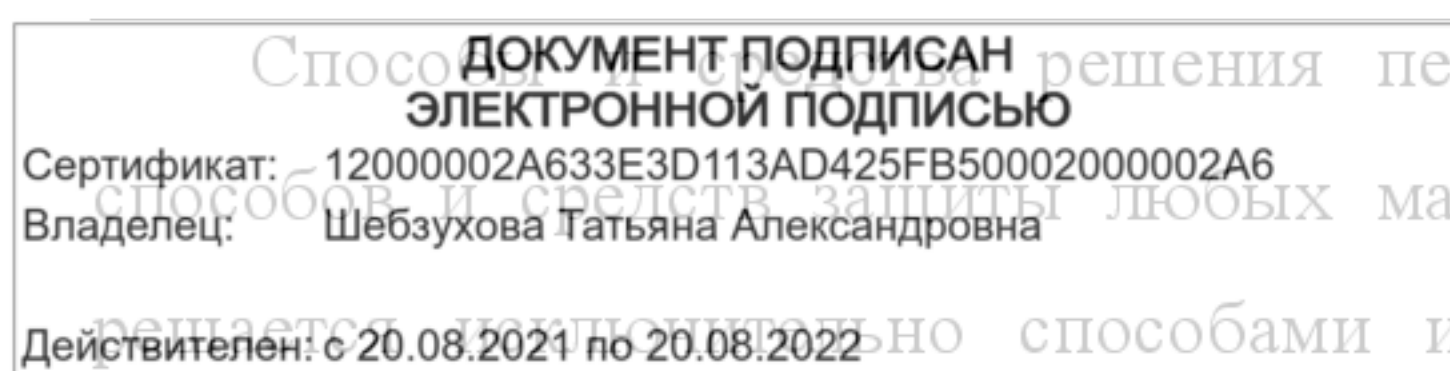
видовую и аналогово-цифровую.

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.



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

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

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

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

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»,

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

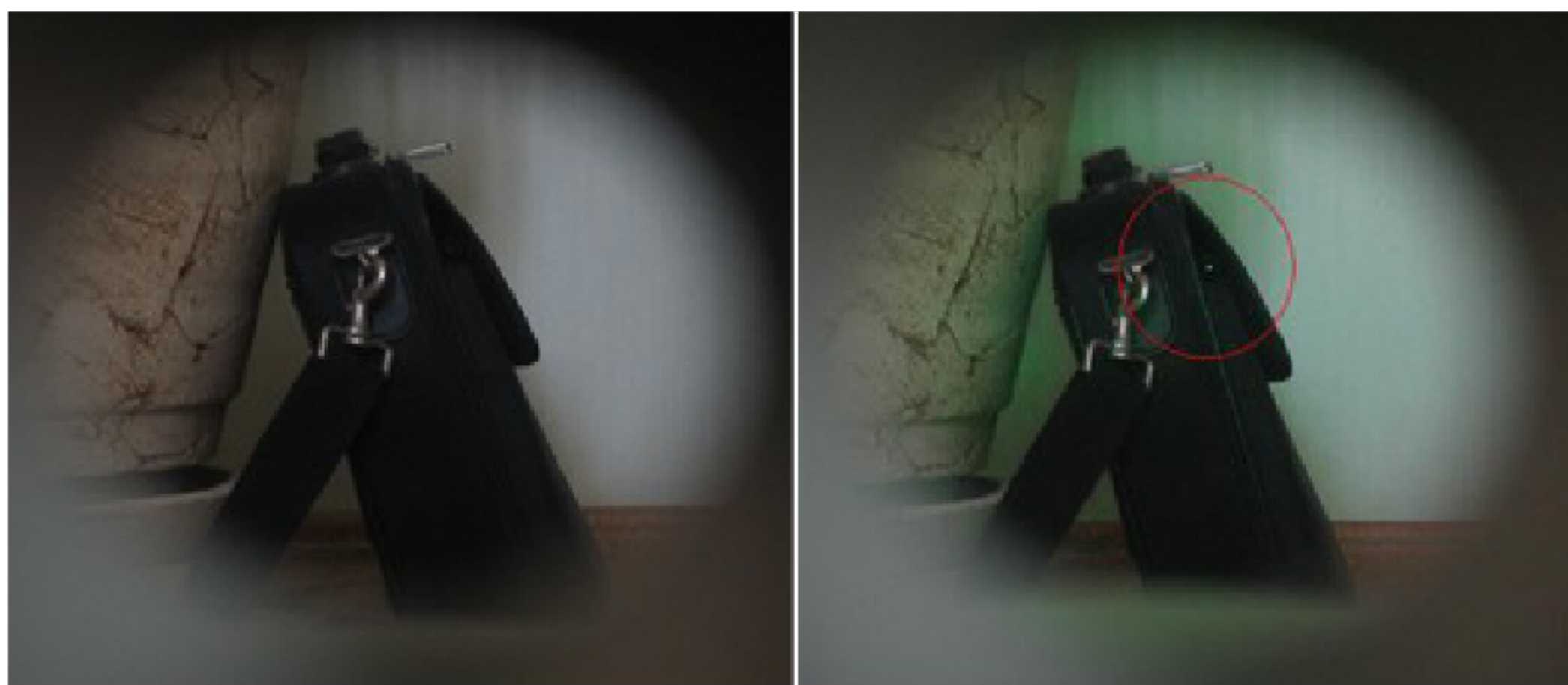


Рис. 2 - Пример выявления видеокамеры

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Щербухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

если интересно, посетил 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.

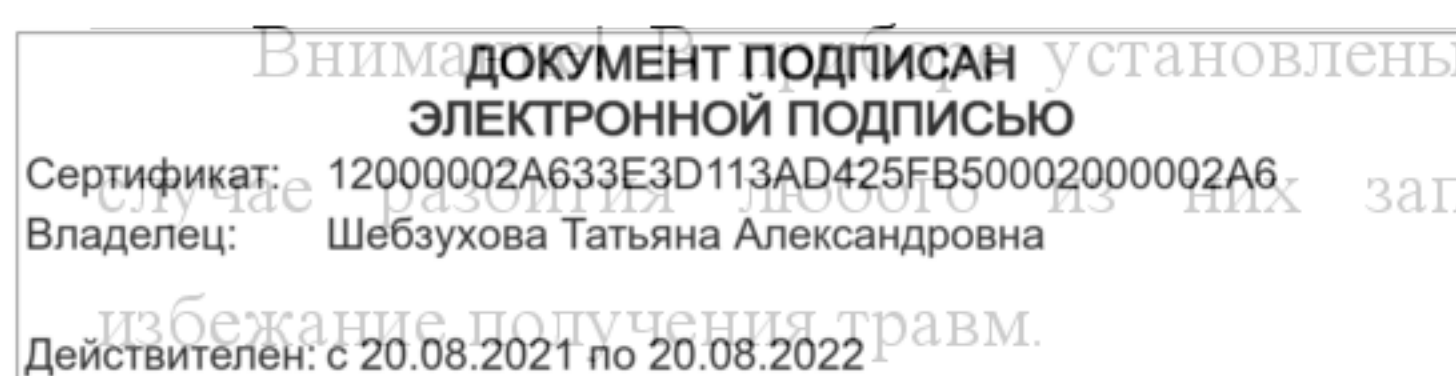
Необходимо при проверке помещений стараться не стоять под прямым углом к бликующей поверхности.

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



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.

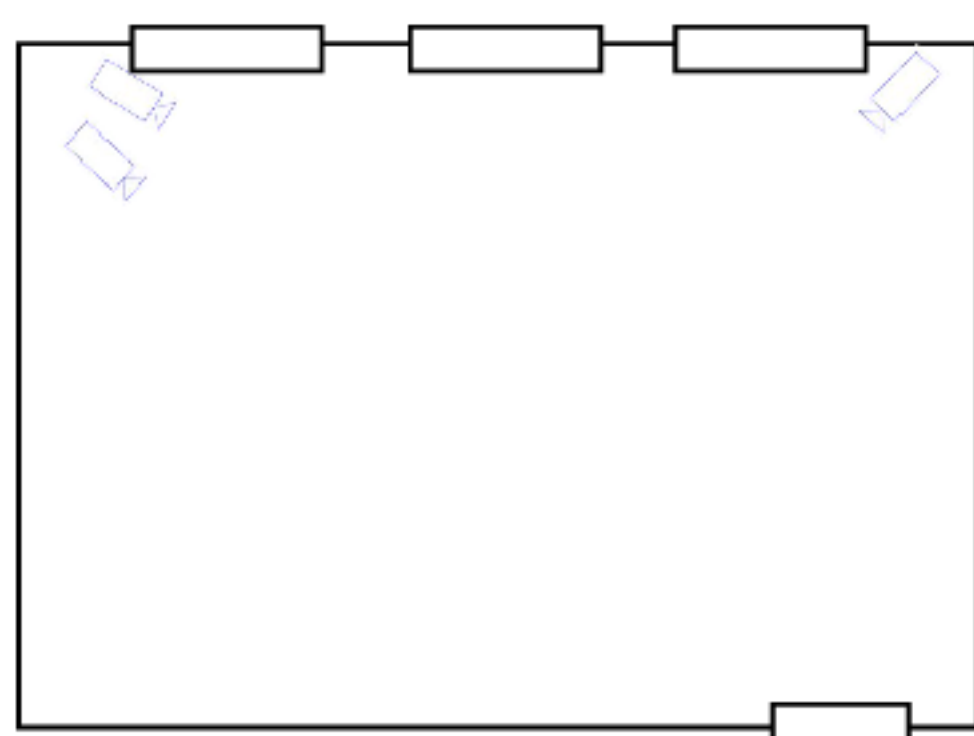
1) Произвести визуальный осмотр защищаемого помещения.

- 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

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

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

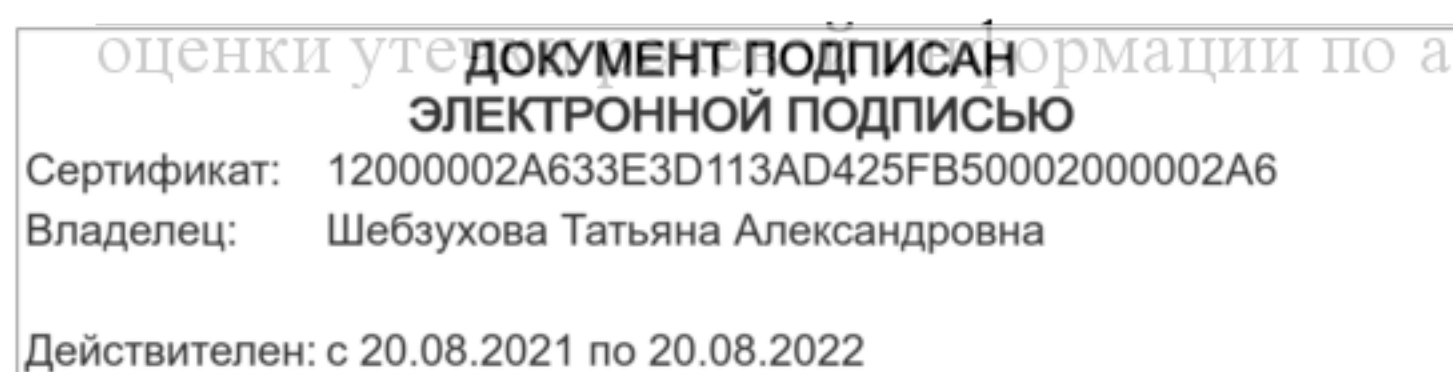
Тема: Качественная оценка утечки речевой информации по акустическому каналу с помощью многофункционального поискового прибора «Спайдер»

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.

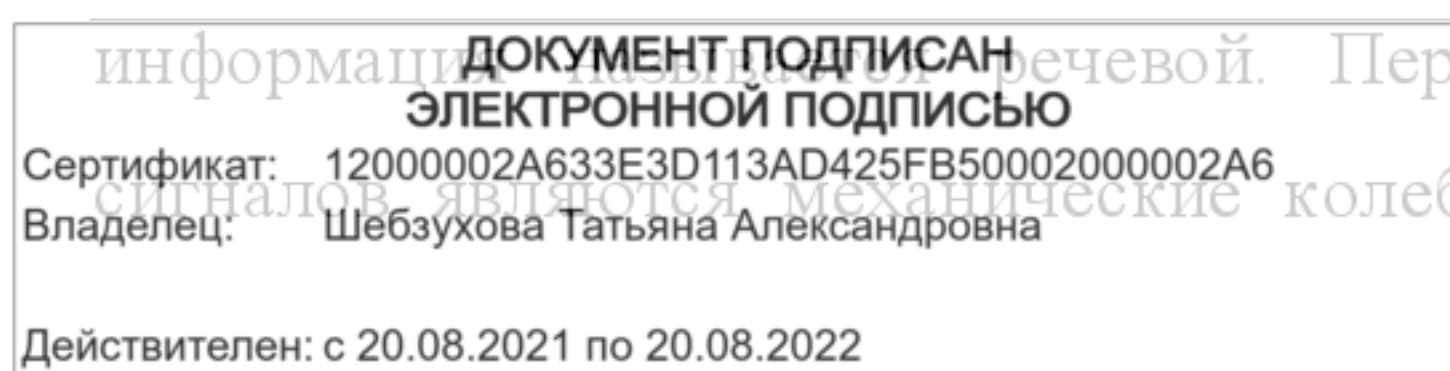
Для качественного решения задач аттестационных испытаний необходимо обладать теоретическими знаниями в разных областях науки – акустики и виброакустики, спектрального анализа, антенно-фидерных устройств, законов распространения электромагнитных колебаний, нормативно-правовых актов и руководящих документов 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 является 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).

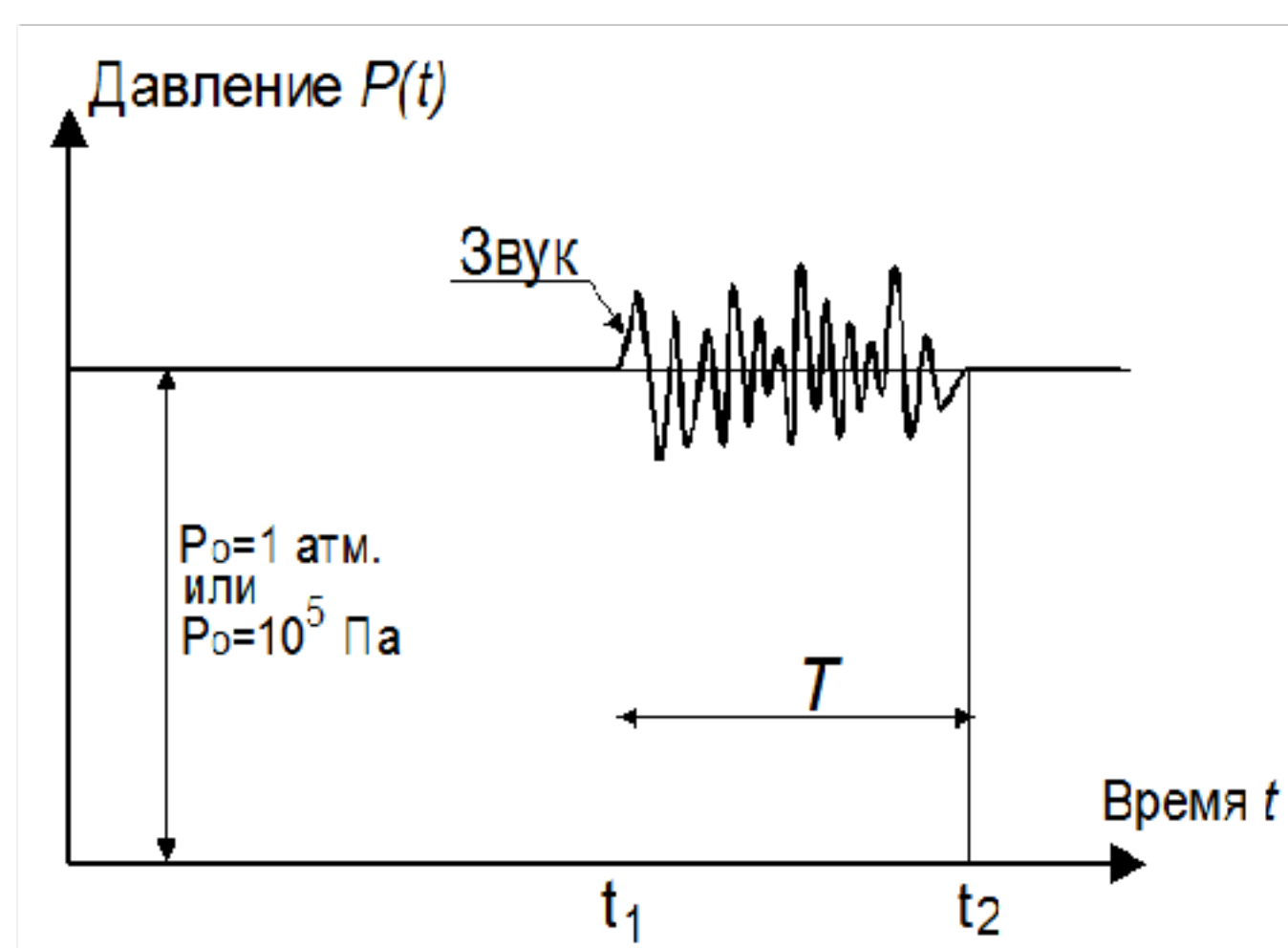


Рис. 2.1. Изменение давление в воздушной среде при возникновении звука

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

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 наделены специальными помещениями (ЗП).

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

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).

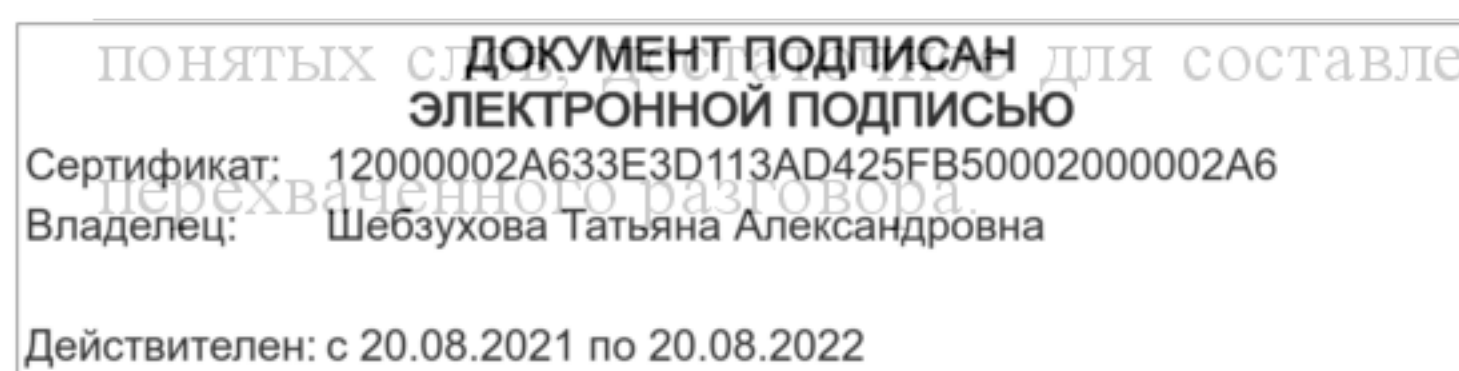
Таблица 2.1.

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



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 $H=1,5$ м. На каждые два погонных метра стены намечается одна контрольная точка, на дверь - одна контрольная точка, на каждую фрамугу окна - одна контрольная точка.

