

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шебзухова Татьяна Александровна
Должность: Директор Пятигорского института (филиал) Северо-Кавказского
федерального университета
Дата подписания: 19.07.2023 14:12:14
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: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

Пятигорск, 2023 г.



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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 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)	3	6	6		13,5
2	Интернет-технологии	ОПК-9,(ИД-1.ИД-2,ИД-3) ОПК-10,(ИД-1.ИД-2,ИД-3)	3	6	6		
3	Электронные почтовые сервисы	ОПК-9,(ИД-1.ИД-2,ИД-3) ОПК-10,(ИД-1.ИД-2,ИД-3)	3	6	6		
4	Информационная безопасность и её составляющие	ОПК-9,(ИД-1.ИД-2,ИД-3) ОПК-10,(ИД-1.ИД-2,ИД-3)	4,5	9	9		
	Итого за 5 семестр		13,5	27	27		13,5
	Итого		13,5	27	27		13,5

Сертификат: 043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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.

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец:
Действителен: с 19.08.2022 по 19.08.2023

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)

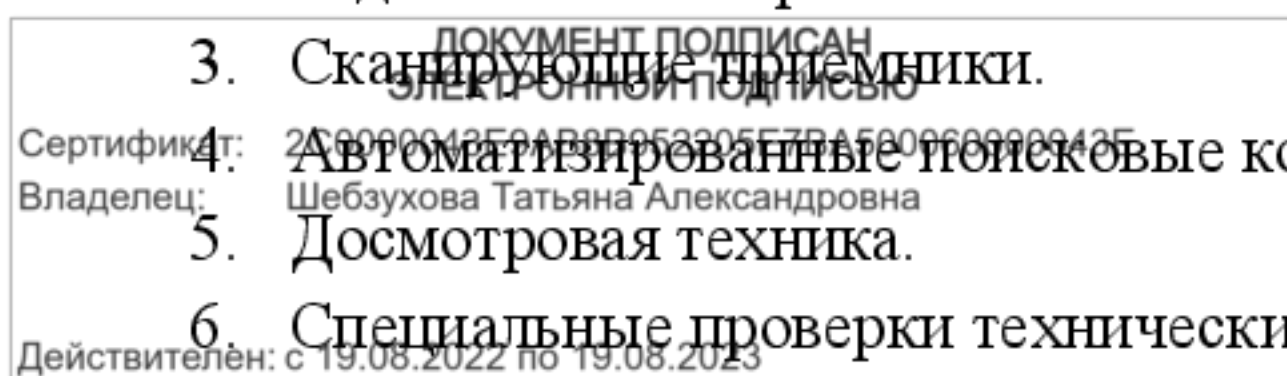
Вопросы для проверки уровня обученности:

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:

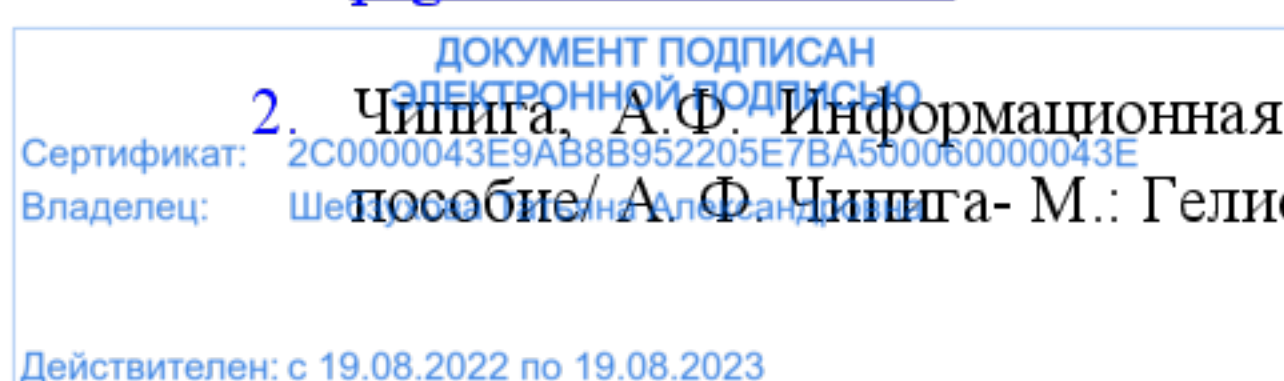
1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.

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. Чишига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А.Ф. Чишига- 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/>

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

Пятигорск, 2023 г.

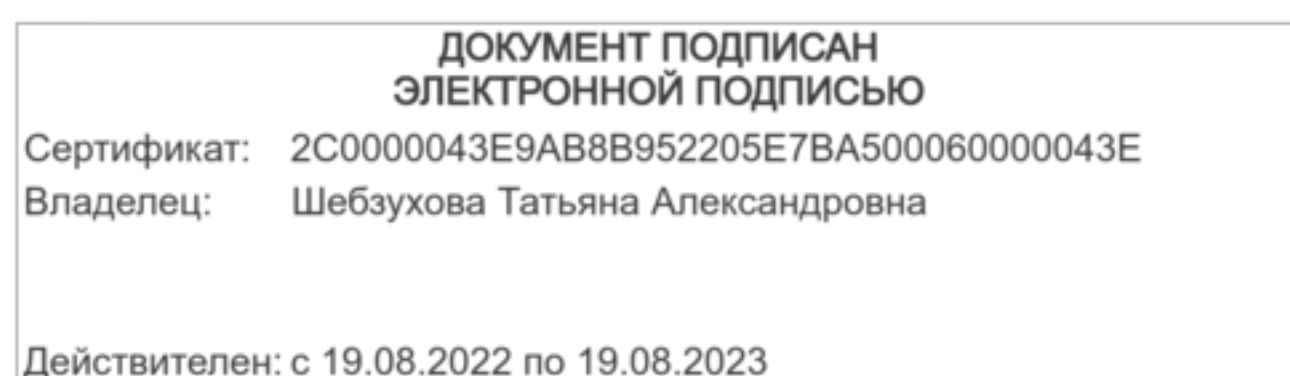
Введение

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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.

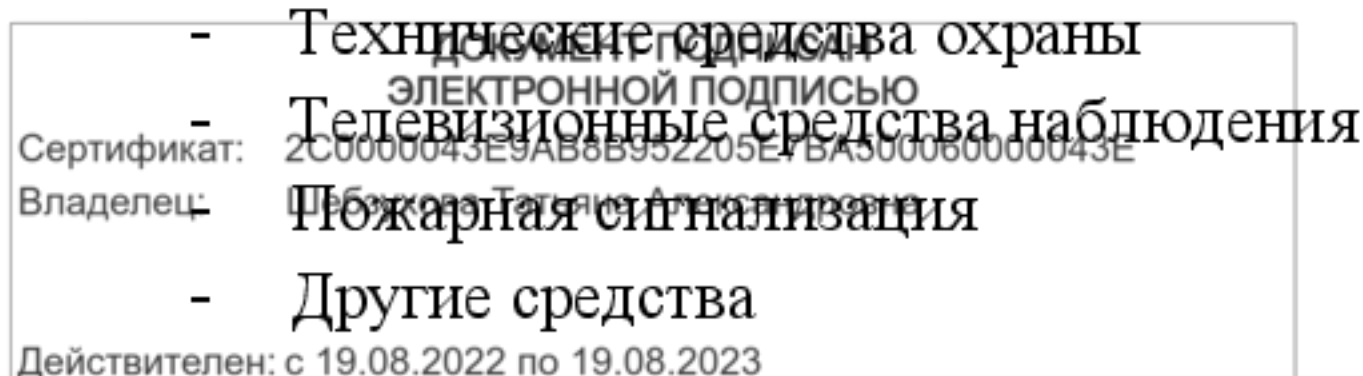
Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

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.: 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.

Сертификат: ЦС0000043ЕМВ88953205573А5000000013
Владелец: Шебзухова Татьяна Александровна

Приложение А.

Действителен: с 19.08.2022 по 19.08.2023

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен с 19.08.2022 по 19.08.2023

№ 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:

Электронная подпись
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: ЦББХОВА Татьяна Александровна
Действителен: с 19.06.2022 по 19.06.2023

* - 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



Рисунок 2 - Схема комплекса "3095"

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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.

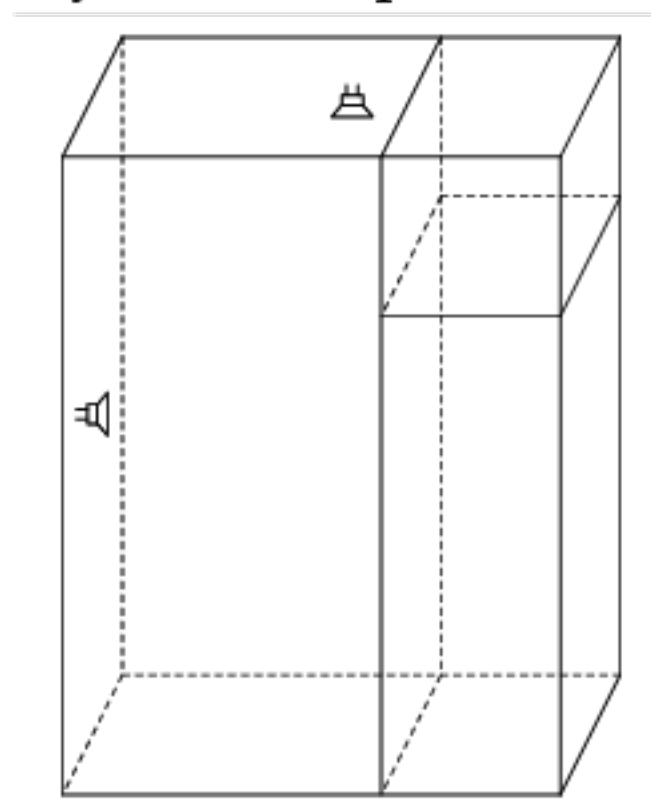
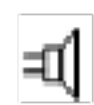


Рисунок 4 - Пример применения аудиоизлучателей для окна

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: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023



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.

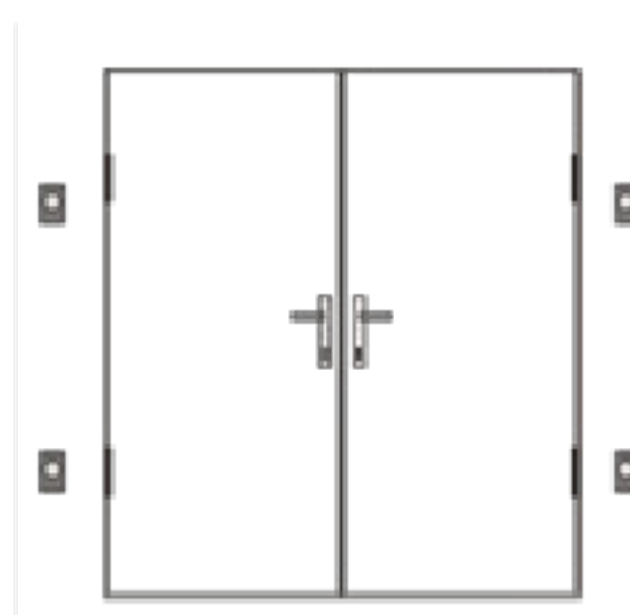


Рисунок 7 - Вариант размещения акустических излучателей для защиты дверного проёма с двумя створами.

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".



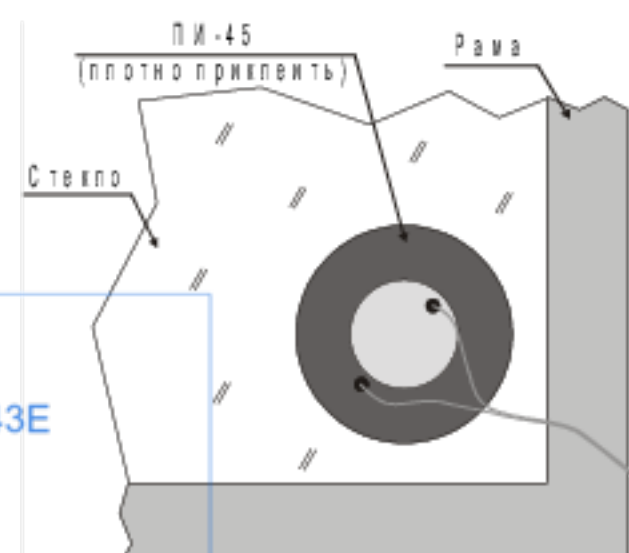
Рисунок 9 - Генераторы-акустоизлучатели "СА-4Б"

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.



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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. Состав комплекса

Сертификат: Владелец:	2C0000043E9AB8B952205E7BA500060000043E Шибзуева Татьяна Александровна	Обозначение на схеме Полное наименование (комментарии)	ID
--------------------------	--	--	----

Действителен: с 19.08.2022 по 19.08.2023

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, обрабатываемыми 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.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

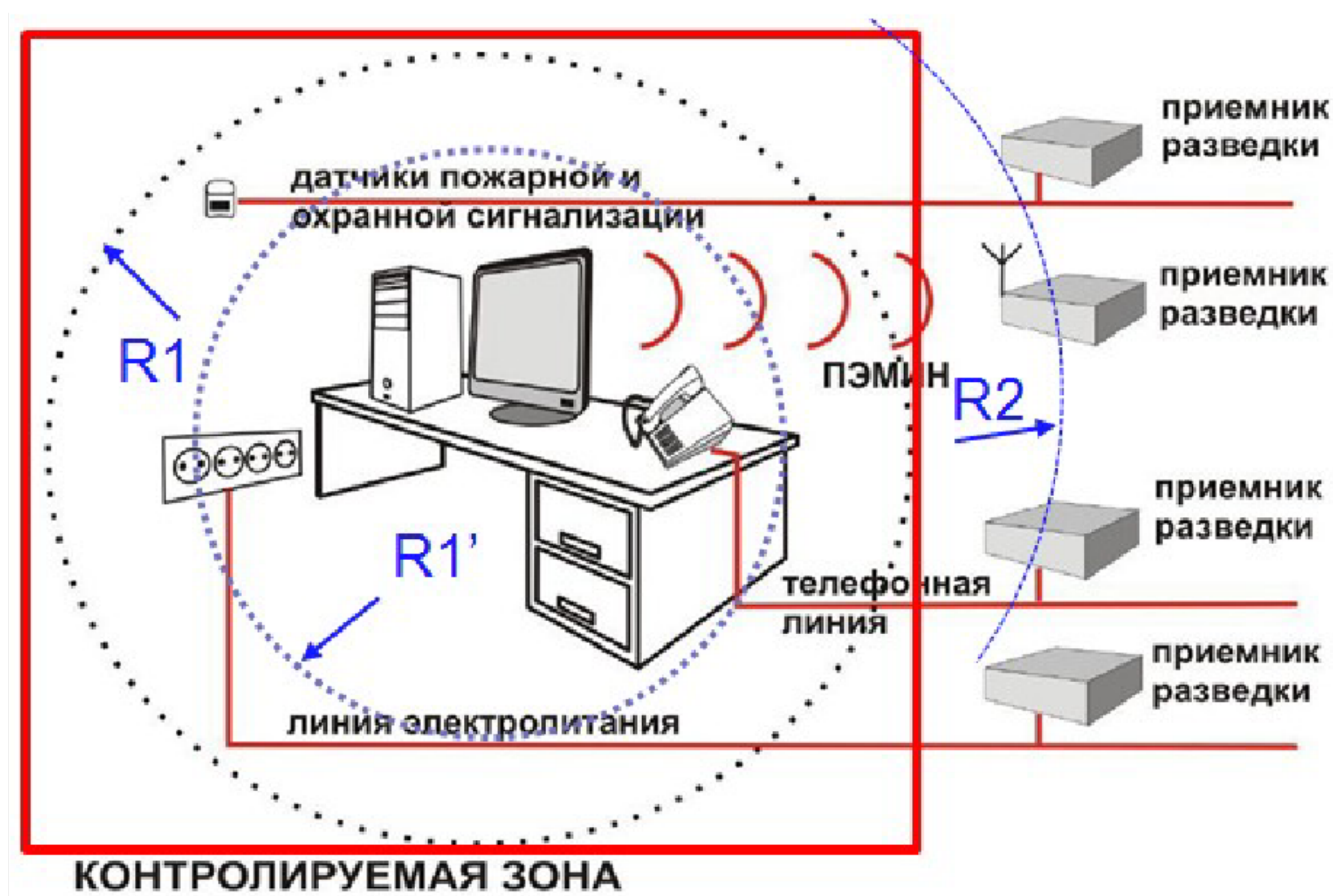


Рис 3.2 Радиусы опасных зон для перехвата информативных сигналов

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухов Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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

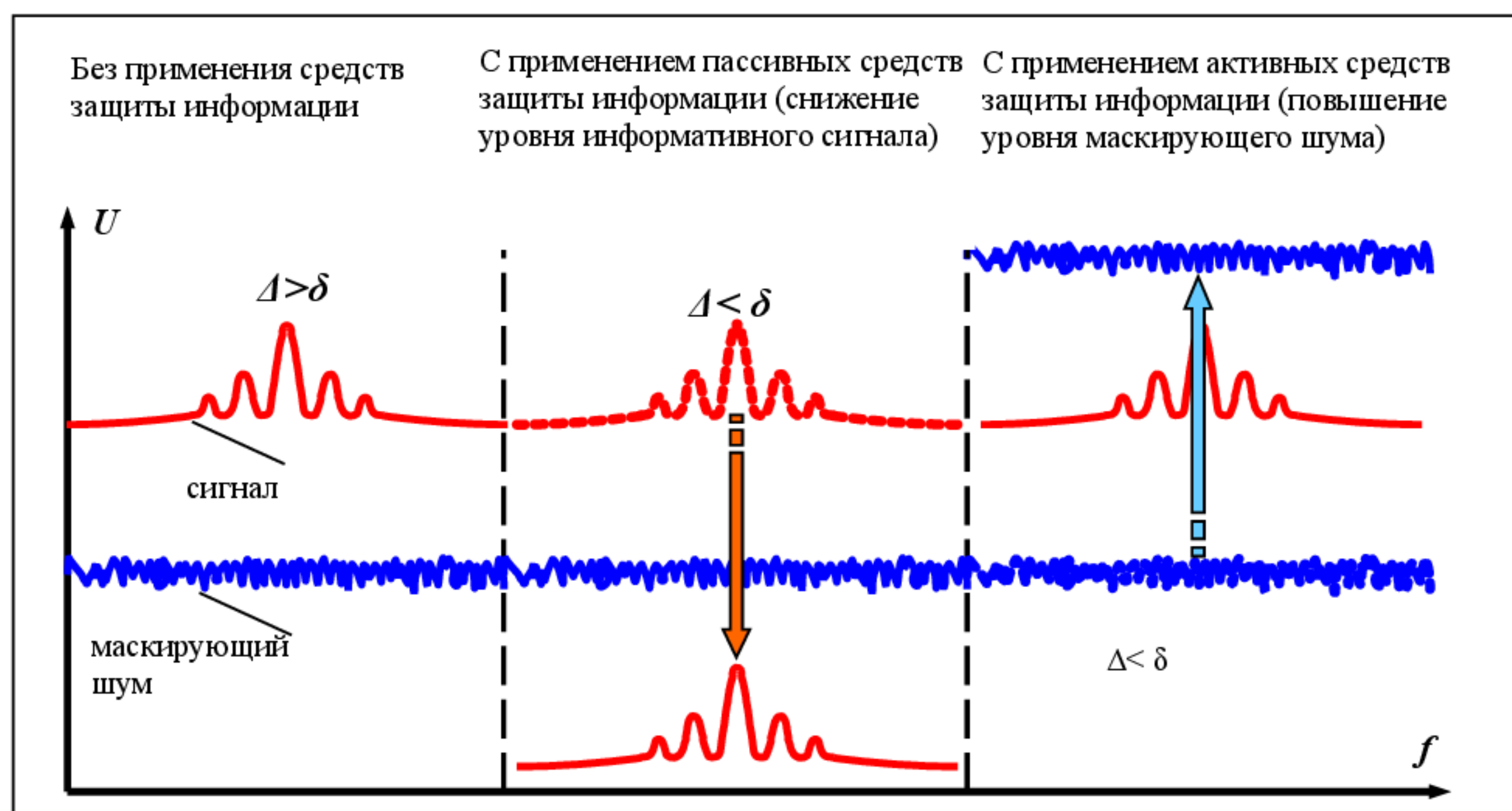


Рисунок 3.3 - Физические основы пассивных и активных методов защиты информации

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

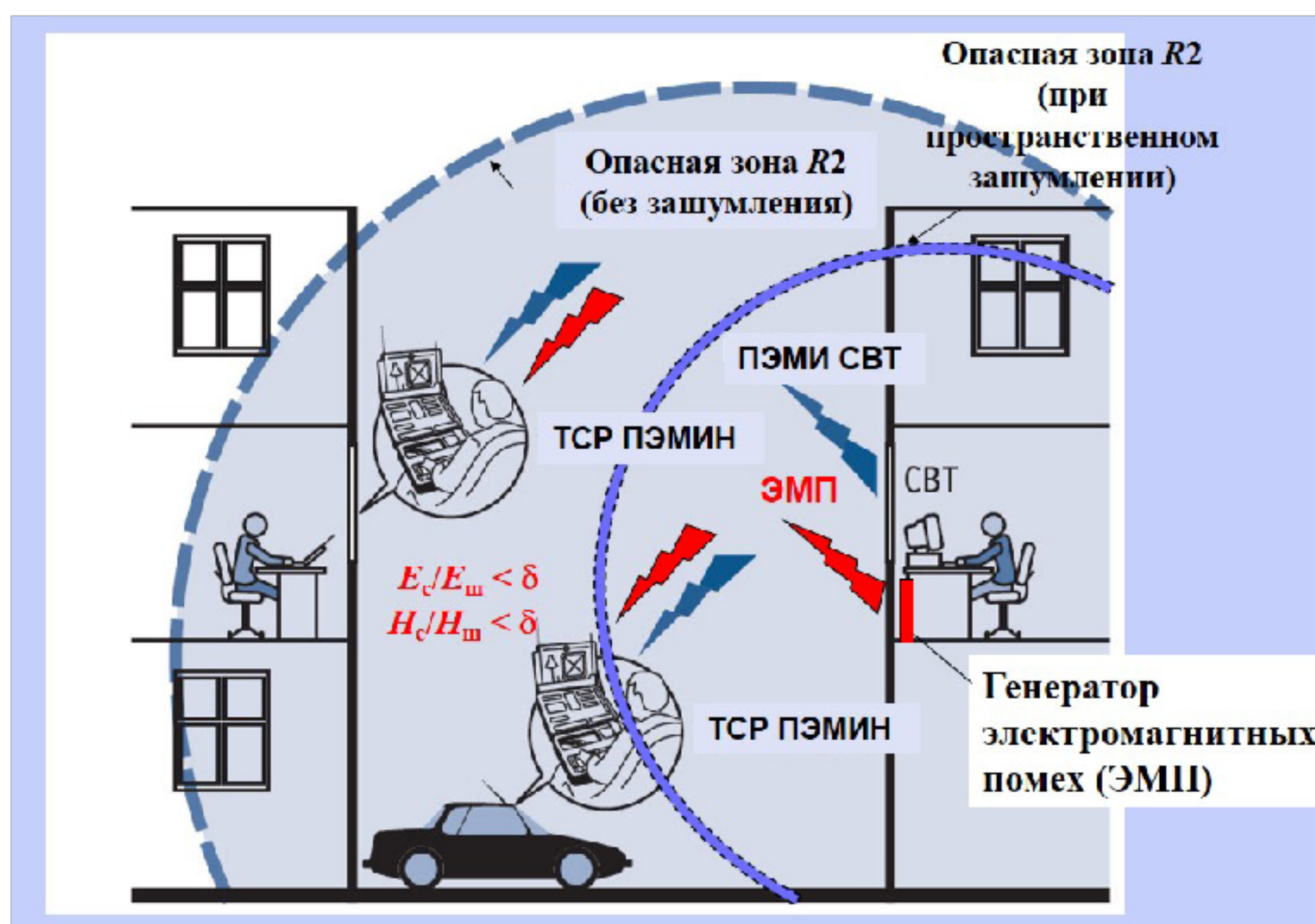


Рис 3.4– схема пространственного электромагнитного зашумления

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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**.

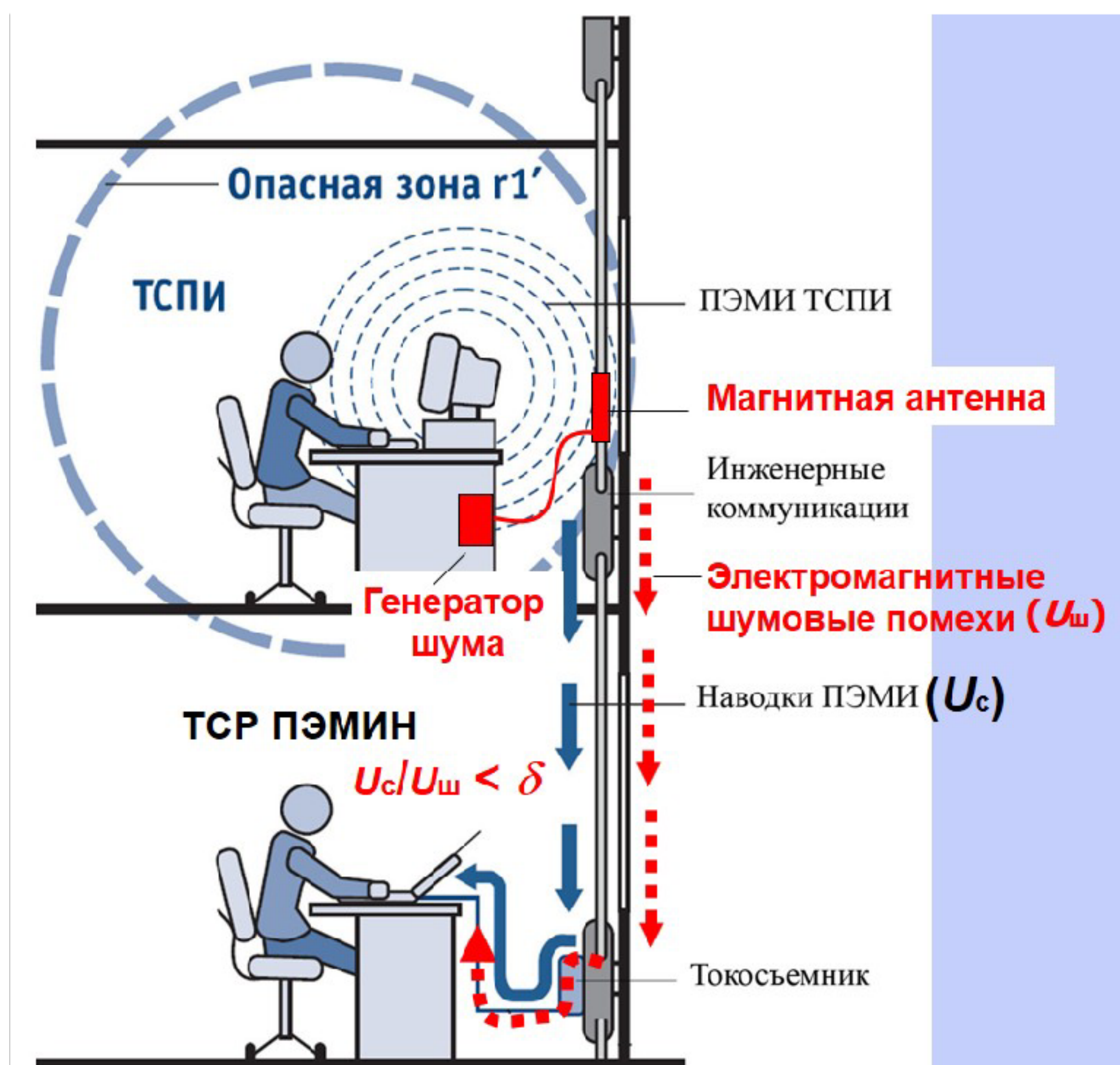


Рис 3.5 – Схема создания шумовых помех в системе отопления

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: 2600000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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).

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

	
Соната-Р3.1	Соната-Р3.1 с дополнительной антенной

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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.

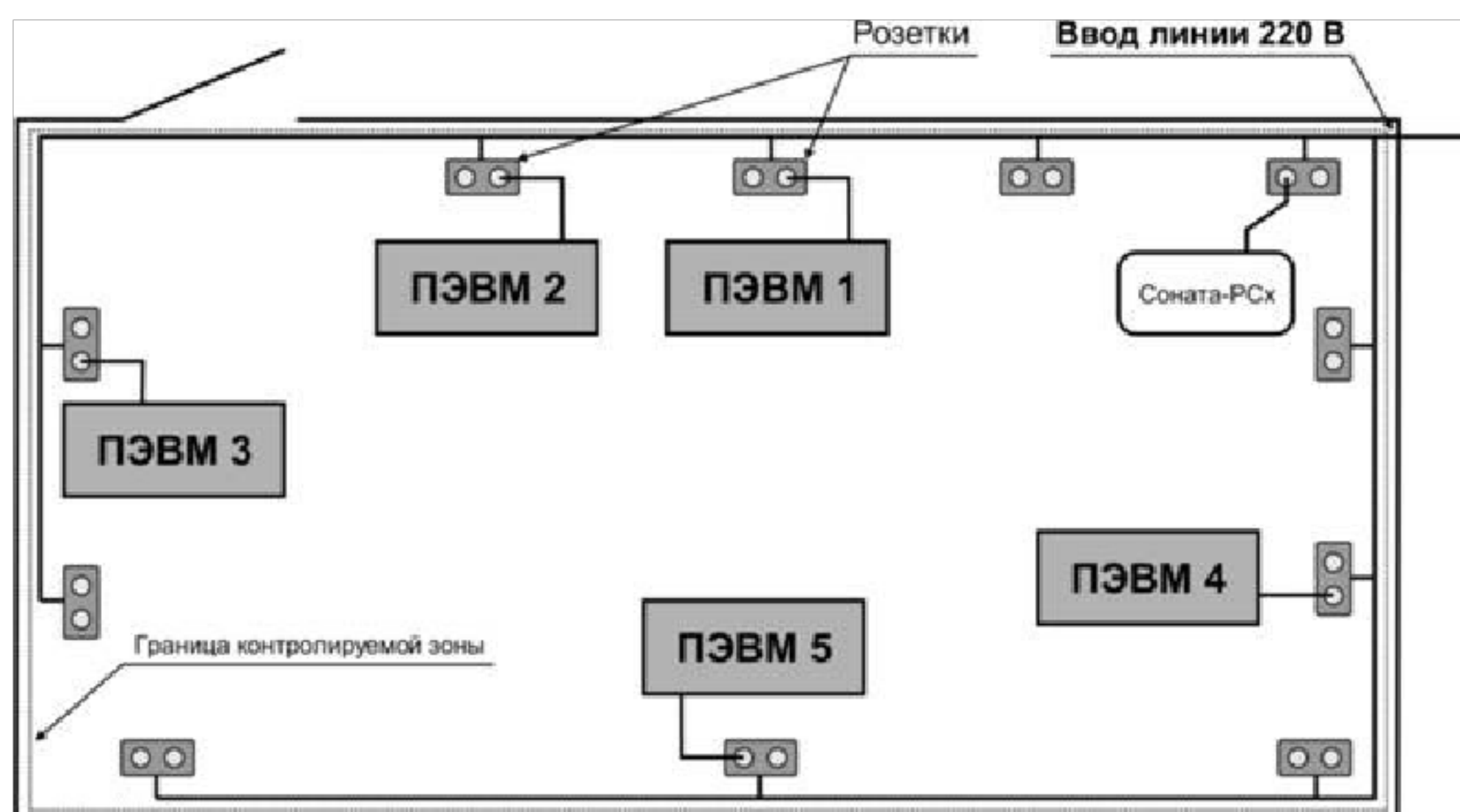


Рисунок 3.11 - Вариант установки устройства «Соната-РС3» на объекте ВП с одним вводом линии 220В

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

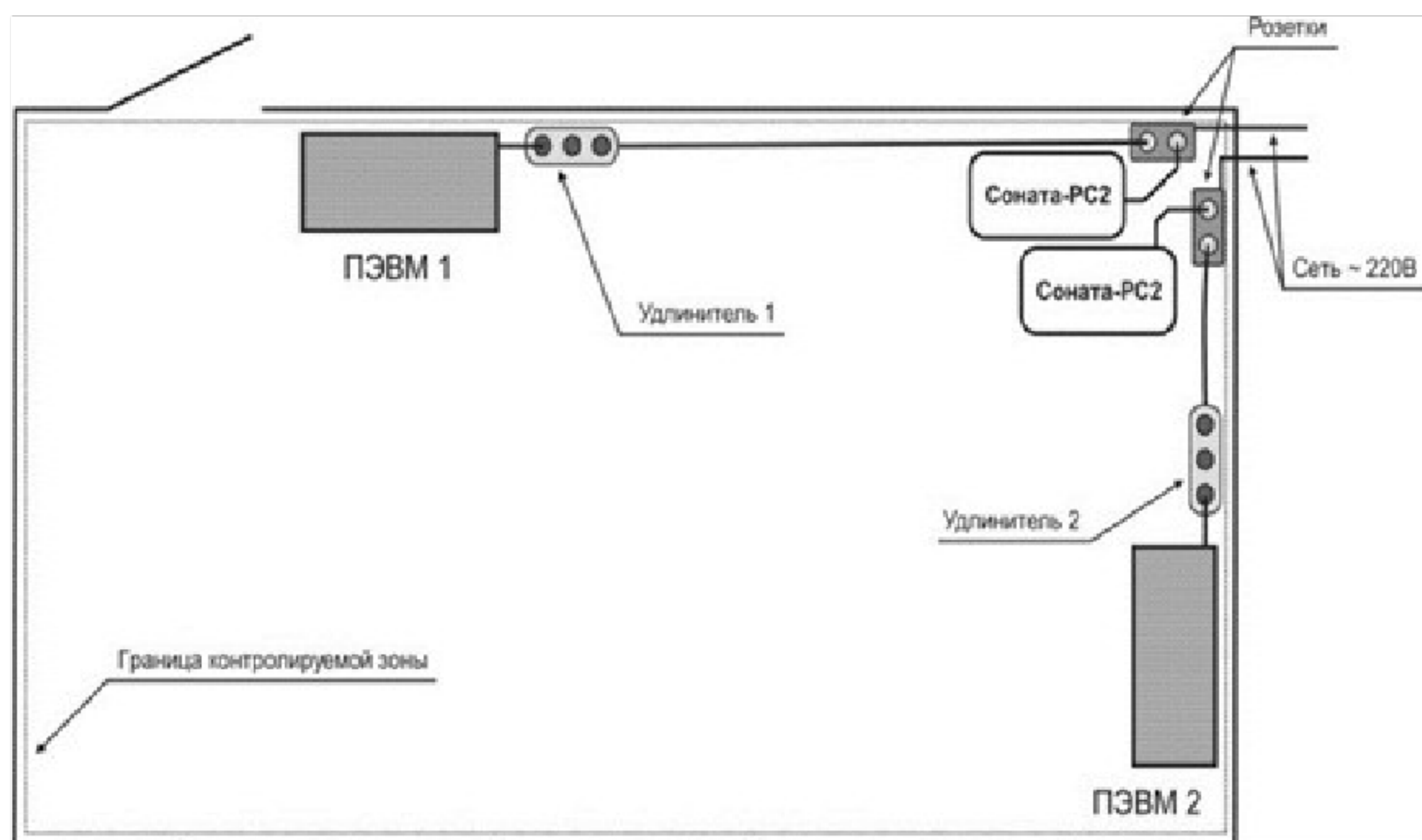


Рисунок 3.12 - Вариант установки устройств «Соната-РС3» на объекте ВП с двумя вводами линий 220В

документ подписан
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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. 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.

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.

