



Рисунок 16 – Внешний вид устройства Соната-BK4.2

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

Параметр	Соната-BK4.1	Соната-BK4.2	Соната-BK4.3
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-BK4.1", "Соната-BK4.2", "Соната-BK4.3" могут применяться с блоком питания и управления "Соната-ИП4.х" совместно с пультом управления и в составе комплексов ТСЗИ.

Вопросы:

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

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

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

Перечень дополнительной литературы:

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

ДОКУМЕНТ ПОДПИСАН
Сертификат: 202009043E2AB8B952305E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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

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 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: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

Пятигорск, 2023 г.

СОДЕРЖАНИЕ

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

Введение.

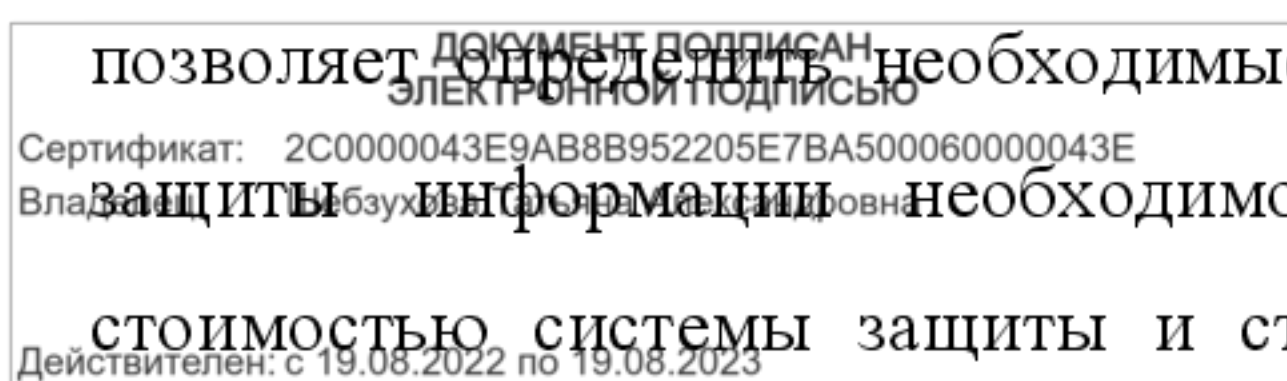
Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

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

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

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

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



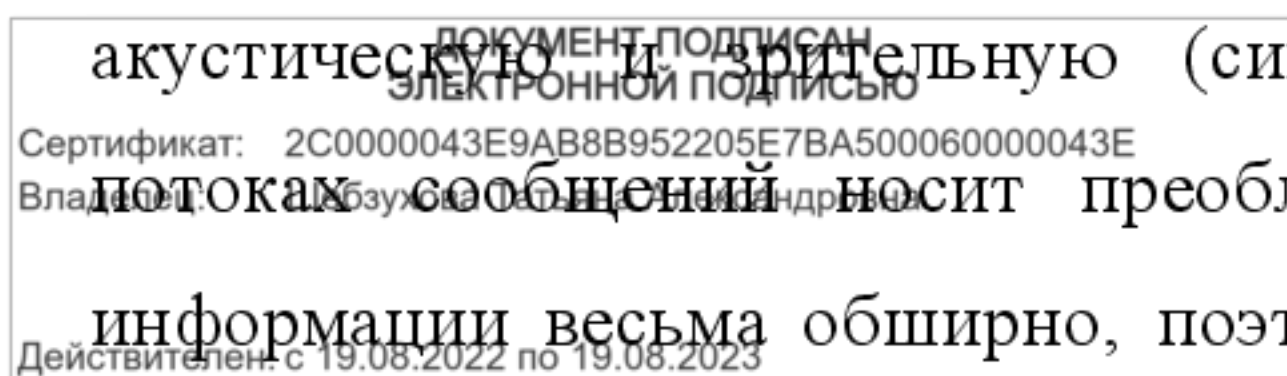
располагая сведениями о рынке открытых отечественных и зарубежных технических средств несанкционированного съема информации, возможно определить необходимые меры и способы защиты информации. Это одна из самых сложных задач в проектировании системы защиты коммерческих секретов.

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

Все возможные способы защиты информации сводятся к нескольким основным методикам:

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

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



видовую и аналогово-цифровую.

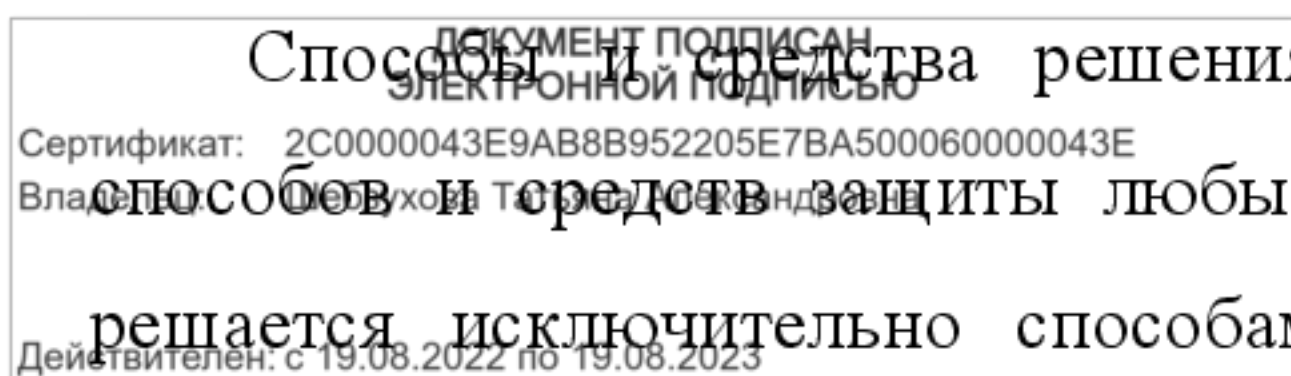
Самыми распространенными способами несанкционированного получения конфиденциальной информации являются:

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

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

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

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



защиты информации.

Лабораторная работа № 1

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

Цель работы: изучить методику поиска объективов скрытых видеокамер.

1. Теоретическая часть

Описание прибора «Оптик»

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

Поиск объектива видеокамеры методом световой локации.

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

Таблица 1.

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

Сертификат
Владелец: 2C0000043E9AB8F952205E7BA500060000043E
Шебзухова Татьяна Александровна
Документ подписан
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Действителен: с 19.08.2022 по 19.08.2023

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: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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

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

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

По окончании заряда на приборе погаснет индикатор CNG.

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



Рис. 1

Прибор готов к работе.

Порядок работы с прибором

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

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

камера может быть не обнаружена.

ДОКУМЕНТ ПОДПИСАН
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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

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

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

На рис. 2 показан пример выявленной видеокамеры

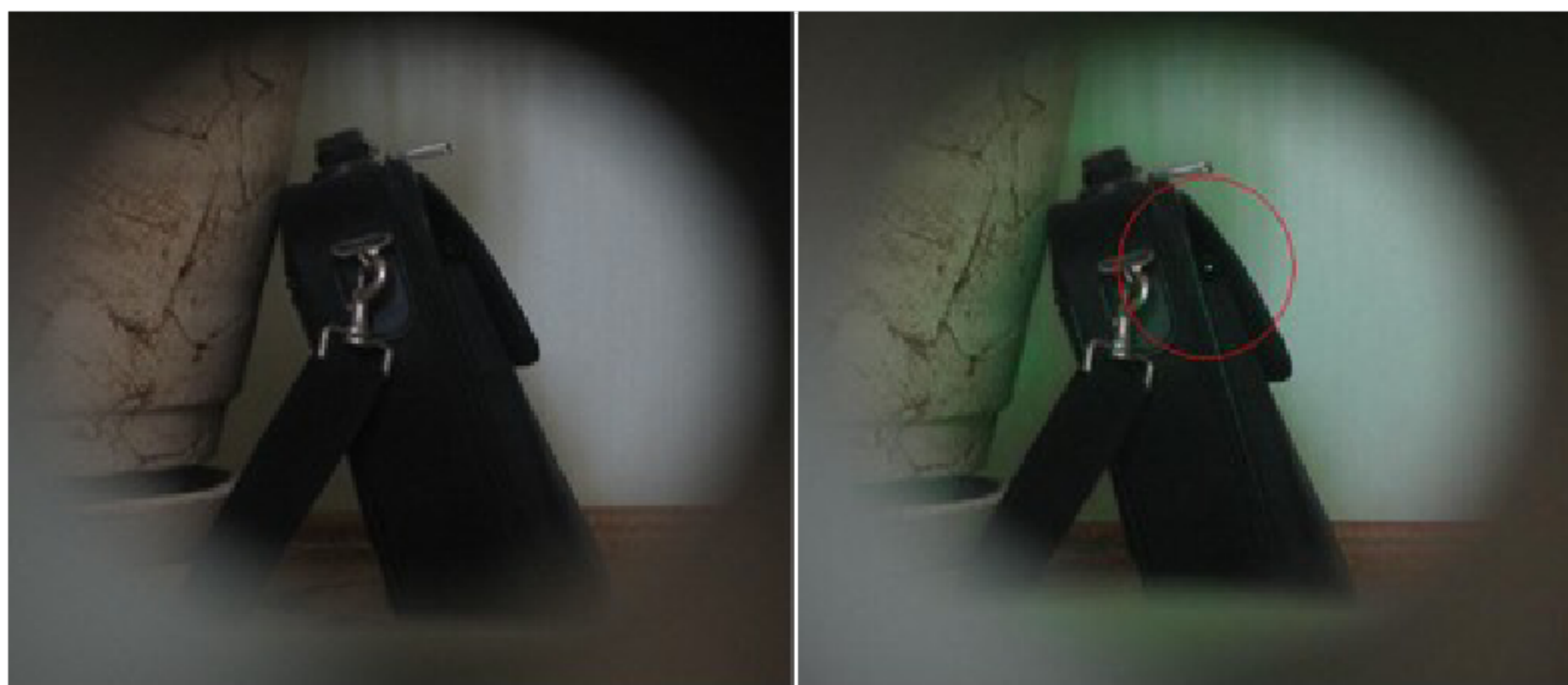


Рис. 2 - Пример выявления видеокамеры

Рекомендации по поиску скрытых камер

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

Вероятнее всего такими местами являются: места работы (столы с сидящими за ними людьми), места отдыха (кресла, диваны, кровати). В случае

если интерес может представлять, посещало ли то или иное лицо помещение – камера может быть направленно на дверной проём.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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

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

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

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

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

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

Правила техники безопасности

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

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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

Избегать попадания прямых солнечных лучей и нагрева прибора.

Не разбирать и не бросать прибор.

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

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

2. Задание.

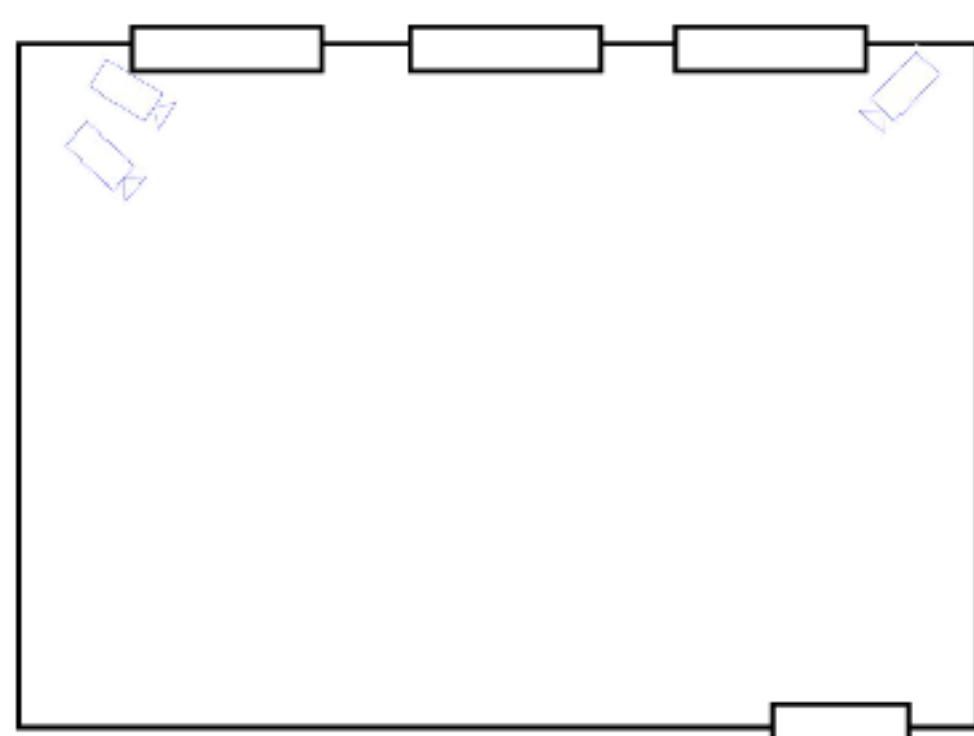
1) Произвести визуальный осмотр защищаемого помещения.

- результат (кол-во в/камер);

2) Произвести осмотр помещения с помощью профессионального обнаружителя скрытых видеокамер «Оптик».

- результат (кол-во в/камер);

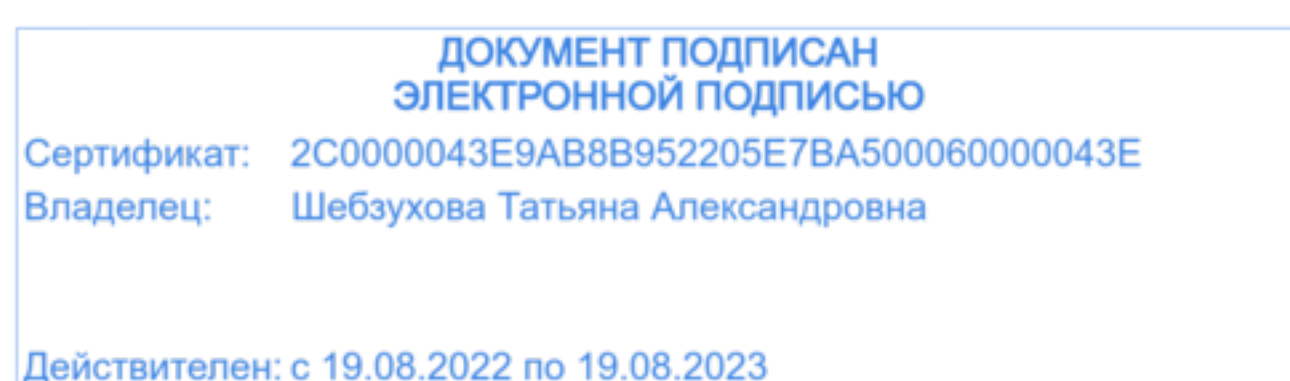
3) Отобразить результаты осмотра на схеме исследуемого помещения.



4) Сделать выводы.

5) Ответить на вопросы.

5. Содержание отчёта и его форма



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

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

6. Вопросы для самоконтроля:

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

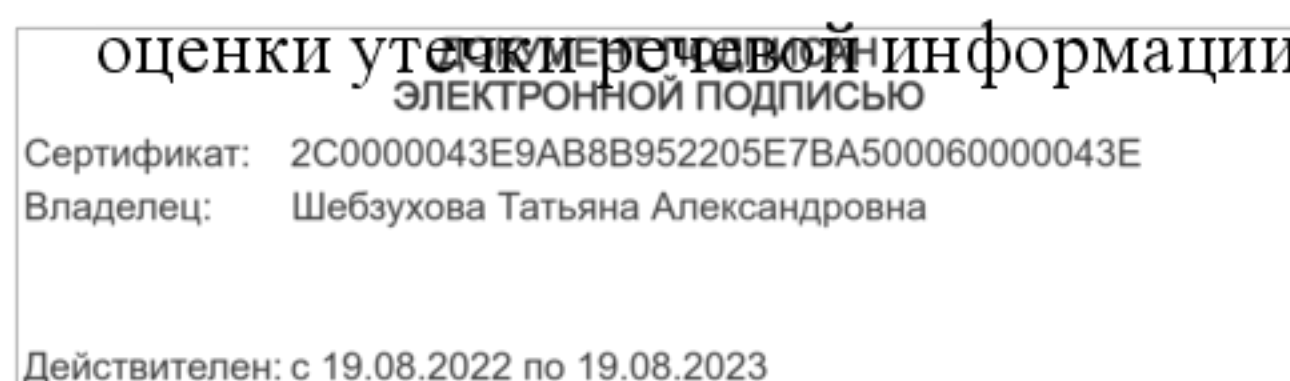
Лабораторная работа № 2

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

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

Задачи лабораторного практикума:

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



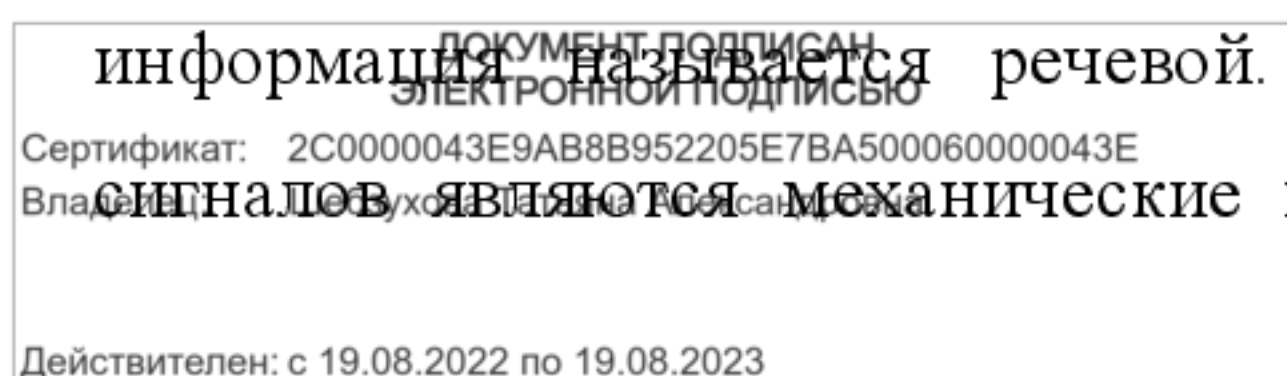
1. Теория.

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

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

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

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



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

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

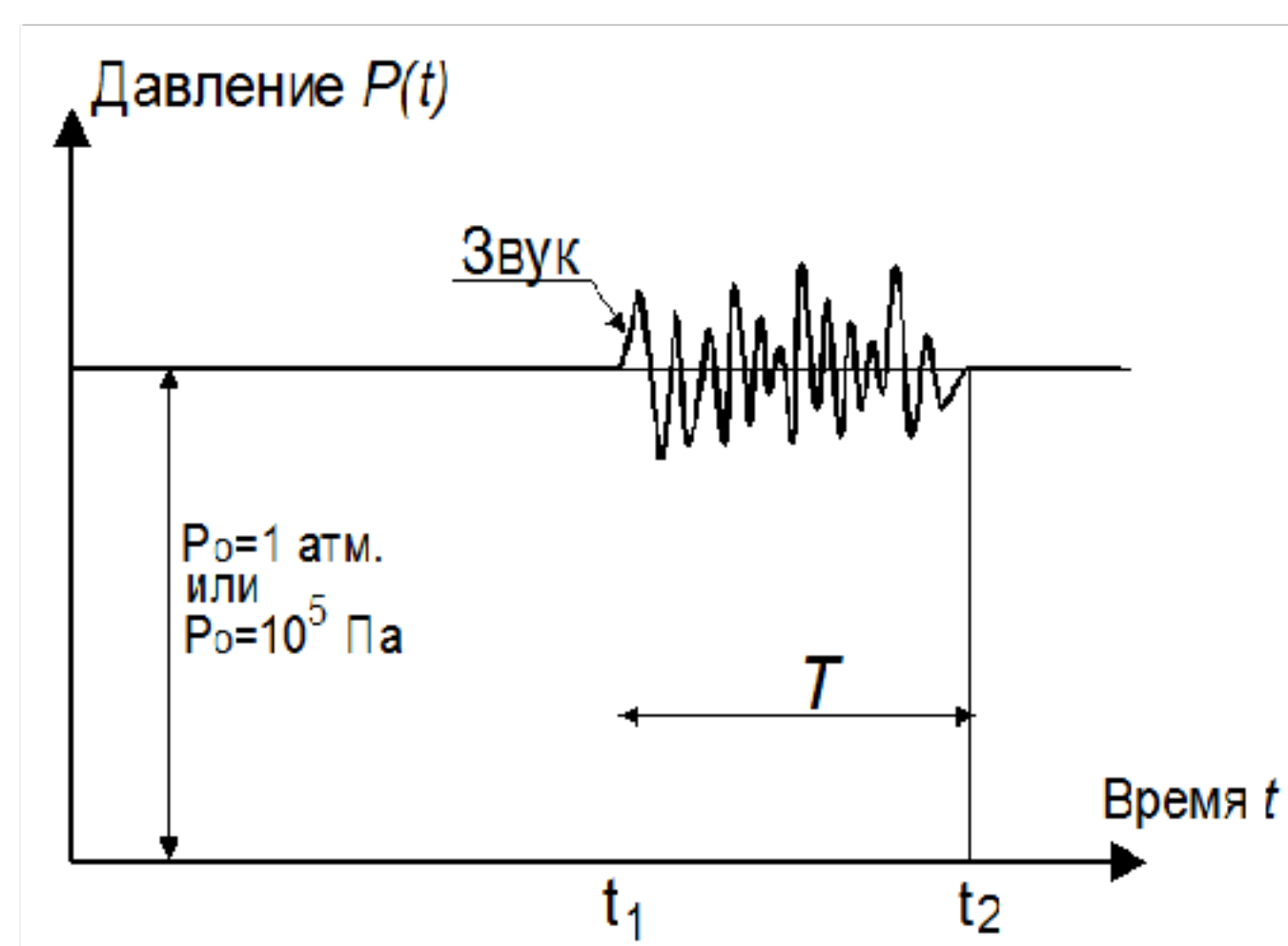


Рис. 2.1. Изменение давление в воздушной среде при возникновении звука

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

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

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

которые называются защищаемыми помещениями (ЗП).

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

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

Таблица 2.1.

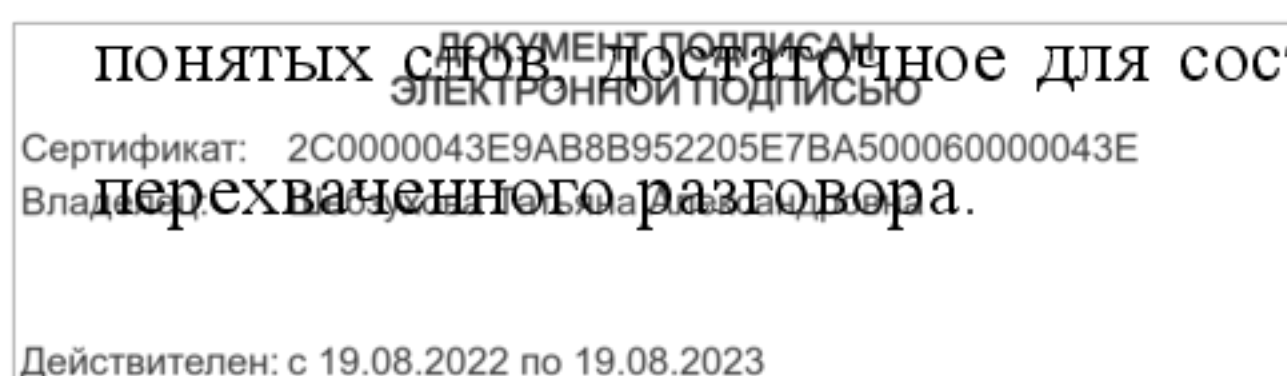
Потенциальные технические каналы утечки речевой информации

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

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

1) Перехваченное речевое сообщение содержит количество правильно

понятых слов, достаточное для составления подробной справки о содержании перехваченного разговора.



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

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

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

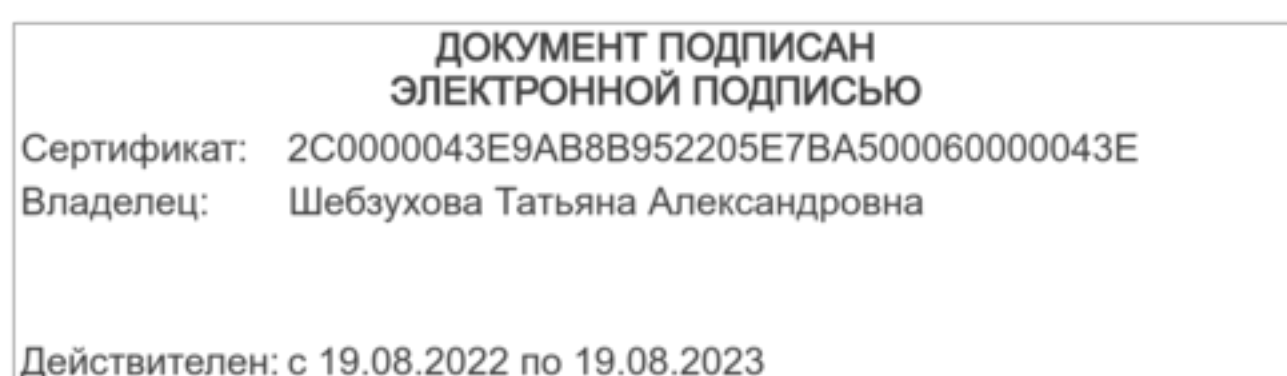
5) При прослушивании фонограммы перехваченного речевого сообщения невозможно установить факт наличия речи.

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

2. Методика выбора контрольных точек

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

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



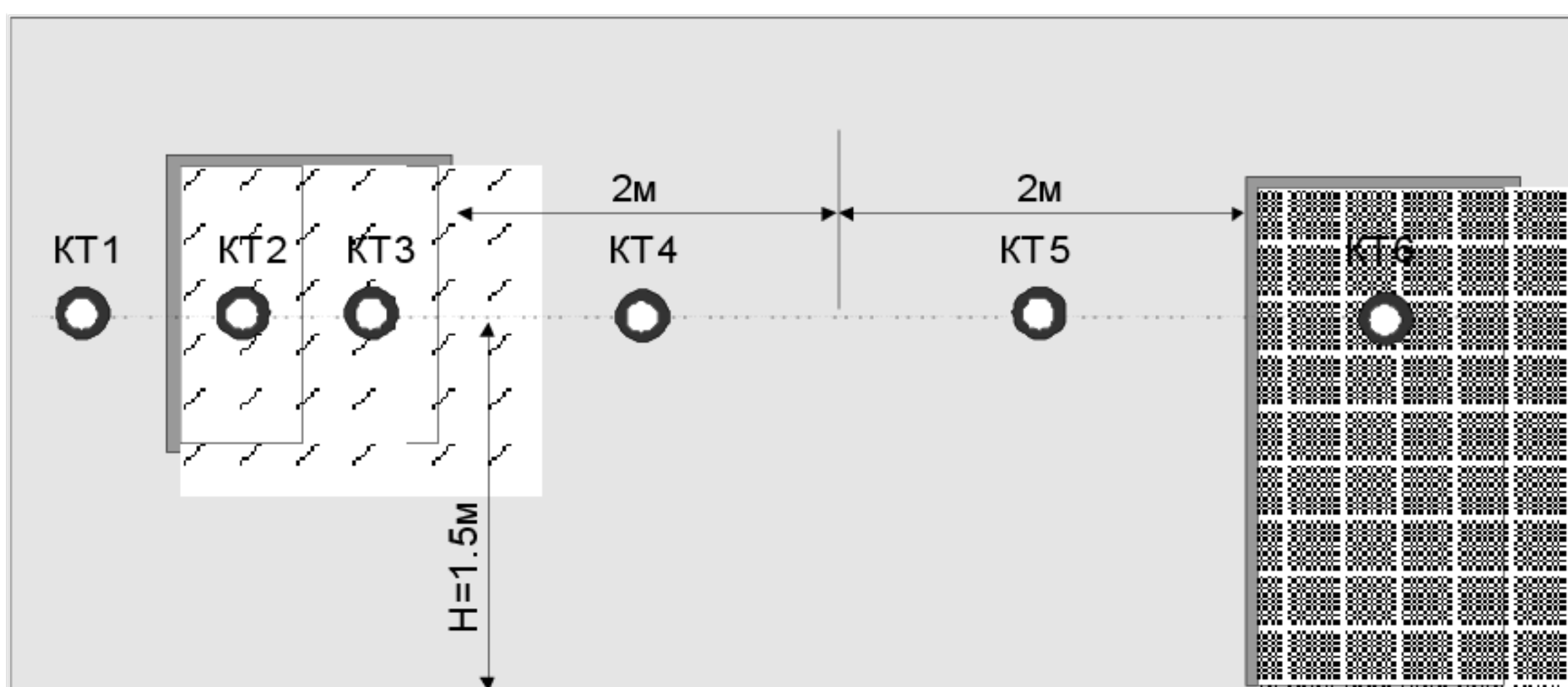


Рисунок 2.2 - Размещение КТ на вертикальных ограждающих конструкциях

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

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

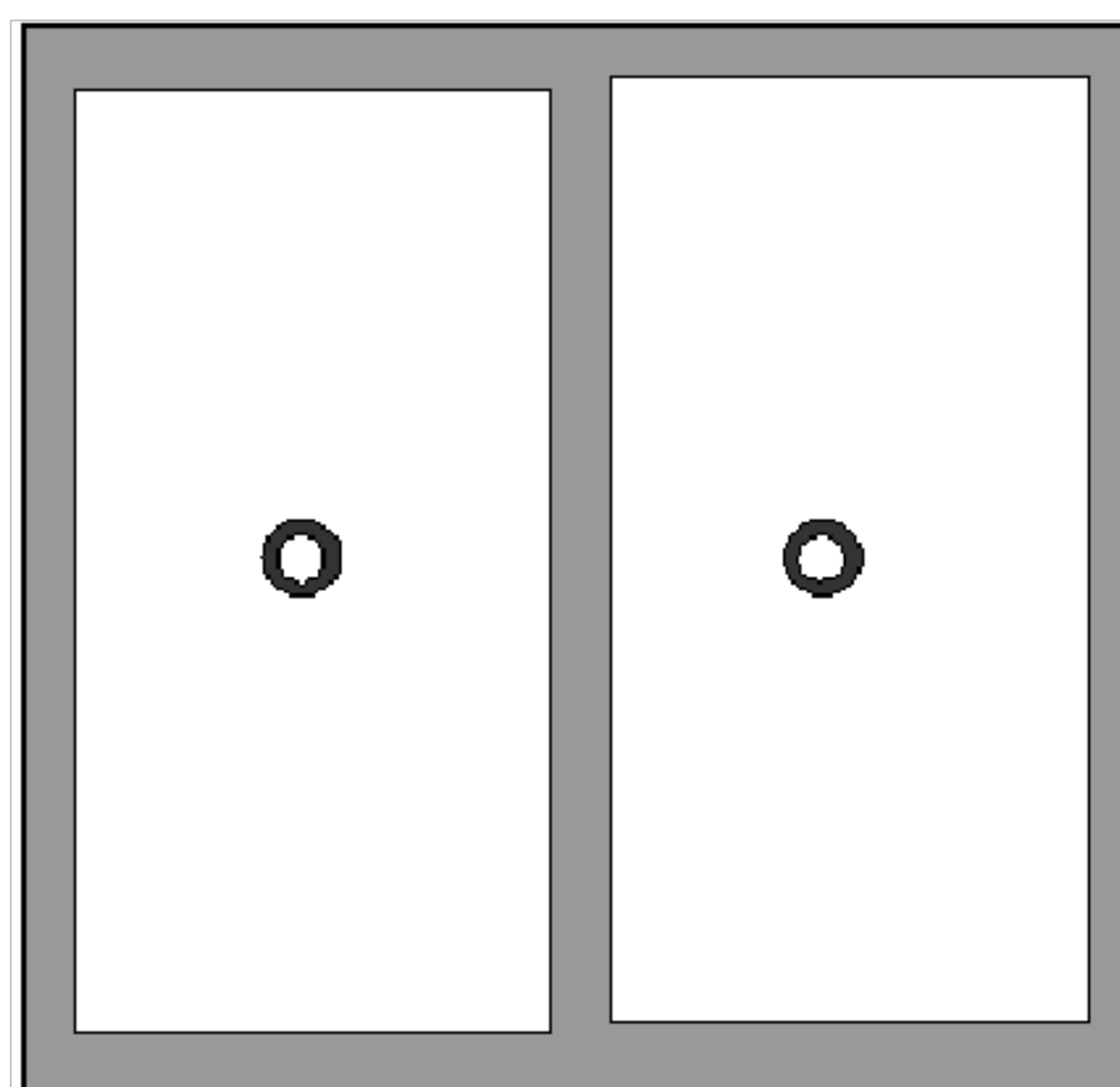


Рисунок 2.3 - Размещение контрольных точек на поверхности оконного остекления для акустических измерений

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

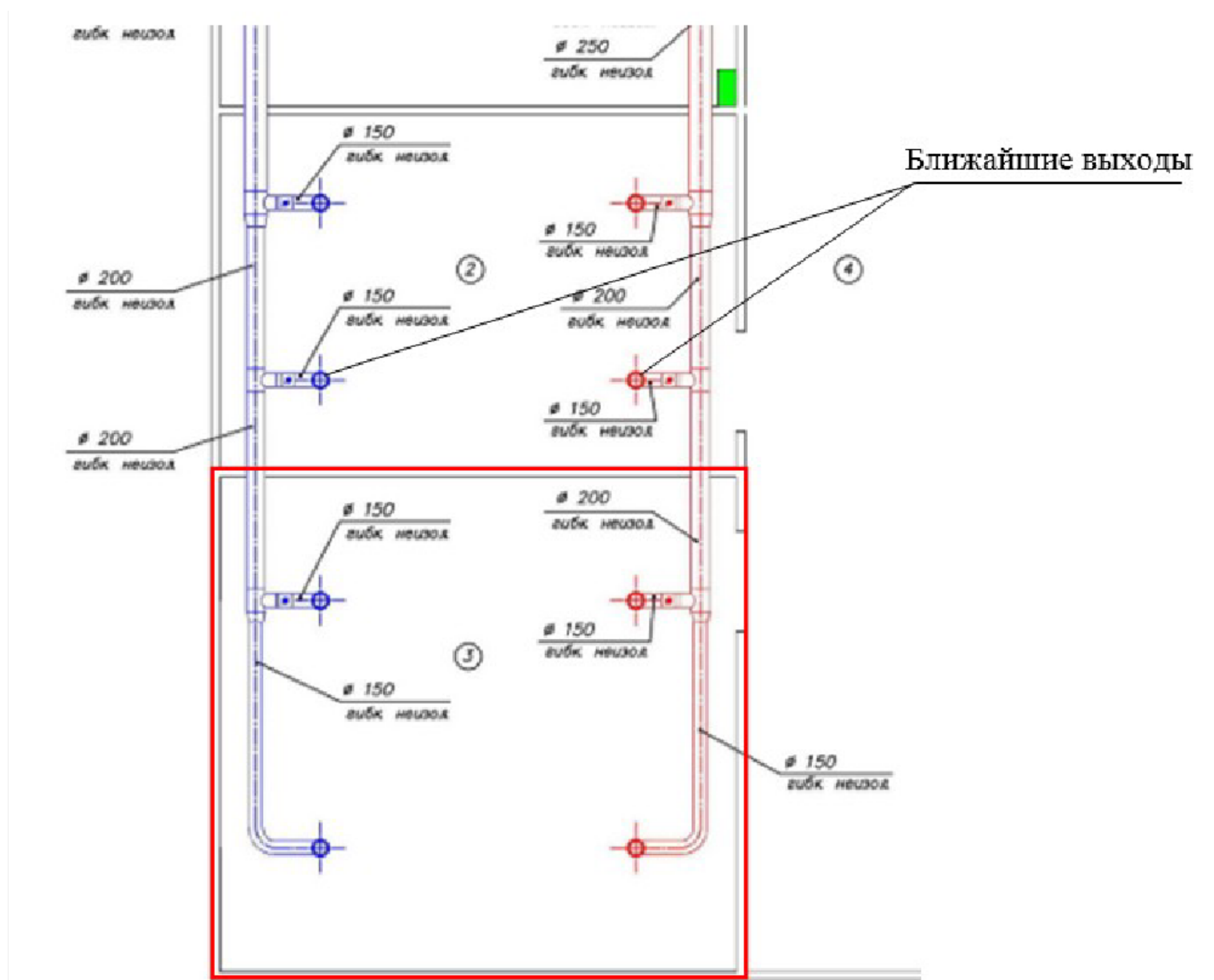


Рисунок 2.4 - Размещение точек выхода для акустических измерений на воздуховодах

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

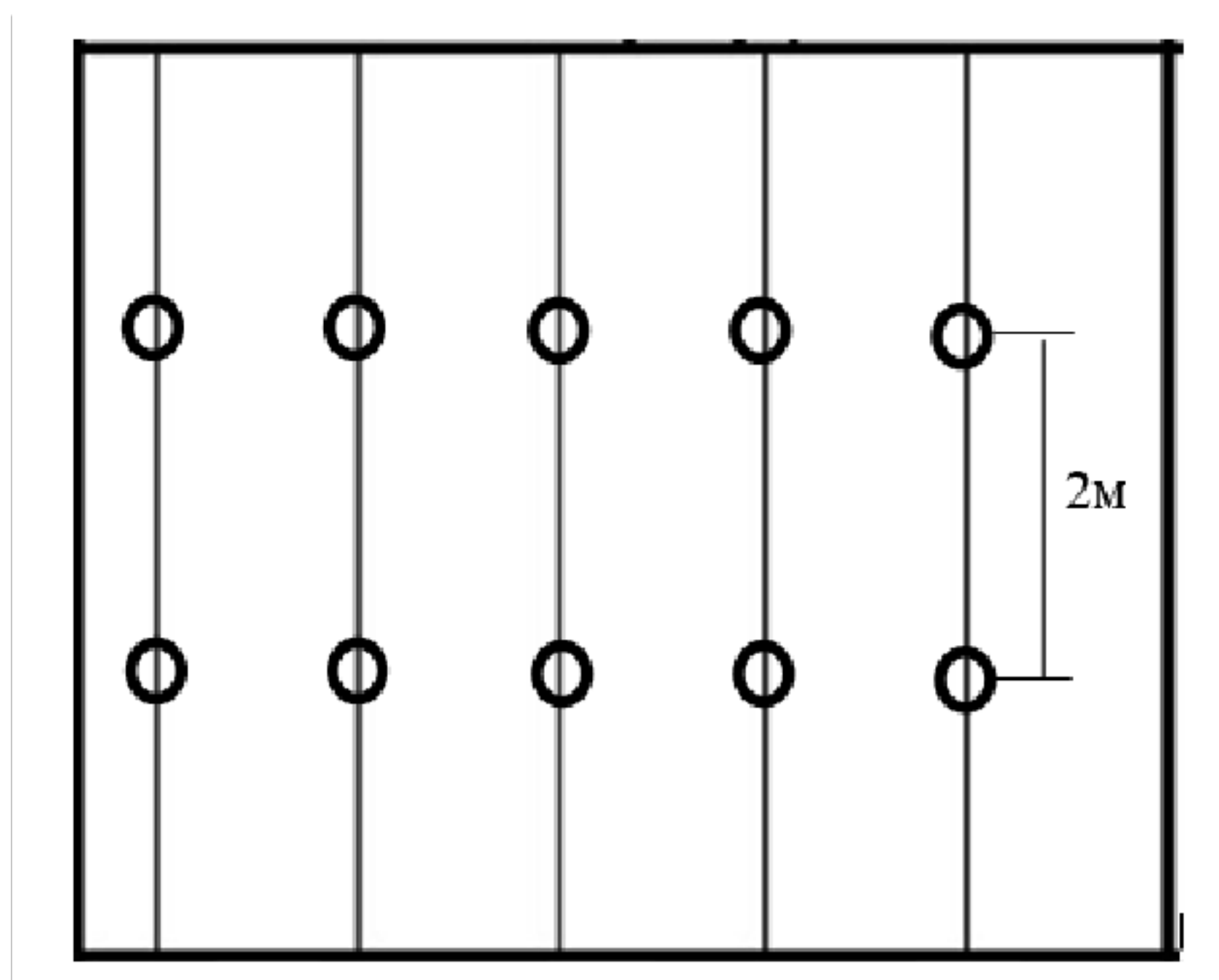


Рисунок 2.5 - Размещение контрольных точек на горизонтальных конструкциях для акустических измерений

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

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

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

2.3 Инструментальное исследование

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

Описание поискового прибора «Спайдер».

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Органы управления и индикации.	
Сертификат:	2C0000043E9AB8B952205E7BA500060000043E
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023	



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

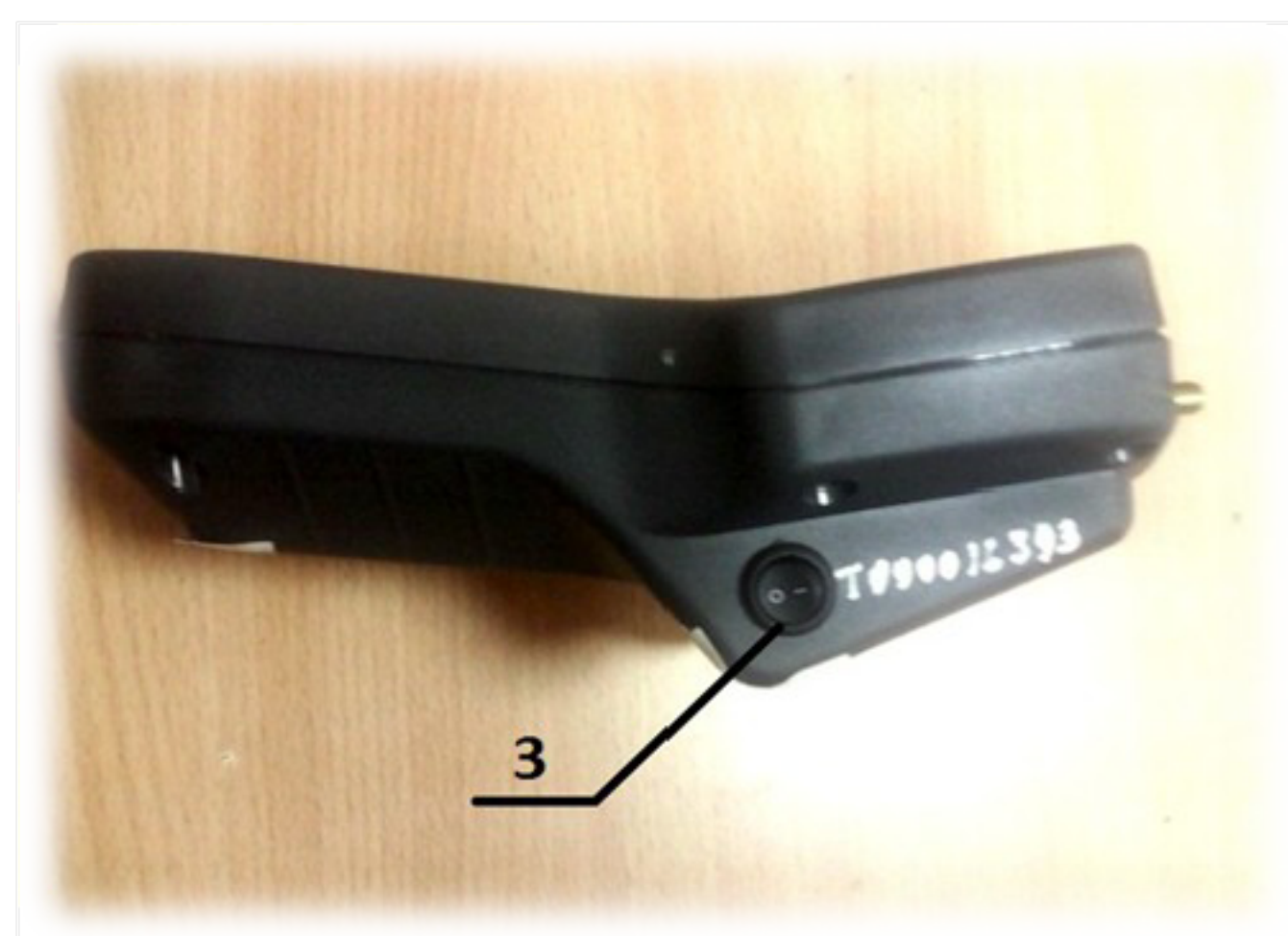


Рисунок 2.7 – многофункциональный поисковой прибор «Спайдер» (вид с правого бока).

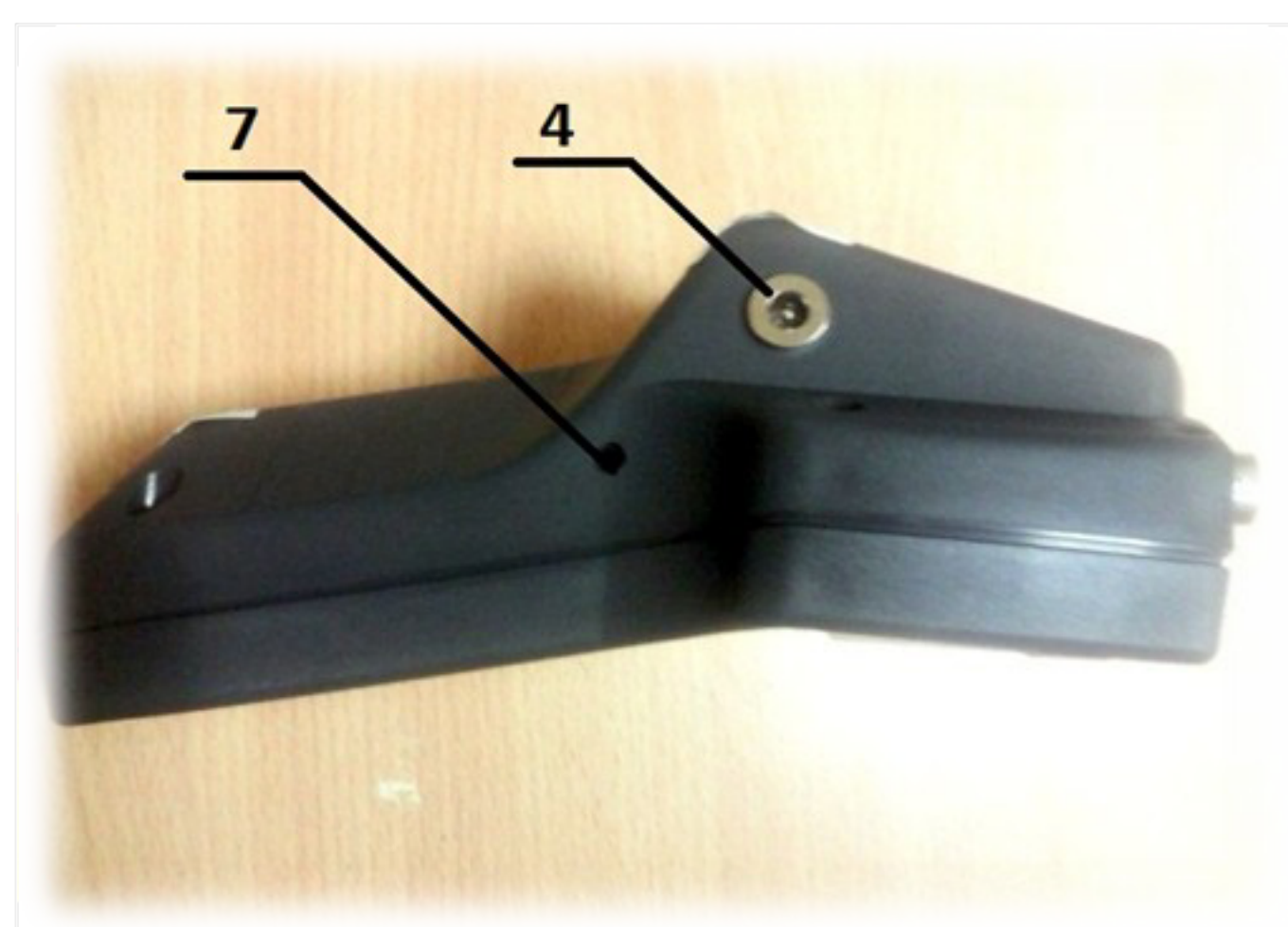


Рисунок 2.8 – многофункциональный поисковой прибор «Спайдер» (вид с левого бока).

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023



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

Описание обозначений:

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

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

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

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

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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

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

- 1) Присоединить к прибору акустический датчик;



Рисунок 2.10 – акустический датчик.

- 2) Включить источник звука внутри проверяемого помещения.
- 3) Включить прибор кнопкой 2, переключив кнопку питания с 0 на 1.

Прибор автоматически перейдет в соответствующий датчику режим работы;

- 4) При необходимости выбрать режим спектрального отображения улавливаемого сигнала кнопкой Fm/Am;
- 5) Микрофон направить на выбранную точку как показано на схеме рис. 2.11.

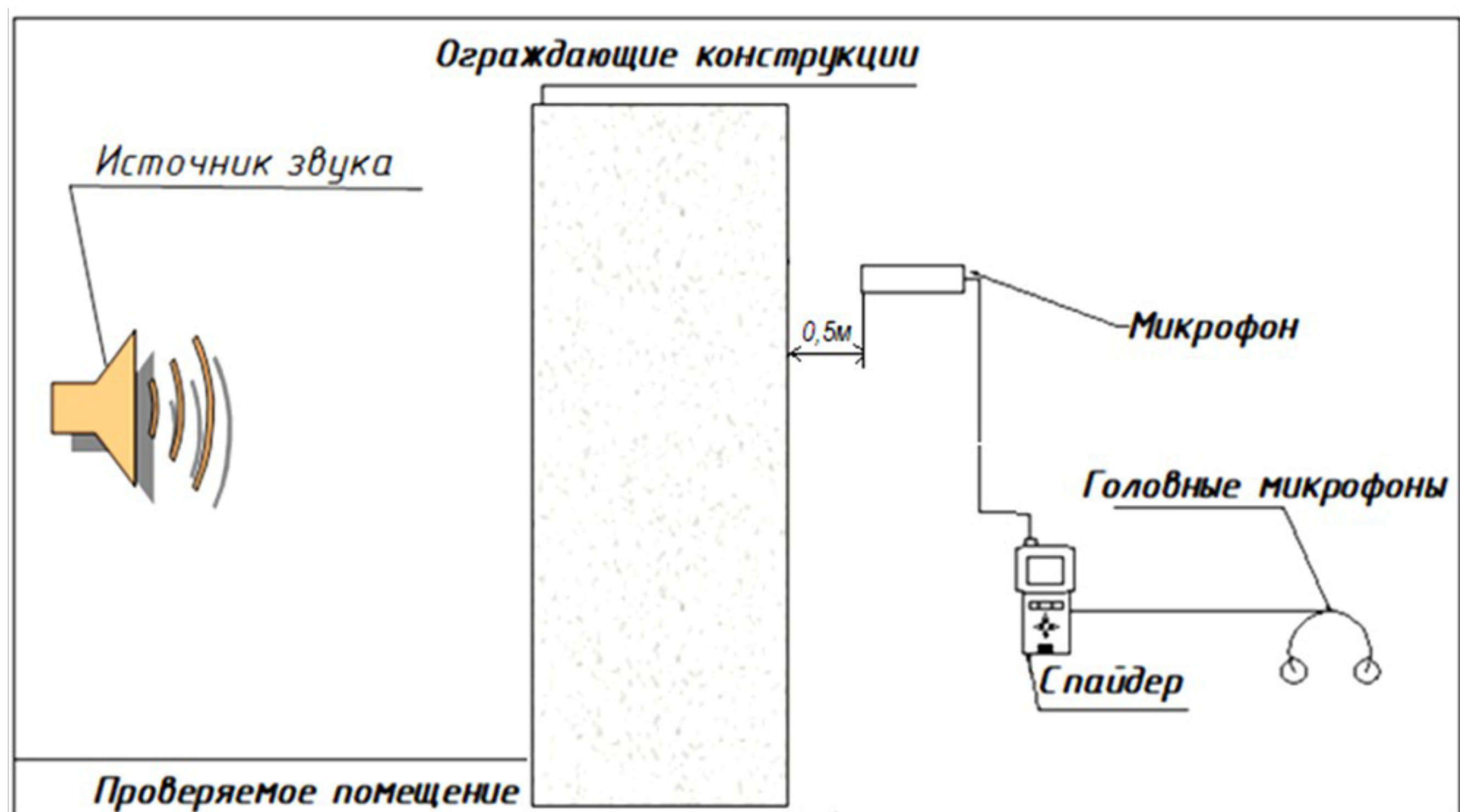


Рисунок 2.11 - Выявление акустических утечек информации с помощью многофункционального поискового прибора «Спайдер»

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

4. Задания по работе:

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

Таблица 2.2 Результаты акустических исследований без САЗ (пример)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННЫМ ПОДПИСЫВАТЕЛЕМ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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

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

6) Сделать выводы.

7) Ответить на вопросы.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

Вопросы для самоконтроля:

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

Лабораторная работа № 3.

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

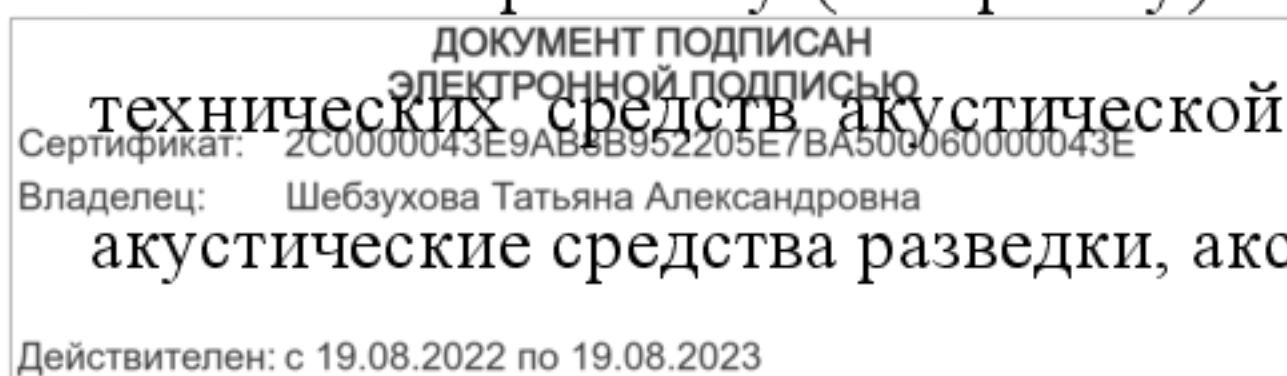
Цель лабораторного практикума: отработка навыков проведения измерений по выявлению виброакустических каналов утечки речевой информации.

Задачи лабораторного практикума:

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

1. Теория.

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



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

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

Таблица 3.1.

Потенциальные технические каналы утечки речевой информации

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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

2. Методика выбора контрольных точек

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

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

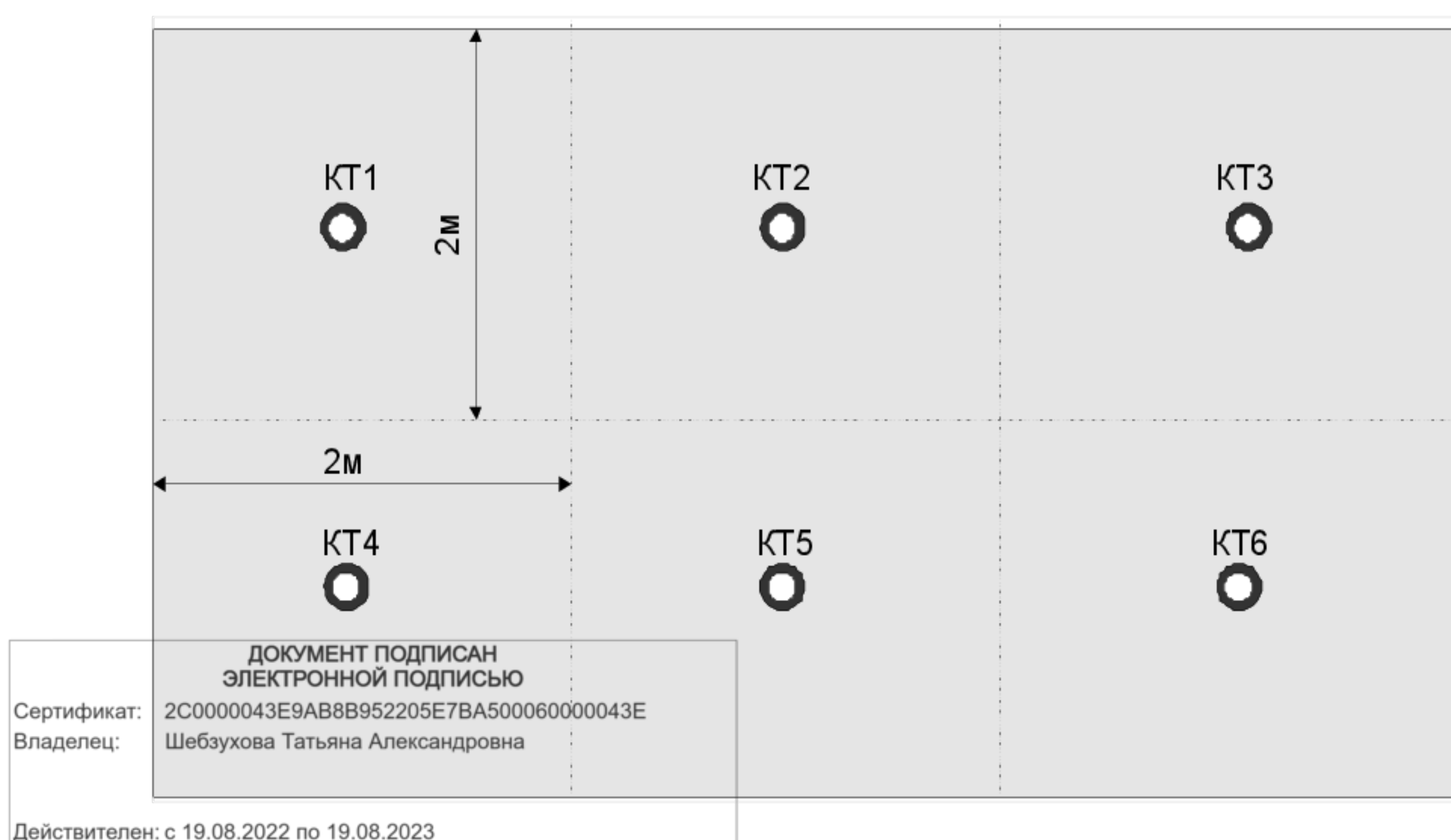


Рисунок 3.1 - Размещение КТ на однородных горизонтальных и вертикальных ограждающих конструкциях

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

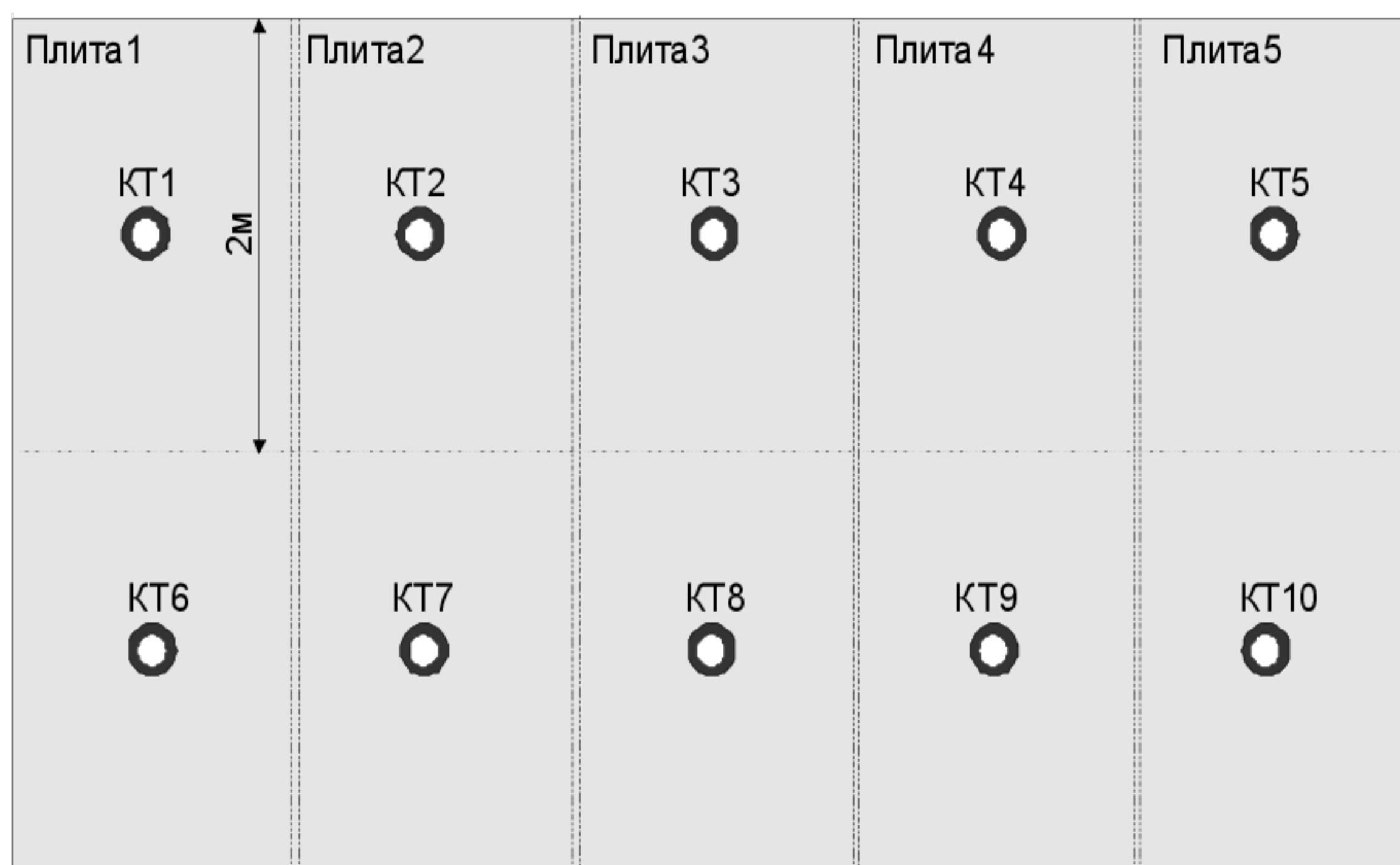


Рисунок 3.2 - Размещение контрольных точек на неоднородной поверхности

Примечание:

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

контрольные точки для выявления утечки.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

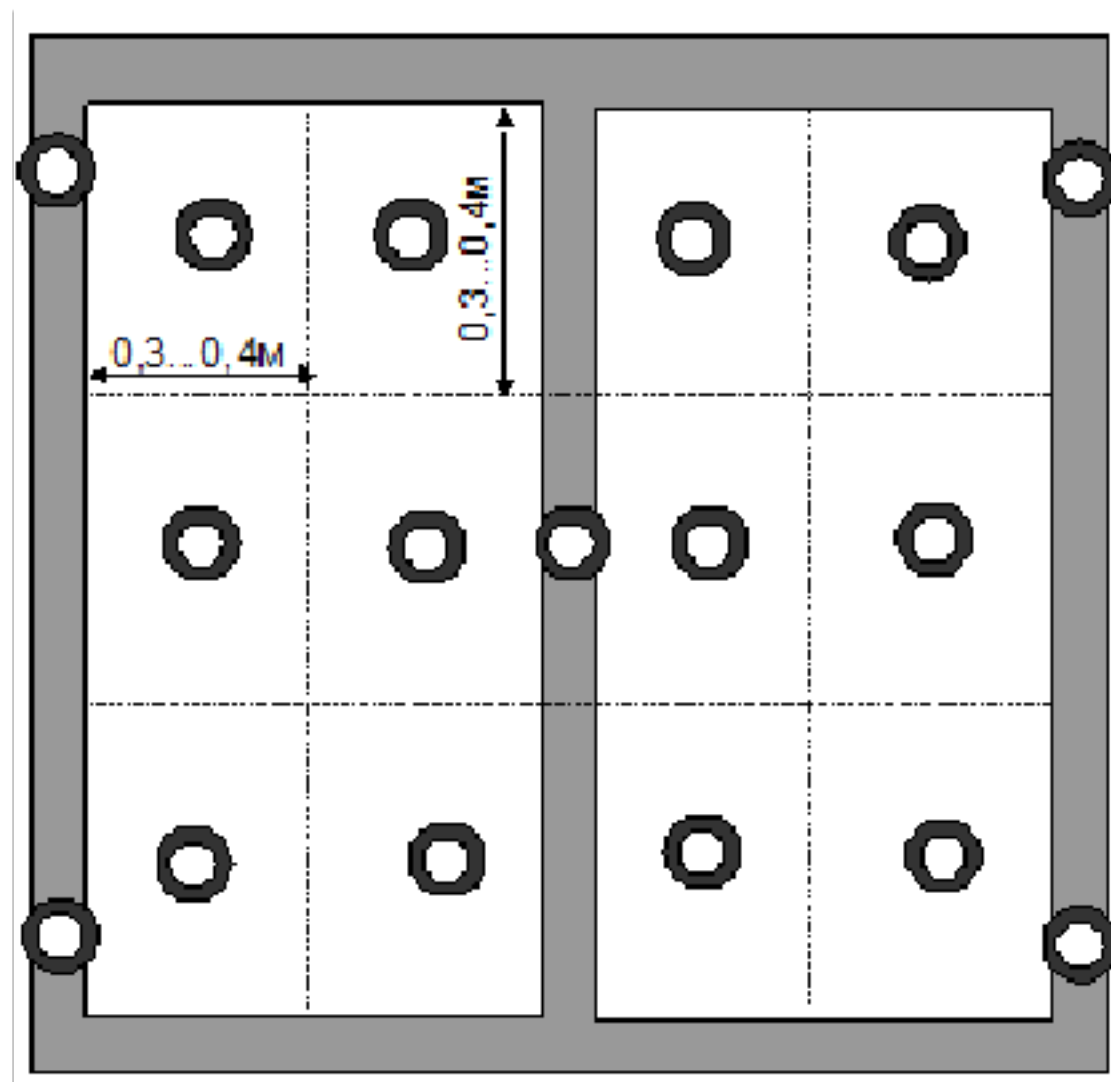


Рисунок 3.3 - Размещение контрольных точек на поверхности оконного остекления для вибрационных измерений

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

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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

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



Рисунок 3.6 – Виброакустический датчик.

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

Задания по работе:

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

виброакустического исследования, полученные в ходе обследования в таблицу

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

Таблица 3.1. Результаты виброакустических исследований без САЗ (вариант)

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2G0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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

4) Сделать выводы.

3. Вопросы для самоконтроля:

1) Что такое вибрационный канал утечки информации?

2) Какие технические средства могут использоваться злоумышленником для ведения акустической речевой разведки по виброакустическому каналу утечки?

3) Каков показатель разборчивости речи для скрывания факта переговоров?

Лабораторная работа № 4.

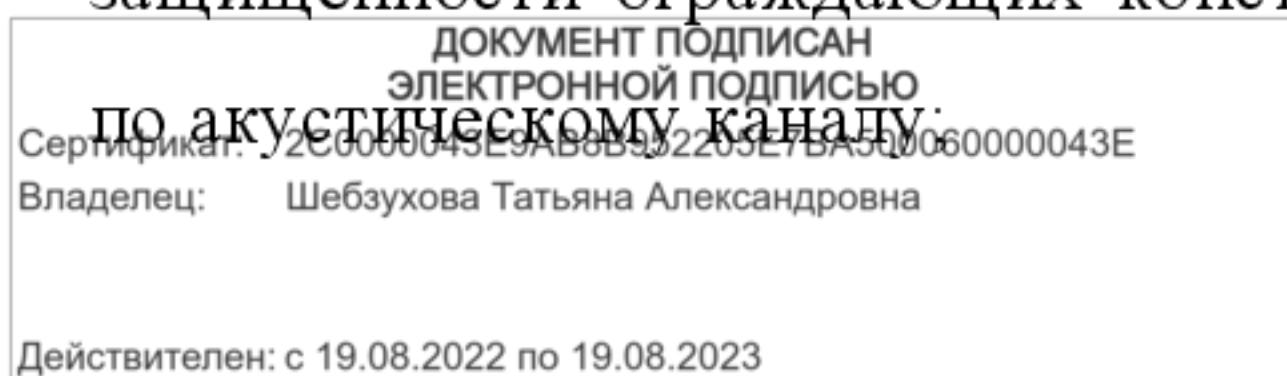
Тема: «Количественная оценка защищенности речевой информации по акустическому каналу через двери с использованием ПАК «Шёпот»»

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

Основными задачами работы являются:

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

по акустическому каналу:



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

1. Теоретическая часть

1.1 Специальные документы РФ по защите информации:

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

1.2. Аудит информационной безопасности по акустическому каналу.

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

Среди важнейших каналов утечки информации являются акустический и виброакустический каналы.

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