Источники и каналы утечки информации. Основы технической защиты информации.

План лекции

УЧЕБНЫЕ ВОПРОСЫ :

1. Понятие и виды каналов утечки информации.

2. Технические каналы утечки информации.

3. Защита информации от утечки по техническим каналам.

4. Специальные проверки объектов информатизации.

ЛИТЕРАТУРА

Нормативно-правовые акты, официальные издания

1. Национальный стандарт РФ ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации».
2. Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
3. Техническая защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056-2005. № 479-ст.

ЛИТЕРАТУРА

Основная литература

1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В.К. Новиков, С.Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : ЮНИТИ-ДАНА, 2019. – 287 с.

2. Основы информационной безопасности в органах внутренних дел : учеб. пособие / сост. А.Б. Сизоненко, С.Г. Клюев, В.Н. Цимбал. - Краснодар : Краснодарский университет МВД России, 2016. – 122 с.

ЛИТЕРАТУРА

Основная литература

3. Костюченко, К.Л. Основы информационной безопасности в органах внутренних дел : учеб. пособие / К. Л. Костюченко, С. В. Мухачев. – Екатеринбург: Уральский юридический институт МВД России, 2015. – 155 с.

1. Понятие и виды каналов утечки информации.

Объект информатизации –

это совокупность **информационных ресурсов, средств и систем обработки информации**, используемых в соответствии с заданной информационной технологией, а также **средств их обеспечения, помещений или объектов** (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или **помещений и объектов, предназначенных для ведения конфиденциальных переговоров**.

Утечка информации –
это неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

УТЕЧКА

Разглашение

Несанкционированный доступ

По техническим каналам

Разглашение информации – это **несанкционированное доведение** защищаемой **информации до потребителей**, **не имеющих права доступа** к этой информации.

Несанкционированный доступ к информации (**НСД**) – **получение** защищаемой **информации** заинтересованными **субъектами с нарушением установленных** нормативными и правовыми документами (актами) или обладателями информации **прав или правил разграничения доступа к защищаемой информации.**

Утечка по техническим каналам –

неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Факторы, способствующие утечке информации:

– несовершенство правового обеспечения защиты информации;

– нарушение установленных правил защиты информации;

– недостаточность сил и средств для перекрытия каналов утечки информации.

Условия, способствующие утечке информации:

объективные:

– недостаточная правовая регламентация вопросов защиты информации по отдельным вопросам деятельности организации;

– текучесть кадров;

– несоответствие условий деятельности сотрудников организации требованиям по защите информации.

Условия, способствующие утечке информации:

субъективные:

– **незнание сотрудниками** организации правовых актов, **требований по защите информации**;
– **недостаточное внимание руководства вопросам** организации работы **по обеспечению защиты информации** в организации;
– **слабый контроль** за выполнением требований по защите информации сотрудниками организации.

Канал утечки информации – это физический путь несанкционированного распространения носителя с защищаемой информацией от ее источника к злоумышленнику.

Каналы утечки информации:

– агентурные ;

– легальные;

– технические .

Каналы утечки информации:

Агентурный канал утечки информации – это использование противником тайных агентов для получения несанкционированного доступа к защищаемой информации.

Каналы утечки информации:

Легальные каналы утечки информации – это использование противником открытых источников информации, выведывание под благовидным предлогом сведений у лиц, которым они доверены по службе.

Каналы утечки информации:

Технические каналы утечки информации подразумевают использование специальных технических средств для несанкционированного доступа к защищаемой информации.

2. Технические каналы утечки информации.

Схема появления канала утечки информации

Технический канал утечки информации представляют собой **совокупность объекта разведки, технического средства разведки**, с помощью которого добывается информация об этом объекте, **и физической среды, в которой распространяется информационный сигнал**.

Технические каналы утечки информации (по физической природе носителя):

– **акустические** (включая и акустико-преобразовательные);

– **визуально-оптические**;

– **материально-вещественные** (бумага, фото, магнитные носители, производственные отходы различного вида – твердые, жидкие, газообразные);

– **электромагнитные** (включая магнитные и электрические).

Технические каналы утечки информации:

– технические каналы утечки речевой информации;

– технические каналы утечки видовой информации;

– технические каналы утечки информации, обрабатываемой техническими средствами;

– технические каналы утечки информации, передаваемой по каналам связи.

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Иногда для них в литературе используется термин «технические средства приема, обработки, хранения и передачи информации» (ТСПИ).

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС или в выделенных помещениях.

Технические каналы утечки речевой информации

Носителем речевой информации являются акустические колебания.

Источником акустического сигнала являются механические колебательные системы, в том числе и органы речи человека.

Технические каналы утечки акустической информации:

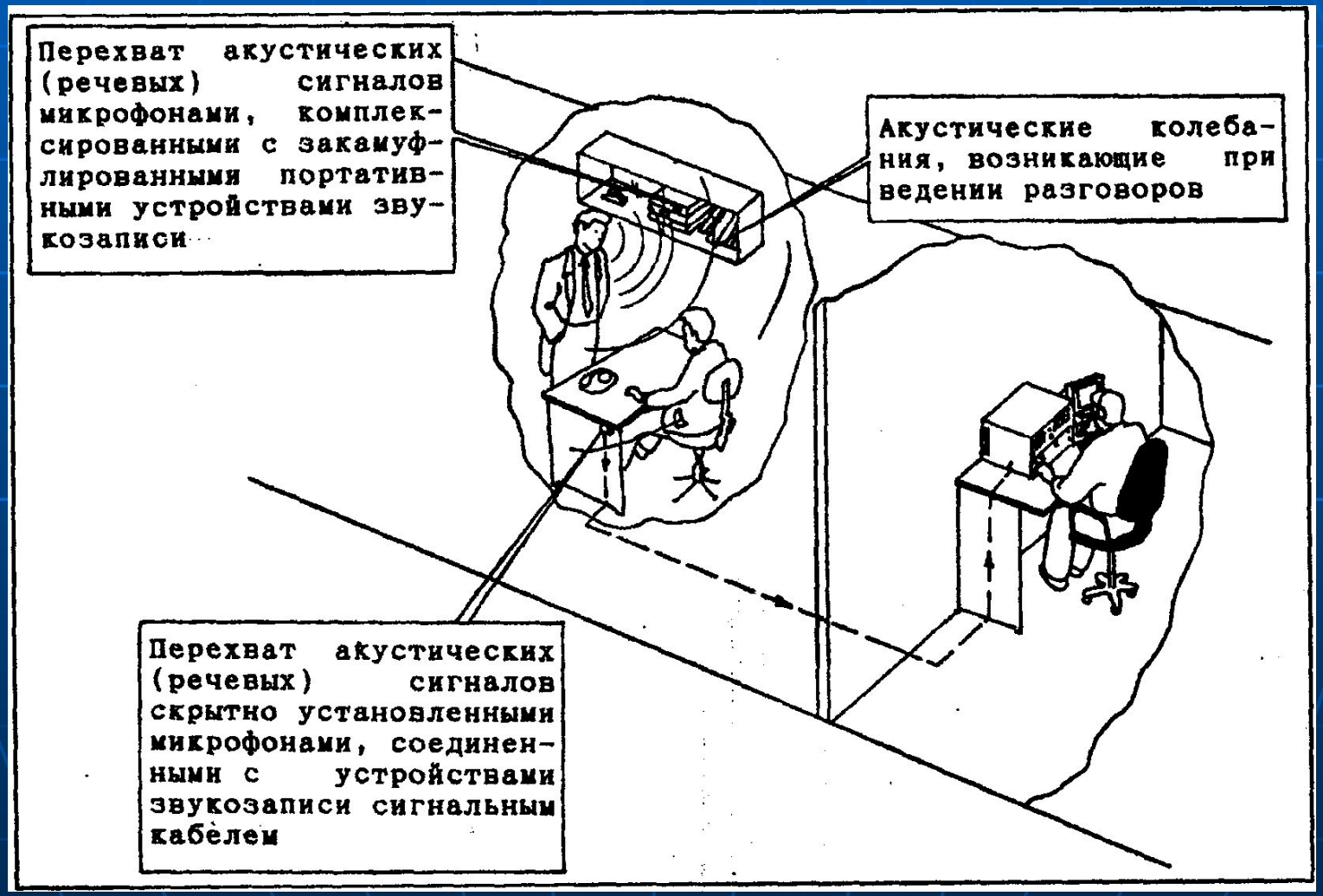
- *воздушные (прямые акустические);*
- *вибрационные (виброакустические);*
- *оптикоэлектронные;*
- *акустоэлектрические;*
- *параметрические.*

В воздушных технических каналах утечки информации **средой распространения акустических сигналов является воздух**, и для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

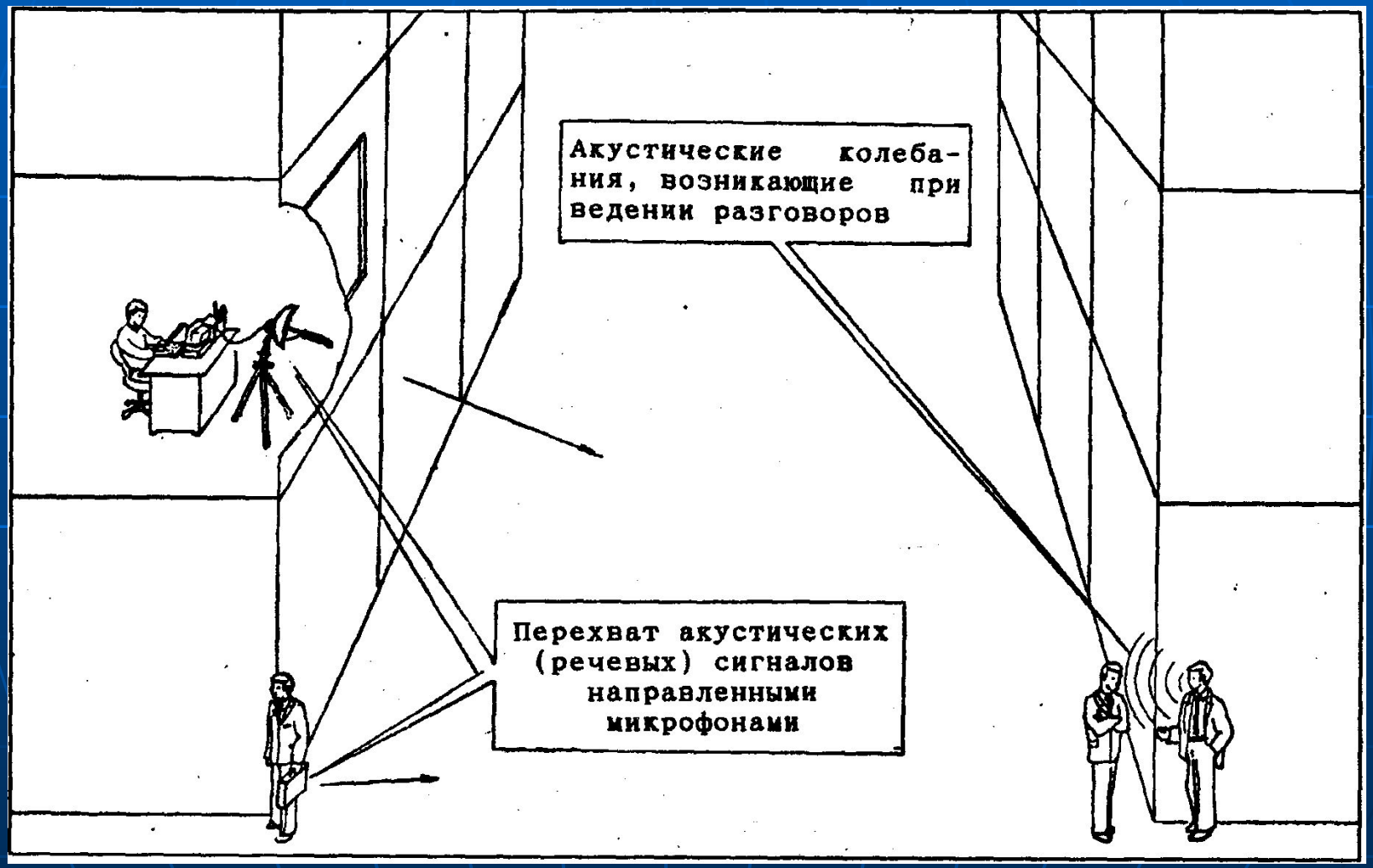
Автономные устройства, конструкционно объединяющие миниатюрные микрофоны и передатчики, называют закладными устройствами перехвата речевой информации, или просто акустическими закладками.

Автономные устройства, конструкционно объединяющие микрофоны и звукозаписывающие устройства, называют диктофонами.

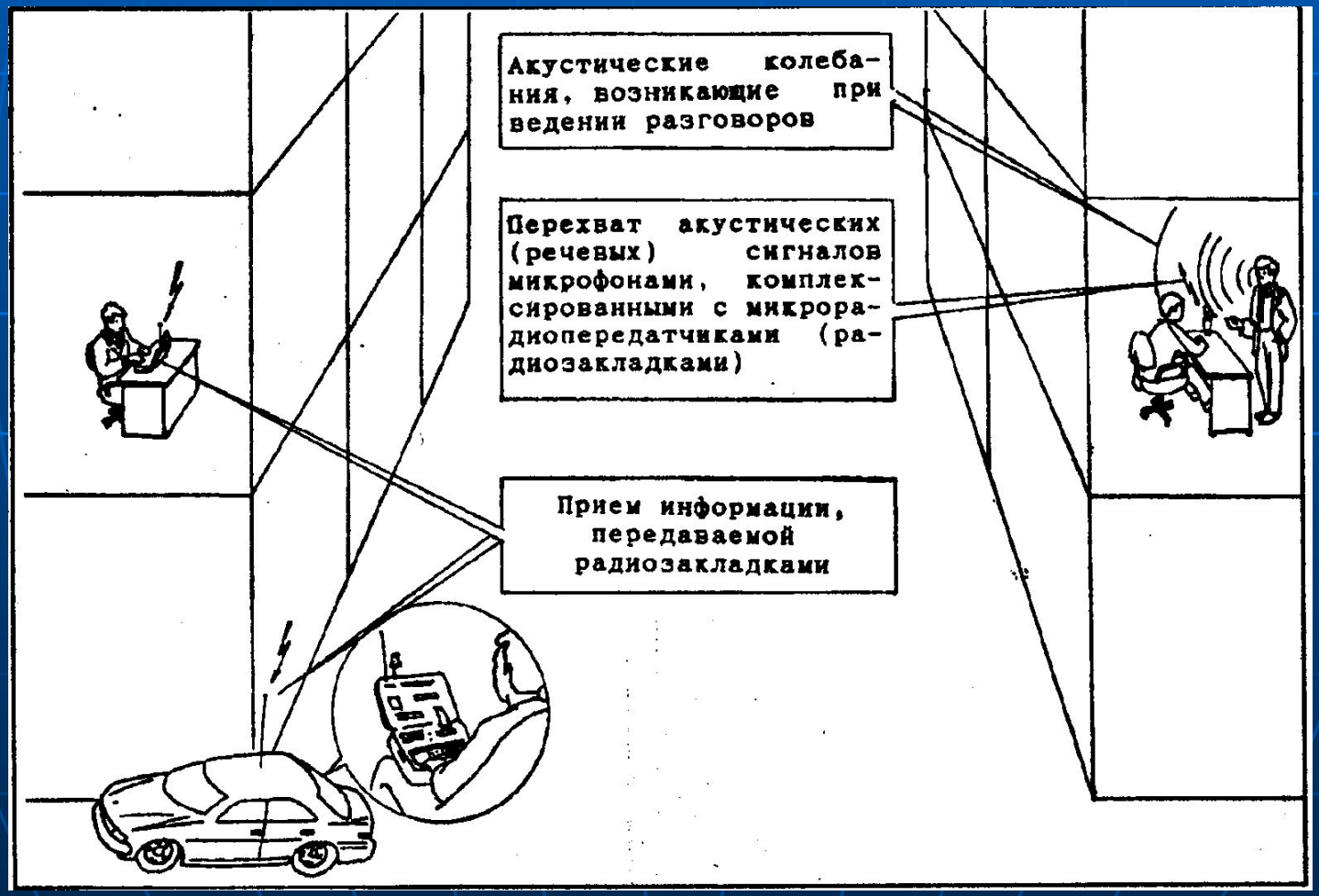
Перехват акустических сигналов микрофонами, комплексированными с портативными устройствами звукозаписи



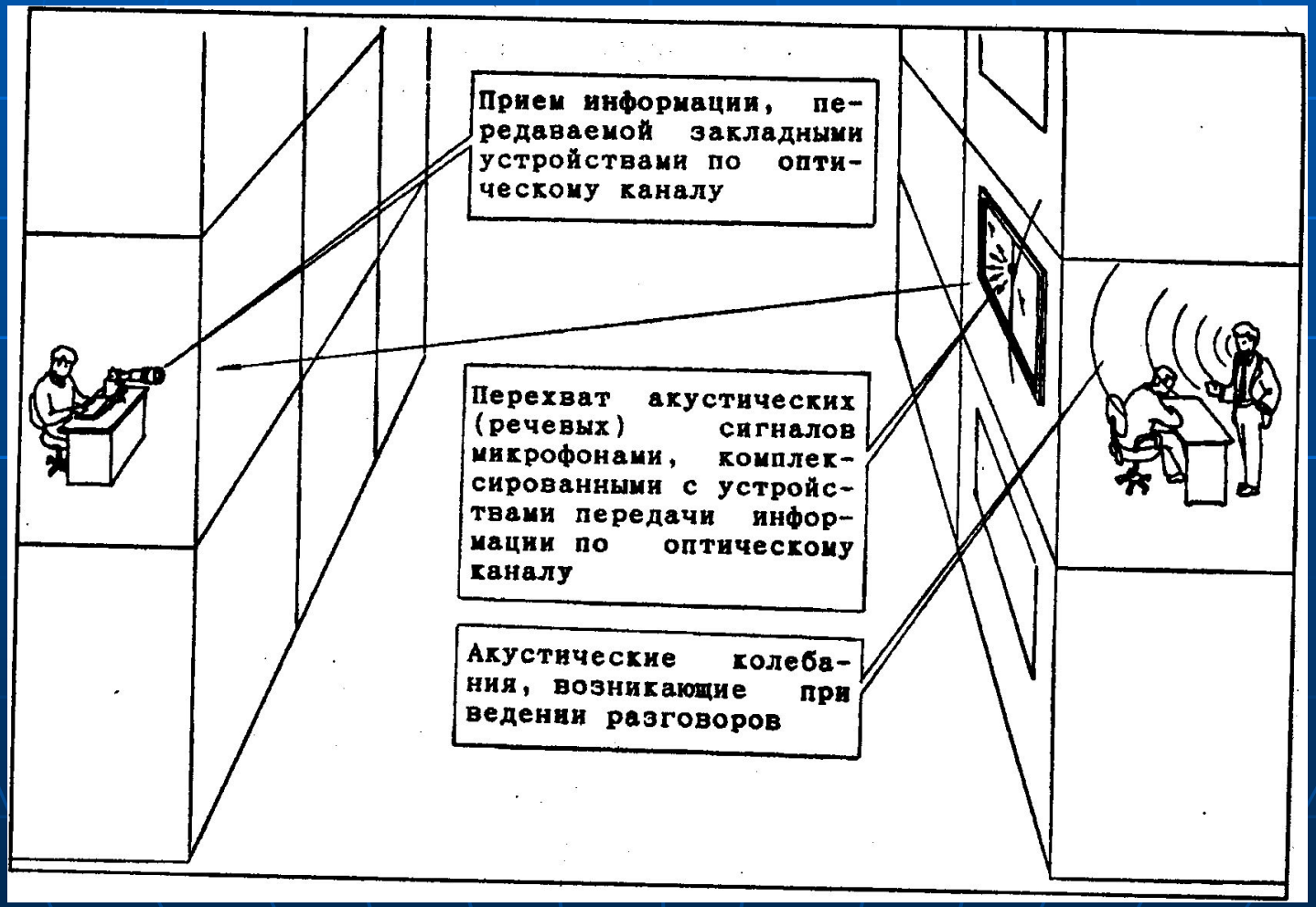
Перехват акустических сигналов направленными микрофонами



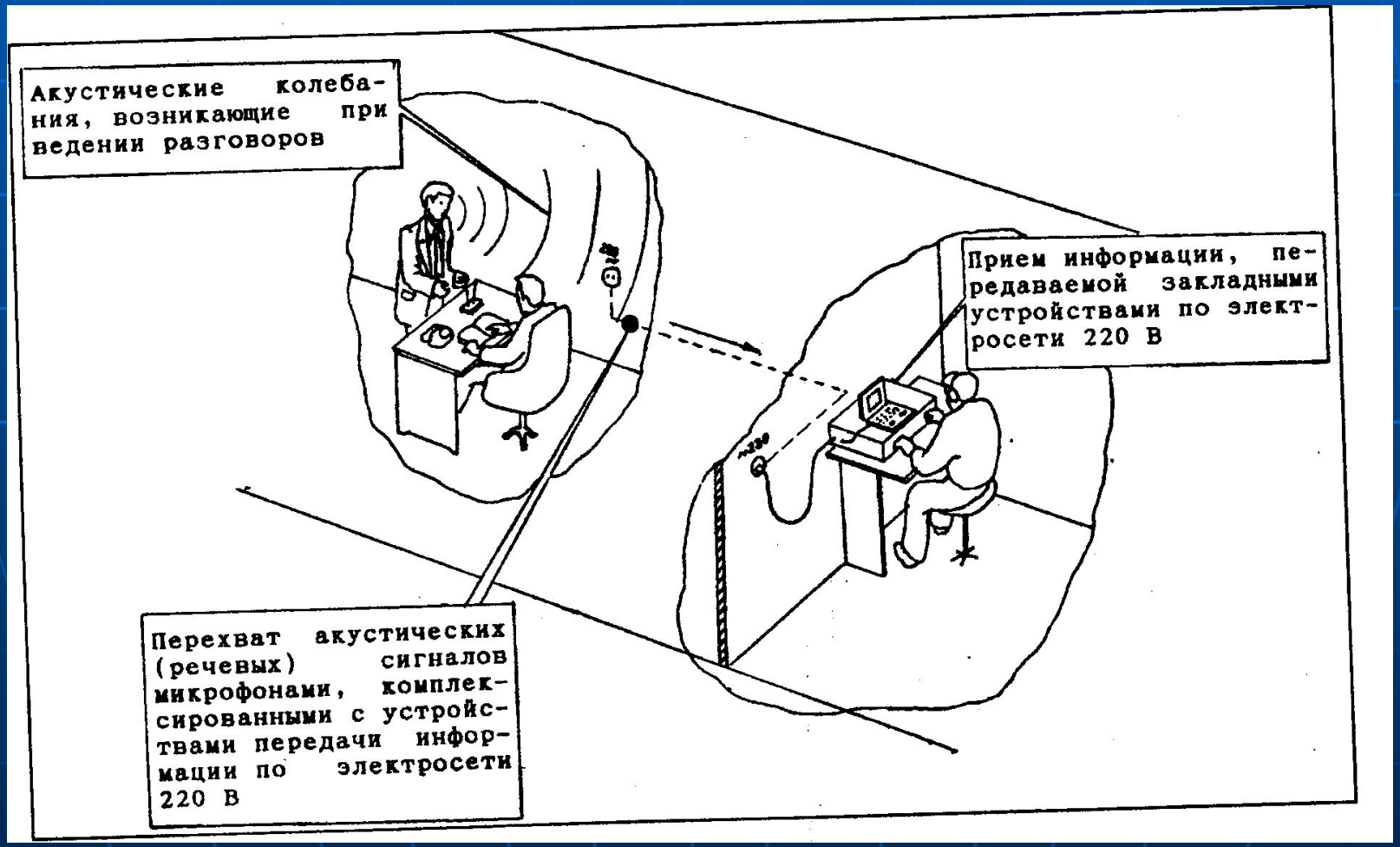
Перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по радиоканалу



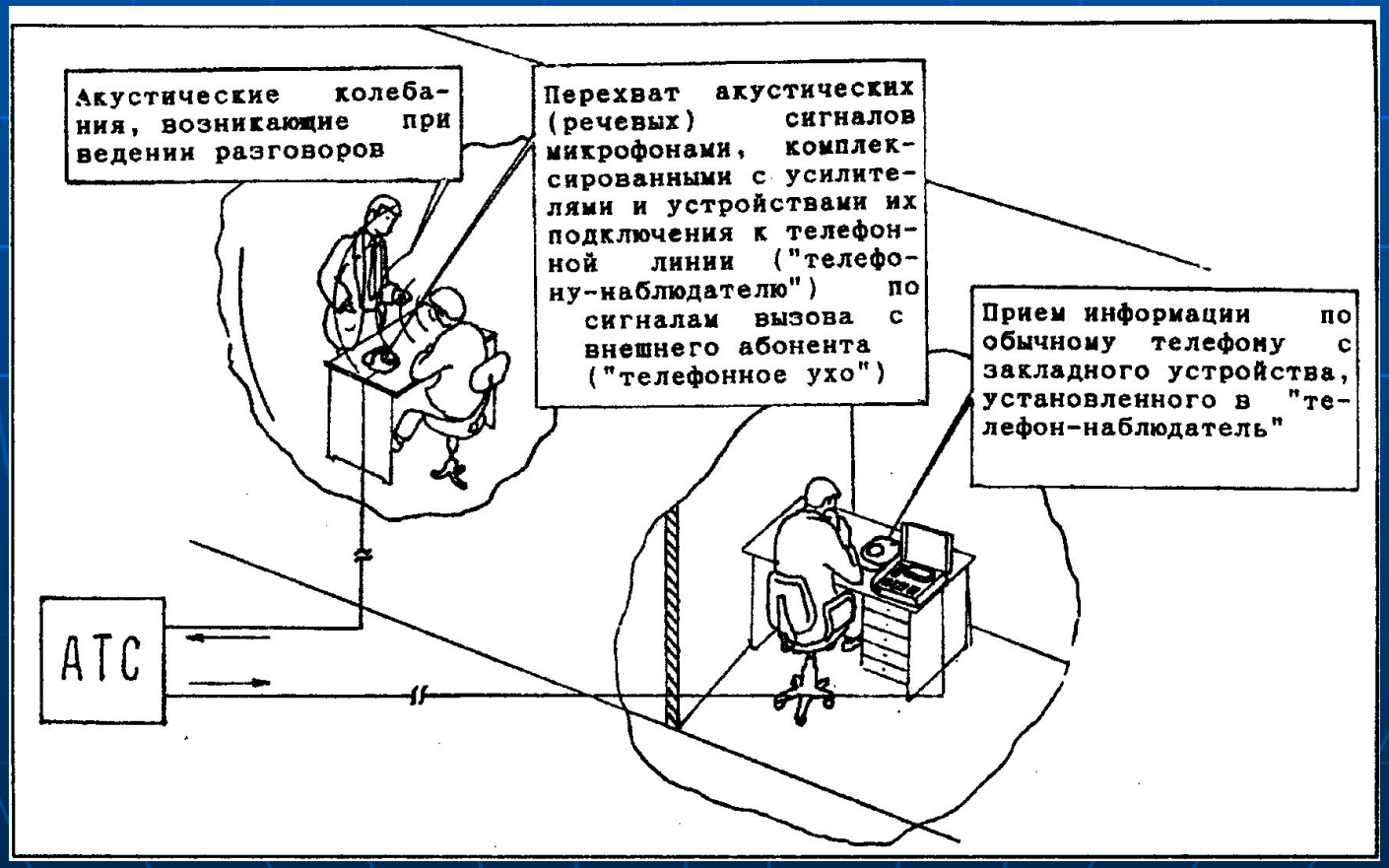
Перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по оптическому каналу



Перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по электросети



Перехват акустических сигналов микрофонами, комплексированными с устройствами их подключения к телефонной линии по сигналам вызова от внешнего абонента

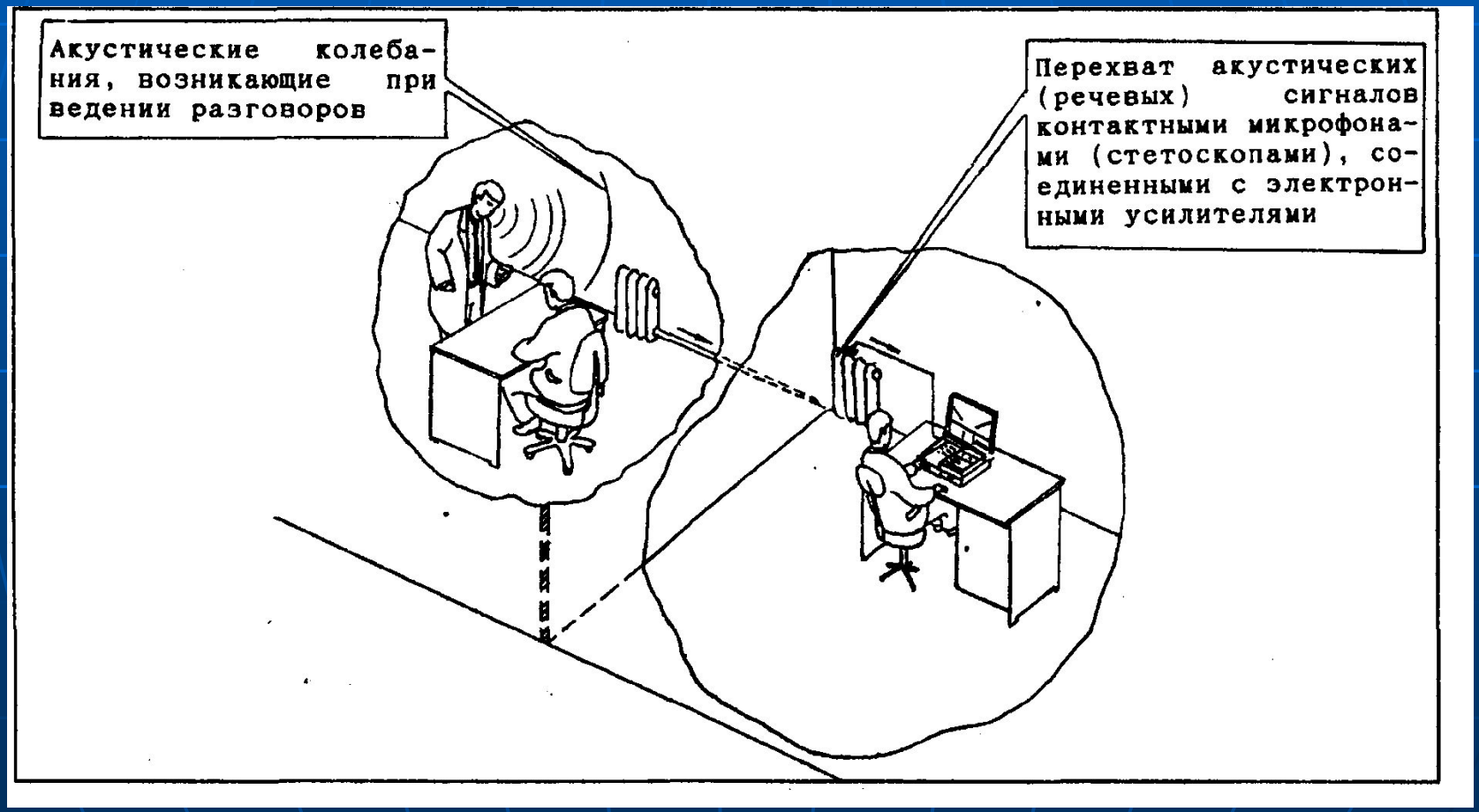


Речевой сигнал, распространяясь в воздухе, может встречать на своем пути различные твердые тела – конструкции зданий и сооружений (стены, потолок, батареи отопления, оконные стекла и т.д.).

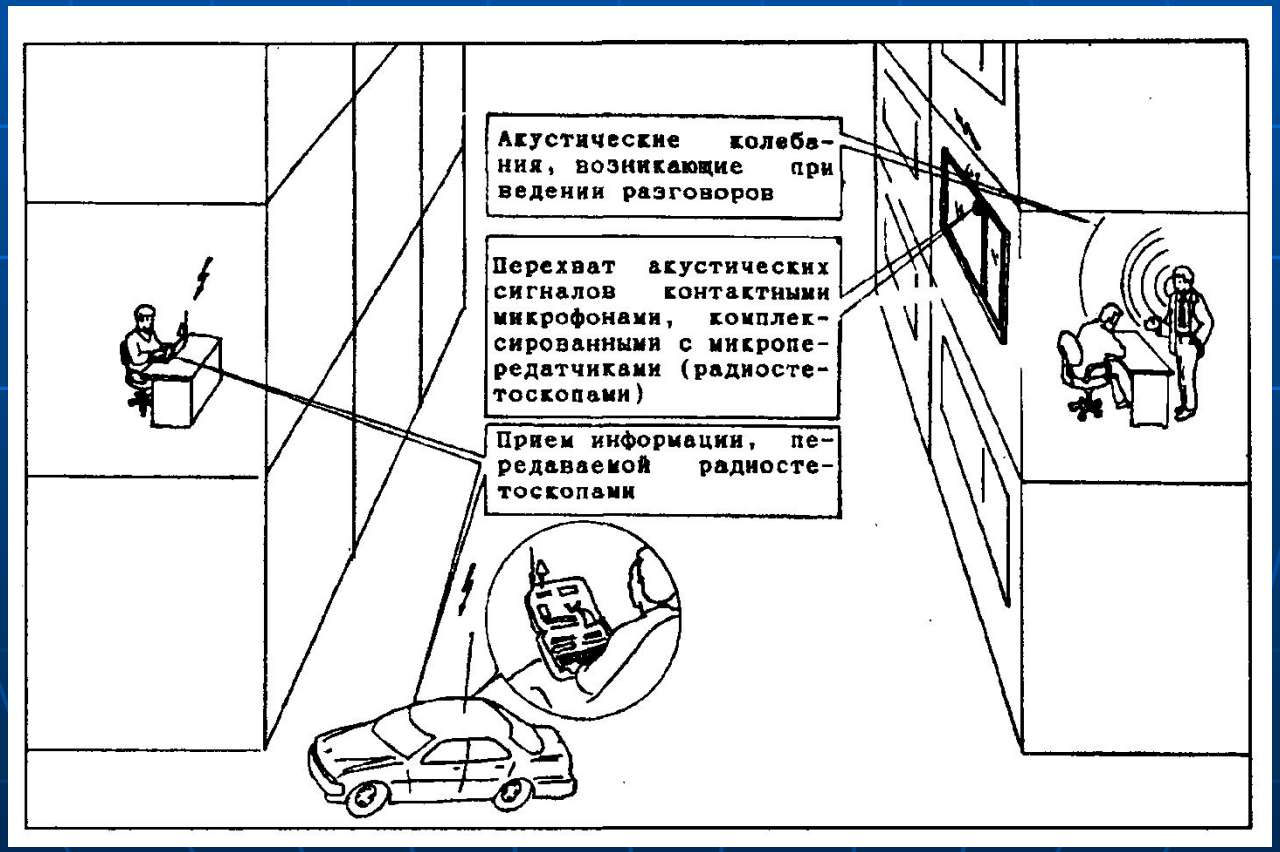
При воздействии сигнала на поверхность твердых тел в последних возникают механические колебания – вибрации, регистрируя которые можно осуществлять перехват акустической (речевой) информации.

Для перехвата акустических колебаний по виброакустическим техническим каналам утечки используются контактные микрофоны (стетоскопы).

Перехват акустических (речевых) сигналов электронными стетоскопами



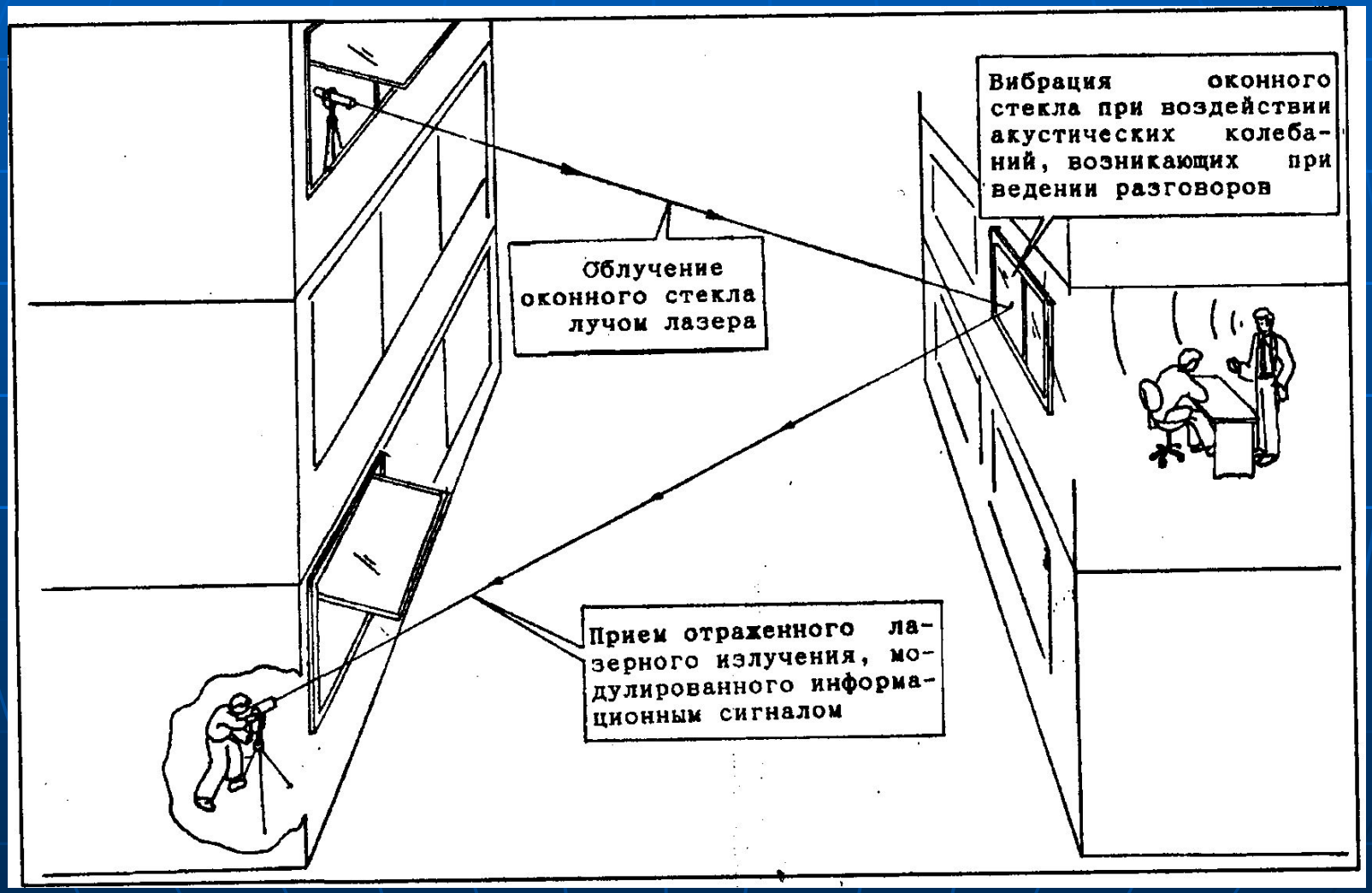
Перехват акустических сигналов электронными стетоскопами, комплексированными с устройствами передачи информации по радиоканалу (радиостетоскопами)



Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т.д.).

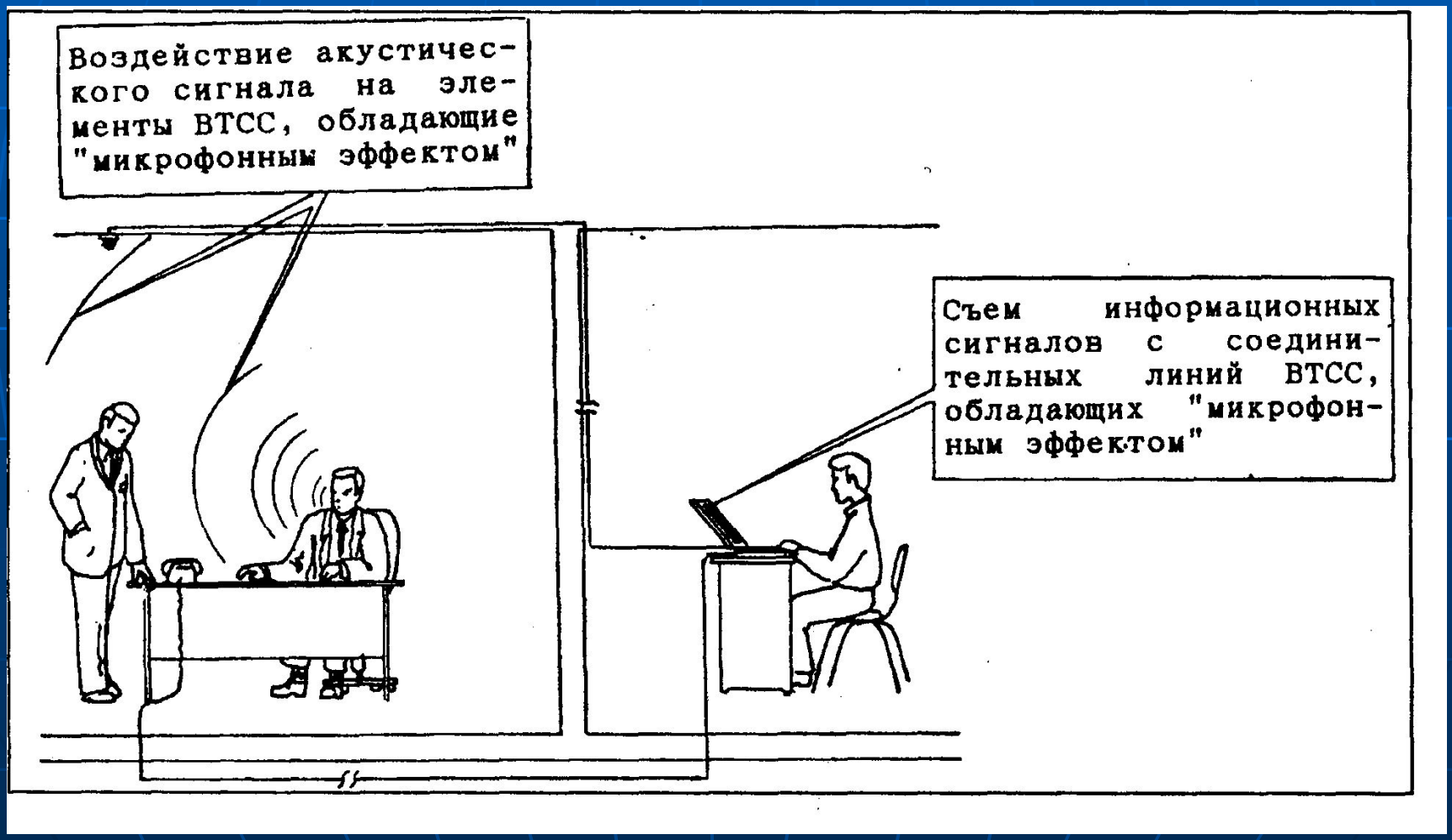
Для перехвата акустической (речевой) информации по данному каналу используются лазерные системы акустической разведки (ЛСАР), которые иногда еще называются «лазерными микрофонами»

Перехват акустических (речевых) сигналов путем лазерного зондирования оконных стекол

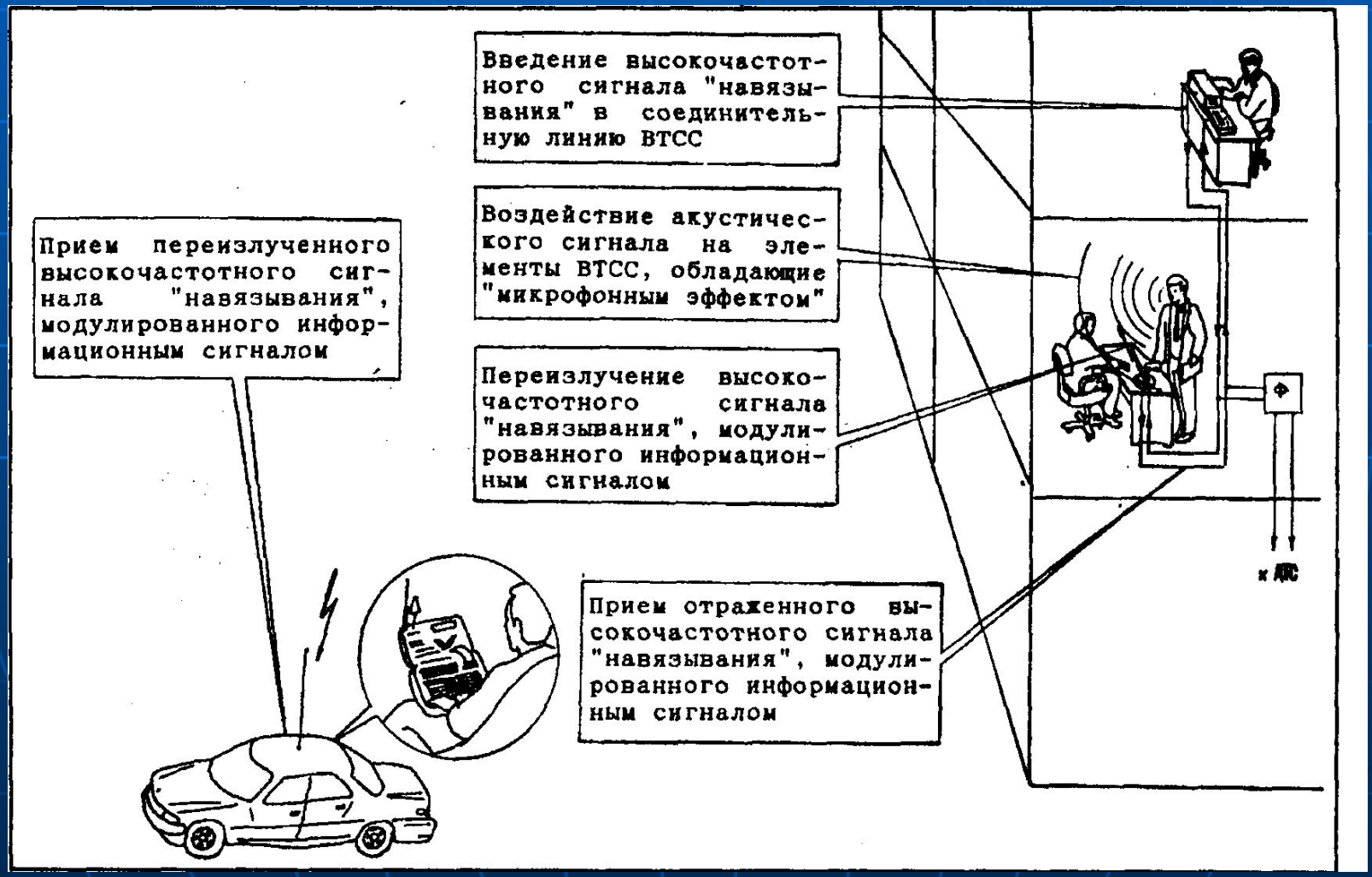


Акустоэлектрические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС, обладающих "микрофонным эффектом", а также путем "высокочастотного навязывания"

Перехват акустических (речевых) сигналов через ВТСС, обладающие "микрофонным эффектом"



Перехват акустических сигналов через ВТСС путем "высокочастотного навязывания"



Параметрические каналы утечки речевой информации

При воздействии речевого сигнала на электрические элементы ОТСС и ВТСС изменяется (незначительно) взаимное расположение элементов схем, что может привести к **изменениям параметров излучаемого ими высокочастотного сигнала**, например, к модуляции его информационным сигналом.

Поэтому этот канал утечки информации называется параметрическим.

Видовая (оптическая информация) – информация, получаемая техническими средствами перехвата в виде изображений объектов или документов.

Способы получения видовой информации :

- *визуальное наблюдение за объектом;*

- *фото- и видеосъемка объекта;*

- *съемка (снятие копий) документов.*

Технически средства получения видовой информации :

- ***монокуляры;***
- ***бинокли;***
- ***телескопы ;***
- ***телевизионные камеры;***
- ***фотоаппараты;***
- ***видеокамеры;***
- ***тепловизоры;***
- ***приборы ночного видения;***
- ***средства для изготовления копий документов.***

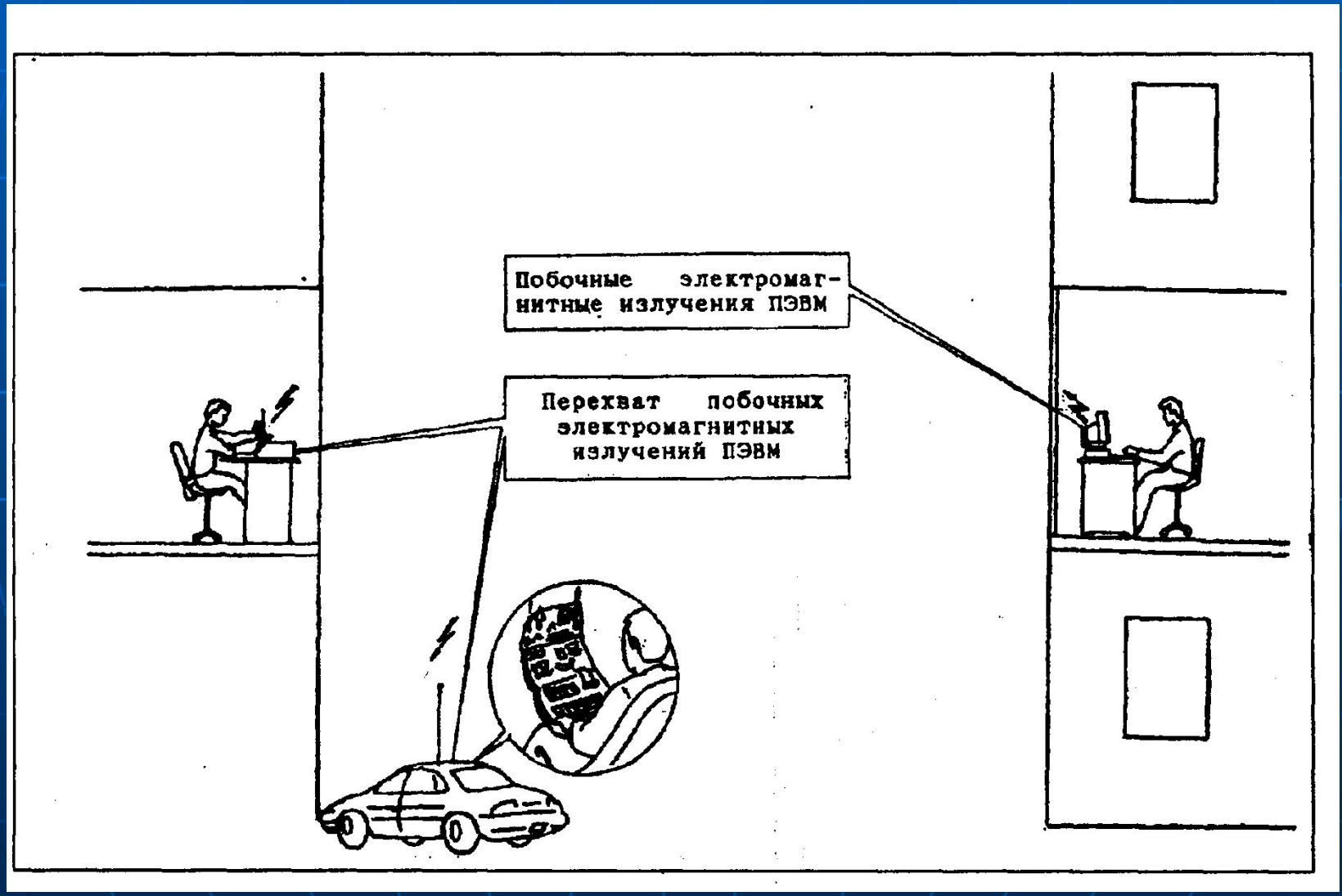
Технические каналы утечки информации, обрабатываемой техническими средствами:

- ***электромагнитные;***
- ***электрические;***
- ***параметрические.***

В ОТСС носителем информации является электрический ток, параметры которого изменяются по закону информационного сигнала.

При прохождении электрического тока по токоведущим элементам ОТСС вокруг них возникает электрическое и магнитное (электромагнитное) поле, модулированное по закону изменения информационного сигнала и которое можно перехватить.

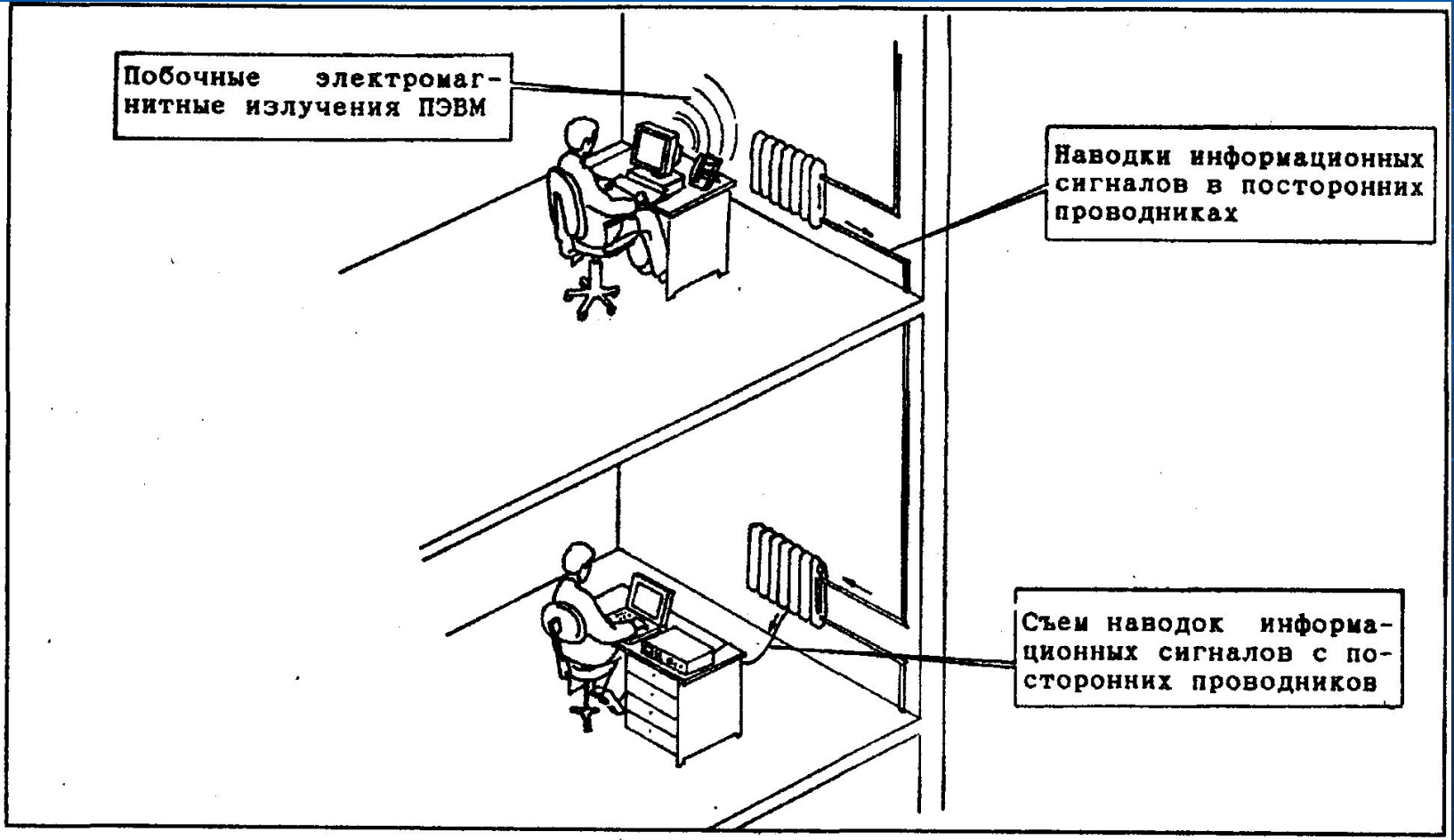
Перехват побочных электромагнитных излучений



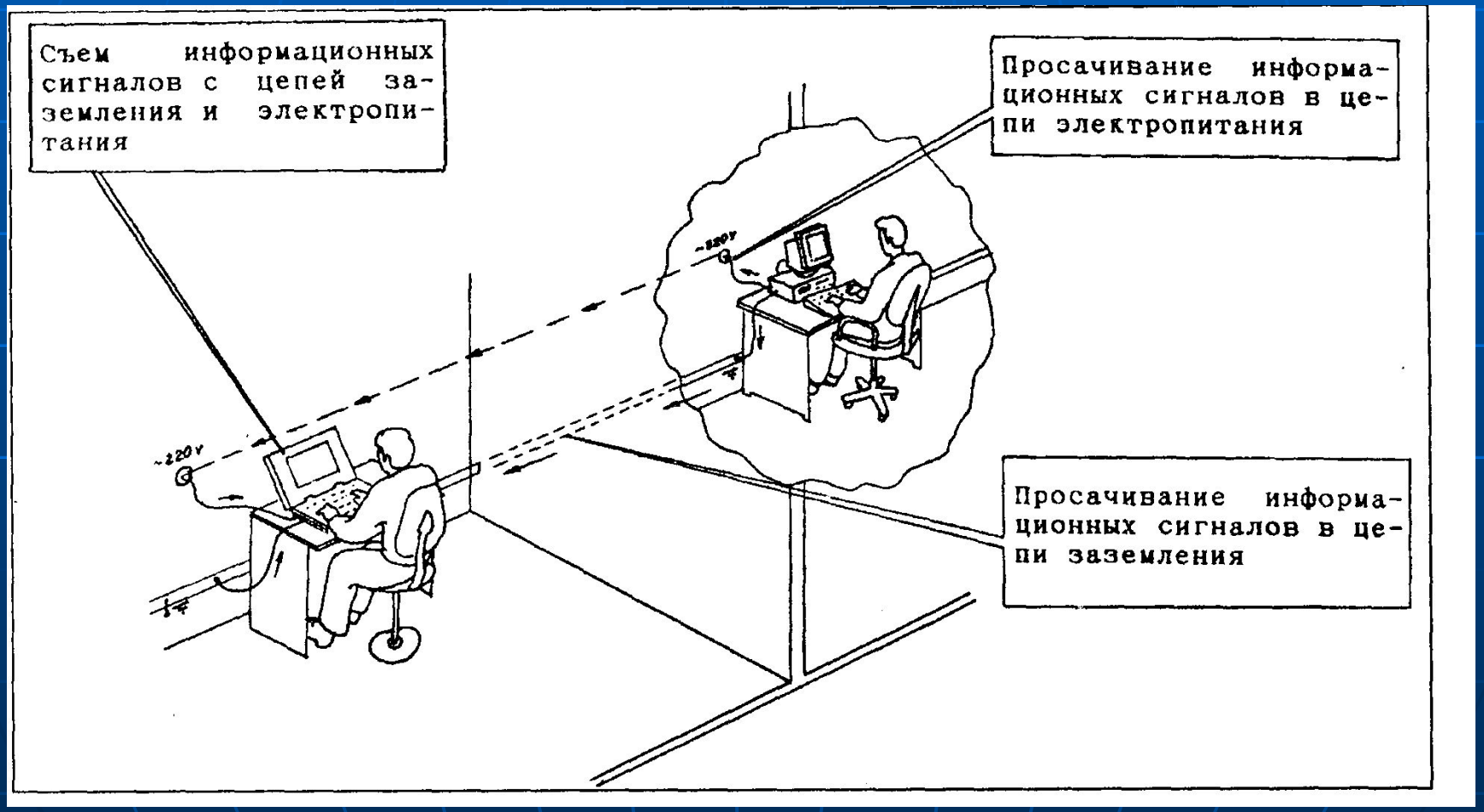
Причинами возникновения электрических каналов утечки информации могут быть:

- наводки электромагнитных излучений ОТСС на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;
- просачивание информационных сигналов в цепи электропитания и зацемления ОТСС;
- перехват информации с установленных в технические средства аппаратных закладок.

Съем наводок информационных сигналов с соединительных линий ВТСС и посторонних проводников



Съем информационных сигналов с цепей заземления и электропитания



Параметрический канал утечки информации

При взаимодействии облучающего электромагнитного поля с элементами технических средств происходит его переизлучение, при этом параметры переизлученного сигнала в ряде случаев модулируются сигналом информационным.

Технические каналы перехвата передаваемой информации :

- *электромагнитные;*
- *электрические;*
- *индукционные.*

Высокочастотные *электромагнитные* излучения передатчиков средств связи могут перехватываться портативными средствами радиоразведки.

Данный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Перехват информации, передаваемой по каналам радиосвязи спутниковым линиям связи

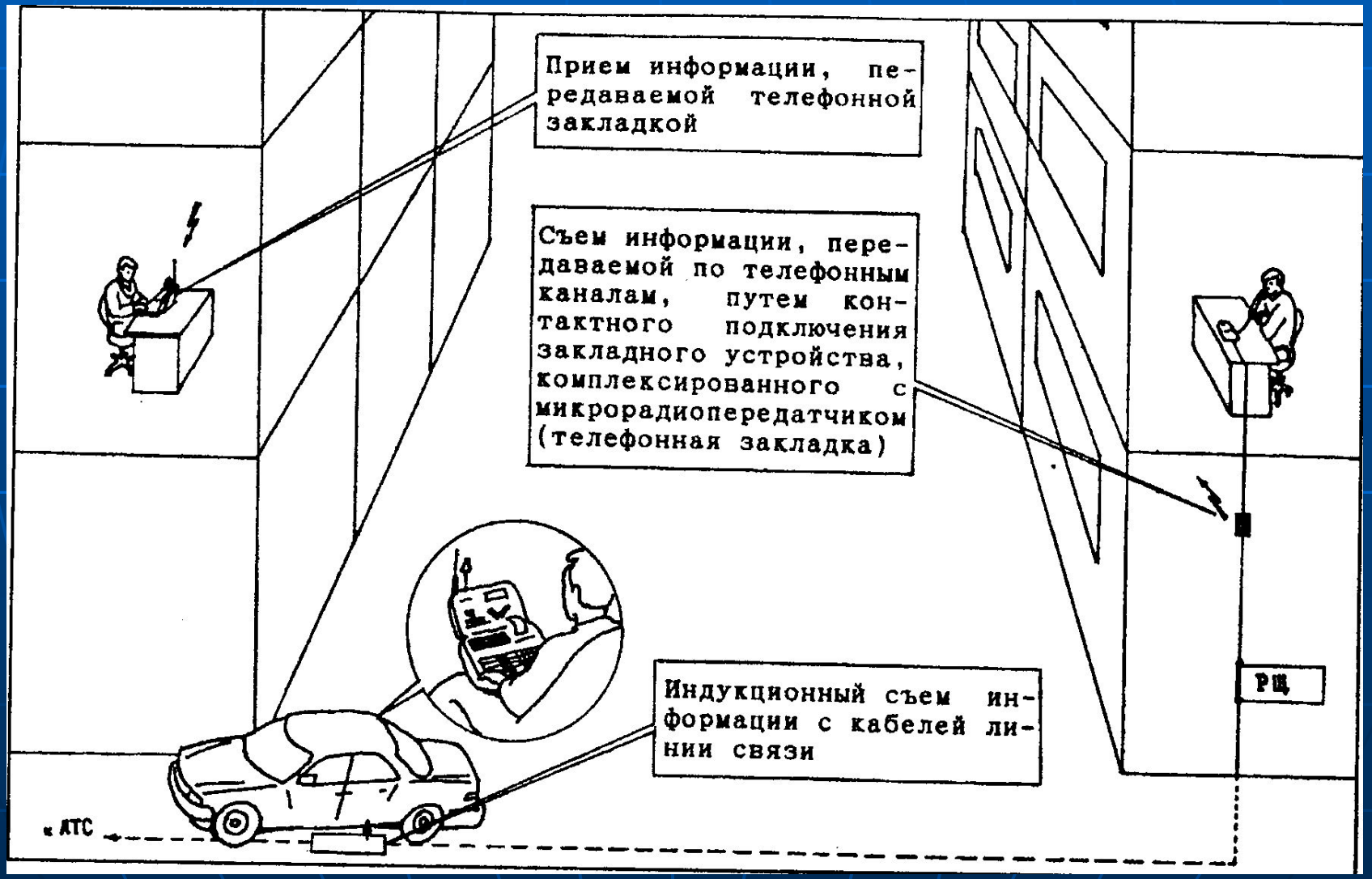
Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры разведки к кабельным линиям связи.

Самый простой способ - это непосредственное параллельное подключение к линии связи.

Спецслужбы наиболее часто используют индуктивный канал перехвата информации, не требующий контактного подключения к каналам связи.

В индуктивном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов.

Съем информации с проводных (кабельных) линий связи



3. Защита информации от утечки по техническим каналам

Защита информации от утечки по техническим каналам в общем плане сводится к следующим действиям:

1. Своевременное определение возможных каналов утечки информации.
2. Определение энергетических характеристик канала утечки информации на границе контролируемой зоны.
3. Оценка возможности контроля каналов утечки со стороны злоумышленников.
4. Исключение или ослабление энергетики каналов утечки.

Защита информации от утечки по техническим каналам достигается:

- *проектно-архитектурными решениями;*
- *организационными мероприятиями;*
- *техническими мероприятиями;*
- *поисковыми мероприятиями (выявление закладных устройств).*

Организационные мероприятия – это мероприятия по защите информации, проведение которых не требует применения специально разработанных технических средств.

К основным организационным и режимным мероприятиям относятся:

- привлечение к проведению работ по защите информации организаций, имеющих лицензию на деятельность в области защиты информации;
- категорирование и аттестация объектов информатизации и выделенных помещений по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

К основным организационным и режимным мероприятиям относятся:

- использование на объекте сертифицированных технических средств обработки и хранения информации, а также вспомогательных технических средств и средств связи;
- установление контролируемой зоны вокруг объекта;
- организация контроля и ограничение доступа на объекты ОТСС и в выделенные помещения

К основным организационным и режимным мероприятиям относятся:

- привлечение к работам по строительству, реконструкции объектов ОТСС, монтажу аппаратуры организаций, имеющих лицензию на деятельность в области защиты информации по соответствующим пунктам;

- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

К основным организационным и режимным мероприятиям относятся:

- **отключение на период закрытых мероприятий технических средств**, имеющих элементы, выполняющие роль электроакустических преобразователей, **от линий связи**;
- и т.д.

***Технические мероприятия** – это мероприятия по защите информации, предусматривающие применение специальных технических средств, а также реализацию технических решений.*

Направлены на закрытие каналов утечки информации путем ослабления уровня информационных сигналов или уменьшением отношения сигнал/шум в местах возможного размещения портативных средств разведки или их датчиков.

Проводятся с использованием

- **активных средств;**
- **пассивных средств.**

Основные технические мероприятия по защите информации:

- *применение пассивных технических средств;*
- *применение активных технических средств;*
- *применение поисковых технических средств.*

Технические мероприятия с использованием пассивных средств :

- *контроль и ограничение доступа на объекты ОТСС и в выделенные помещения;*
- *локализация излучений;*
- *развязывание информационных сигналов.*

Технические мероприятия с использованием активных средств :

- *пространственное зашумление;*
- *линейное зашумление ;*
- *уничтожение закладных устройств.*

Защита информации, обрабатываемой техническими средствами

Пассивные методы защиты направлены на:

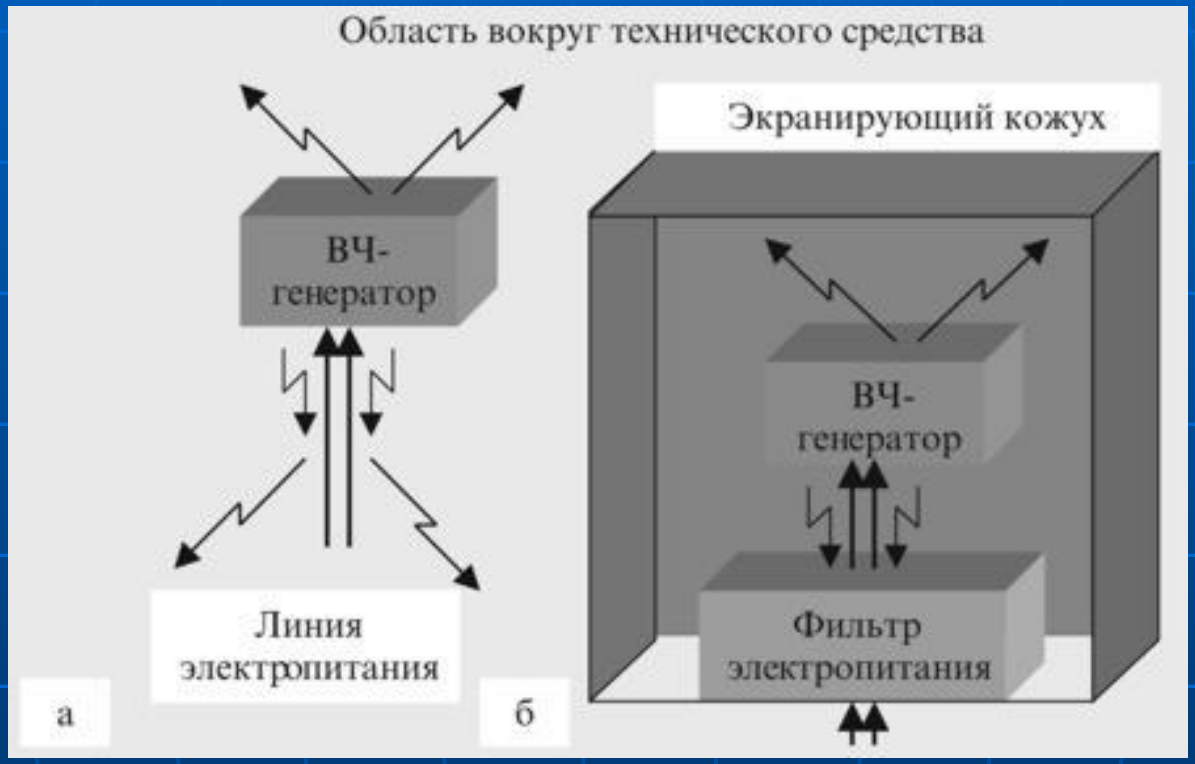
- ослабление побочных электромагнитных излучений ОТСС на границе контролируемой зоны (путем экранирования);
- ослабление наводок побочных электромагнитных излучений ОТСС в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны (путем заземления);

Защита информации, обрабатываемой техническими средствами

Пассивные методы защиты направлены на:

- **исключение (ослабление) просачивания информационных сигналов ОТСС в цепи электропитания, выходящие за пределы контролируемой зоны (путем фильтрации).**

Экранирование устройств



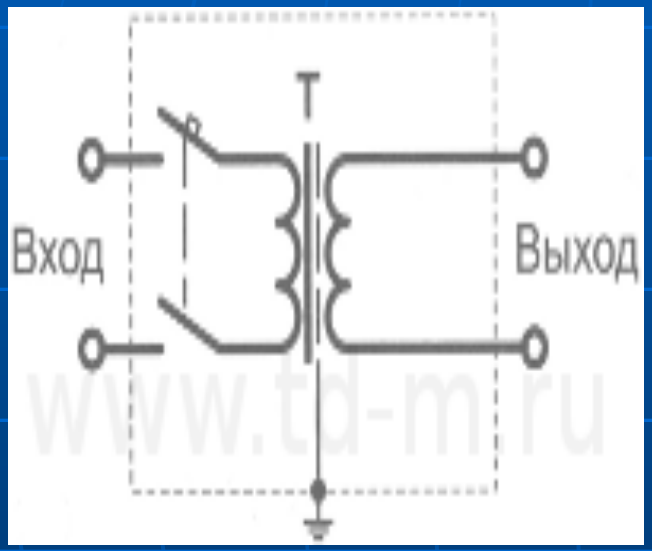
Электромагнитное экранирование основано на замыкании экраном, обладающим высокой электропроводностью и (или) магнитопроводностью электрического и магнитного полей соответственно.

Заземление

Заземление – это соединение электрической сети или оборудования с заземляющим устройством.

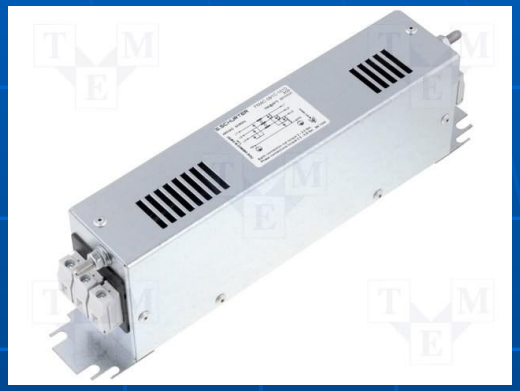
Заземляющее устройство состоит из заземлителя и заземляющего проводника, соединяющего заземляемую точку с заземлителем.

Разделительные трансформаторы



Разделительные трансформаторы – это специальные трансформаторы, обеспечивающие развязку первичной и вторичной цепей по сигналам наводки. Таким образом, во вторичную цепь трансформатора не проникают наводки, появляющиеся в цепи первичной обмотки.

Помехоподавляющие фильтры



Помехоподавляющие фильтры предназначены для подавления сигналов с частотами, лежащими за пределами рабочей полосы частот.

Различают два типа фильтров:

- **фильтры, предназначенные для сети питания переменным током частотой 50Гц;**
- **фильтры, предназначенные для установки в цепи ВТСС.**

Защита информации, обрабатываемой техническими средствами

Активные методы защиты направлены на:

- **создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны (путем пространственного зашумления);**

- **создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС с целью уменьшения отношения сигнал/шум на границе (путем линейного зашумления).**

Требования к системе пространственного зашумления:

- система должна создавать электромагнитные помехи в диапазоне частот возможных побочных излучений ОТСС;

- создаваемые помехи не должны иметь регулярной структуры (поскольку за счет цифровой фильтрации любой шумовой сигнал, имеющий регулярную структуру, может быть исключен из общего сигнала);

Требования к системе пространственного зашумления:

- система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией (поэтому выбору антенн для генераторов помех уделяется особое внимание);
- на границе контролируемой зоны уровень помех, создаваемых системой пространственного зашумления, не должен превышать требуемых норм.

Генераторы «белого» шума

Излучают широкополосный шумовой сигнал, существенно превышающий уровни побочных электромагнитных излучений.

Данные генераторы могут применяться для защиты широкого класса технических средств:

- **электронно-вычислительной техники;**
- **систем звукоусиления и звукового сопровождения;**
- **систем внутреннего телевидения и т.д.**

Метод синфазной помехи

В основном применяется для защиты ЭВМ. В качестве помехового сигнала в этом случае используются импульсы случайной амплитуды, синхронизированные с импульсами компьютера. В результате система зашумления генерирует «имитационную помеху», по спектральному составу соответствующую скрываемому сигналу, но превышающую его в несколько раз по амплитуде. Поскольку импульсы имеют случайную амплитуду, то выделить информационную составляющую сигнала не представляется возможным.

Системы линейного зашумления применяются для маскировки наведенных сигналов в посторонних проводниках и соединительных линиях, выходящих за пределы контролируемой зоны.

Наиболее часто применяются системы зашумления линий электропитания.

Защита видовой информации

- **располагать объекты** защиты так, **чтобы исключить отражение света** в стороны возможного расположения злоумышленника (пространственные ограждения);
- **уменьшить отражательные свойства** объекта защиты;
- **уменьшить освещенность объекта** защиты (энергетические ограничения);
- **использовать средства преграждения или** значительного **ослабления отраженного света**: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;

Защита видовой информации

- применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;
- использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;
- осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона;
- применять маскирующие средства сокрытия объектов в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

Защита речевой информации

Пассивные методы направлены на:

- **ослабление акустических сигналов на границе контролируемой зоны;**
- **ослабление информационных электрических сигналов в соединительных линиях ВТСС, обладающих микрофонным эффектом;**
- **ослабление сигналов высокочастотного навязывания во ВТСС, обладающих микрофонным эффектом;**
- **обнаружение излучений акустических закладок и диктофонов;**
- **обнаружение несанкционированных подключений к телефонным линиям связи.**

Ослабление акустических (речевых) сигналов осуществляется путем **звукоизоляции** помещений.

Звукоизоляция помещений **обеспечивается** с помощью **архитектурных и инженерных решений**, а также применением специальных **строительных и отделочных материалов**.

Защита речевой информации

Активные методы направлены на:

- **создание маскирующих акустических и вибрационных помех** с целью уменьшения отношения сигнал/шум на границе контролируемой зоны;
- **создание маскирующих электромагнитных помех в соединительных линиях ВТСС**, обладающих микрофонным эффектом;
- **электромагнитное подавление диктофонов**;
- **ультразвуковое подавление диктофонов**;
- создание маскирующих электромагнитных помех в линиях электропитания ВТСС, обладающих микрофонным эффектом;

Защита речевой информации

Активные методы направлены на:

- создание прицельных радиопомех акустическим и телефонным радиозакладкам с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;

- подавление средств несанкционированного подключения к телефонным линиям;

- уничтожение (вывод из строя) средств несанкционированного подключения к телефонным линиям.

Системы акустического зашумления:

- *генераторы белого шума;*
- *генераторы «речеподобных» помех;*
- *ультразвуковые генераторы;*
- *системы виброакустической маскировки.*

При использовании генераторов белого шума по периметру помещения располагаются шумящие колонки.

Данный метод сейчас мало используется, ввиду дискомфорта для находящихся в помещении людей.

Речеподобные помехи формируются путем наложения определенного количества речевых сигналов.

«Речевой хор» - помеха формируется путем смешения фрагментов речи нескольких человек (дикторов).

Фонемный клонер – помеха формируется из скрываемого сигнала с помощью синтезатора речеподобных помех .

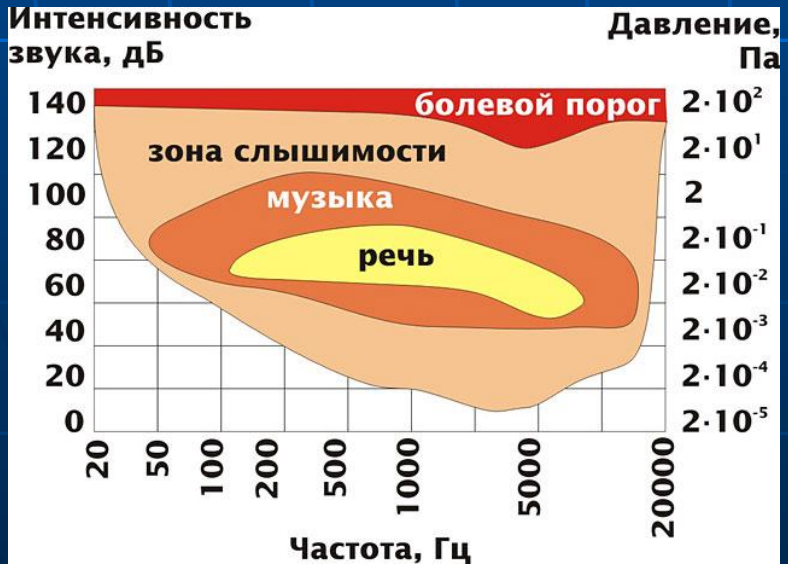
Этапы формирования речевых помеховых сигналов:

-**из записи голоса диктора**(ов) путем клонирования основных фонемных составляющих их речи **синтезируется "псевдоречь"**, представляющая некоторую последовательность сигналов;

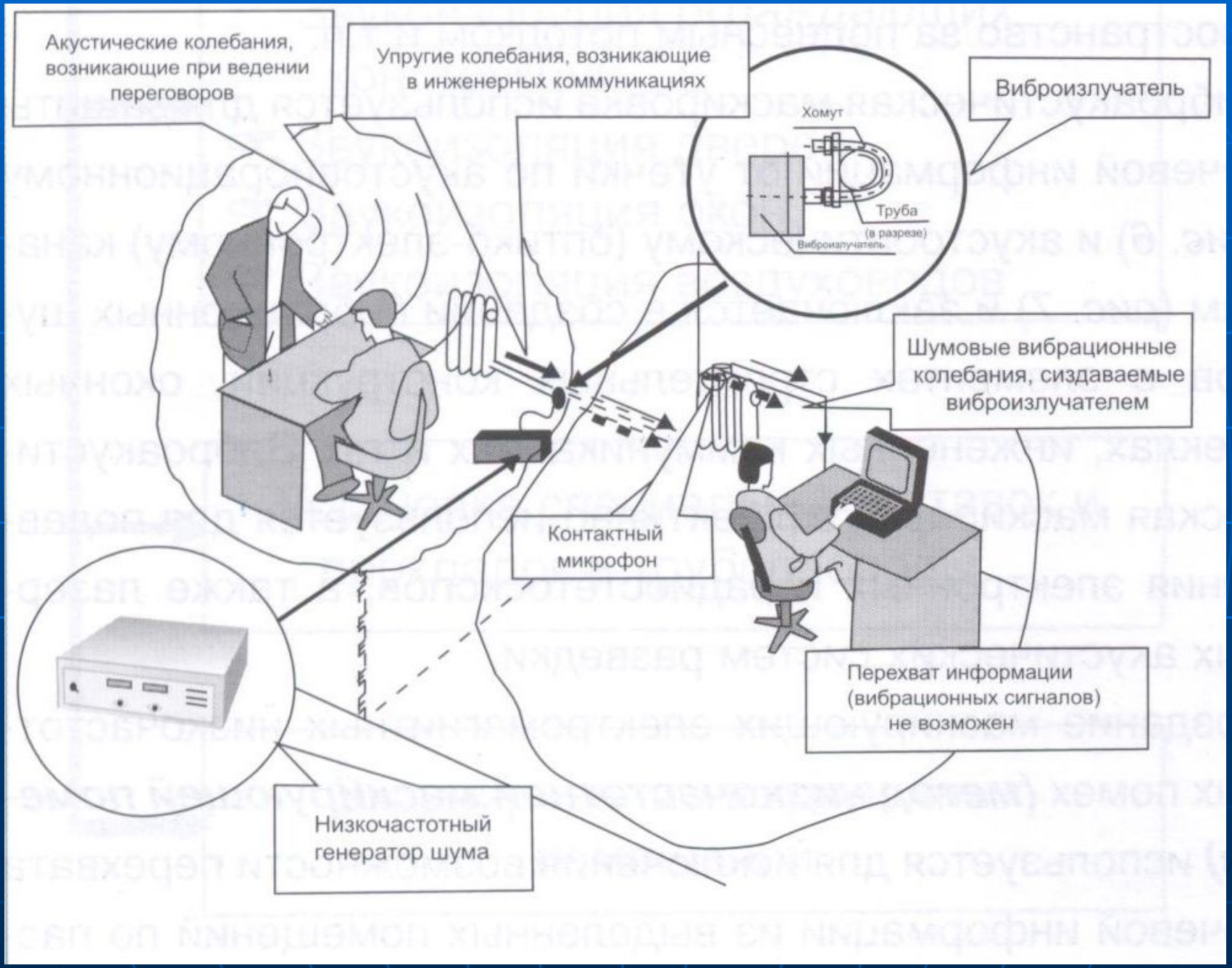
-**синтезатор помехи**, в памяти которого содержится "псевдоречь", по случайному закону **берет из нее случайные куски**, которые и поступают на вход тракта помехового канала.

Ультразвуковые генераторы излучают ультразвуковые **колебания на двух частотах** (более 22кГц), которые не воспринимаются органами слуха человека.

При одновременном **воздействии на микрофон** звукового сигнала и двух мощных **сигналов** ультразвуковой частоты **возникает интерференционный процесс и** разностная частота **подавляет звуковой сигнал**.



При виброакустической маскировке формирования акустических помех применяются специальные генераторы, к выходам которых подключены вибрационные излучатели, установленные на окнах, стенах и т.д.


Акустические колебания, возникающие при ведении переговоров
Упругие колебания, возникающие в инженерных коммуникациях
Виброизлучатель
Хомут
Труба
(в разрезе)
Виброизлучатель
Шумовые вибрационные колебания, сиздаваемые виброизлучателем
Контактный микрофон
Перехват информации (вибрационных сигналов) не возможен
Низкочастотный генератор шума

Подавители сигналов **– группа приборов, предназначенная для подавления сигналов большинства стандартов:**

GSM 900 МГц;
GSM 1800 Мгц;
CDMA 800 МГц;
GPS 1500 МГц;
3G 2100 МГЦ;
Wi-Fi 2400 МГц.

4. Специальные проверки объектов информатизации.

Специальное исследование **(объекта защиты информации)** ***- это исследование, проводимое в целях выявления каналов утечки защищаемой информации и оценки соответствия защиты информации на объекте защиты требованиям нормативных и правовых актов в области защиты информации.***

Специальная проверка - проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

Специальные проверки

специальные проверки технических средств

специальные обследования помещений

Порядок проведения специальной проверки определяется Правительством РФ и проводится соответствующими органами ФСБ России или организациями, имеющими необходимые лицензии

Специальная проверка технических средств (ТС) — это комплекс мероприятий по поиску электронных устройств съема информации (закладных устройств), возможно внедренных в ТС.

Специальным проверкам подвергаются ТС иностранного производства, а также ТС отечественного производства, содержащие комплектующие иностранного производства, предназначенные:

— для обработки сведений, составляющих государственную тайну;

— для размещения в защищаемых помещениях;

— для обработки информации с ограниченным доступом.

Специальное обследование помещений –

это комплекс технических мероприятий, проводимых с использованием специализированных технических средств, в целях выявления возможно внедренных электронных средств съема информации (закладных устройств) в ограждающих конструкциях, мебели и предметах интерьера защищаемого помещения.

Специальное обследование помещений проводится:

— периодически (в соответствии с заранее разработанным планом-графиком);
— после проведения в помещениях каких-либо работ (ремонта, монтажа оборудования, изменения интерьера и т. д.);
— после неконтролируемого посещения посторонними лицами;
— во всех случаях, когда возникает подозрение в утечке информации через возможно внедренные средства несанкционированного съема информации.

Поисковые мероприятия:

Первый уровень — в результате проверки могут быть обнаружены активные радиоизлучающие изделия, установленные непосредственно в проверяемом или смежных с ним помещениях (радиомикрофоны с автономным источником питания, телефонные радиопередатчики).

Поисковые мероприятия:

Второй уровень — могут быть обнаружены все устройства первого уровня плюс сетевые передатчики, использующие в качестве канала передачи сеть питания 220В, 50Гц.

Поисковые мероприятия:

Третий уровень — могут быть выявлены все изделия второго уровня плюс все типы кабельных микрофонных систем, а также оргтехника, работающая в режиме передачи за границы зоны охраны сигнала, содержащего полезную информацию.

Поисковые мероприятия:

Четвертый уровень — могут быть выявлены все типы заносных и закладных электронных устройств перехвата информации и естественные каналы утечки информации.

Обычно в качестве поисковой техники используют :

- *нелинейные локаторы;*
- *индикаторы поля;*
- *сканирующие радиоприемники;*
- *анализаторы спектра.*

Нелинейные локаторы способны обнаруживать и определять местоположение любых полупроводниковых электронных устройств, независимо от того функционируют они в данный момент или нет.

Дальность обнаружения составляет от десятков сантиметров до нескольких метров.

Индикаторы поля **выявляют практически все виды радиосигналов, включая широкополосные шумоподобные сигналы, сигналы с псевдослучайной скачкообразной перестройкой несущей частоты и т.д.**

К их недостаткам относится низкая чувствительность, в результате чего они обнаруживают сигналы закладок при расстояниях до них не более 1-2м.

Анализаторы спектра **позволяют определить амплитуду и частоту спектральных компонент, входящих в состав анализируемых процессов.**

Основное предназначение данного типа приборов заключается в том, что они помогают определить к какому типу излучения относится детектированный сигнал.

Сканирующие приемники функционально аналогичны индикаторам поля, но имеют большую чувствительность в широком диапазоне частот и позволяют непосредственно определить частоты, на которых работают радиозакладки.

Многофункциональный поисковый прибор ST 031 "Пиранья" включает в себя

- высокочастотный детектор-частомер;
- сканирущий анализатор проводных линий;
- детектор ИК-излучений;
- детектор низкочастотных магнитных полей;
- дифференциальный низкочастотный усилитель;
- виброакустический приемник;
- акустический приемник.

Вспомогательные поисковые приборы:

- *обнаружители пустот;*
- *металлоискатели;*
- *рентгеновские установки; тепловизоры.*

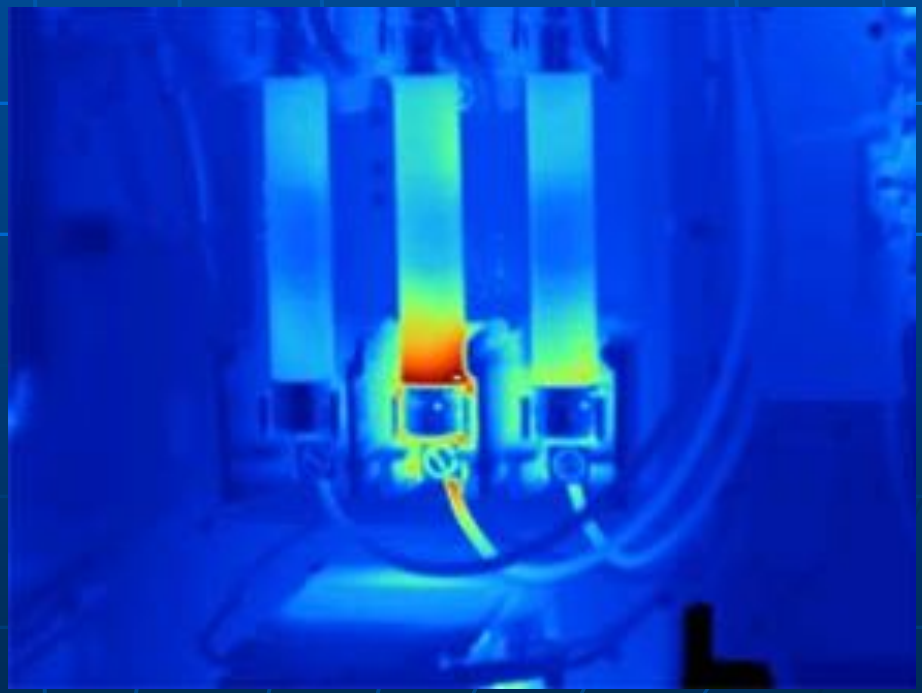
Обнаружители пустот **позволяют обнаруживать возможные места установки закладных устройств в пустотах стен или других деревянных или кирпичных конструкциях.**

Металлоискатели (металлодетекторы) **реагируют на наличие в зоне поиска электропроводных материалов, прежде всего металлов, и позволяют обнаруживать корпуса или иные металлические элементы закладок.**

Переносные рентгеновские установки **применяются для просвечивания предметов, назначение которых не удается выявить без их разборки прежде всего тогда, когда она невозможна без разрушения найденного предмета.**

Тепловизоры - это теплотехнические приборы, позволяющие получать бесконтактным способом инфракрасные изображения.

Такие изображения в цвете показывают поверхностную температуру объекта, позволяя детектировать "ненормально" горячие области.



Выделенное помещение (ВП) –

специальное помещение, предназначенное для проведения собраний, совещаний, бесед и других мероприятий речевого характера по секретным или конфиденциальным вопросам.

Аттестат выделенного помещения –

документ, выдаваемый органом по аттестации (сертификации) или другим специально уполномоченным органом, подтверждающий наличие необходимых условий, обеспечивающих надежную акустическую защищенность выделенного помещения в соответствии с установленными нормами и правилами.

Аттестат объекта защиты –

документ, выдаваемый органом по сертификации или другим специально уполномоченным органом подтверждающий наличие на объекте защиты необходимых и достаточных условий для выполнения установленных требований и норм эффективности защиты информации.

Переаттестация объекта информатизации производится в случае:

- **изменение категории объекта;**
- **изменение расположения ОТСС или ВТСС;**
- **замена ОТСС или ВТСС на другие;**
- **замена технических средств защиты информации;**
- **изменения в монтаже и прокладке слаботочных и соловых кабельных линии;**
- **несанкционированное вскрытие опечатанных корпусов ОТСС или ВТСС;**
- **производство ремонтно-строительных работ в выделенных помещениях и пр.**