Основы кибербезопасности

Лекция 4/1
«Понятие об источниках и каналах утечки информации; основы технической защиты информации»

Учебные вопросы:

. Понятие и структура технического канала утечки информации.

2. Классификация технических каналов утечки информации.

3. Технические каналы утечки информации. Модель и способы утечки.

4. Основные меры защиты информации от утечки по техническим каналам.

Под ***утечкой информации по техническим каналам*** понимается *неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации*.

Техническая защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056-2005: утв. Приказом Ростехрегулирования от 29 декабря 2005 г. № 479-ст . Введ. 2006-06-01.

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.*

См.: Национальный стандарт Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст)

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

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

См.: Национальный стандарт РФ ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст)

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.*

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

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

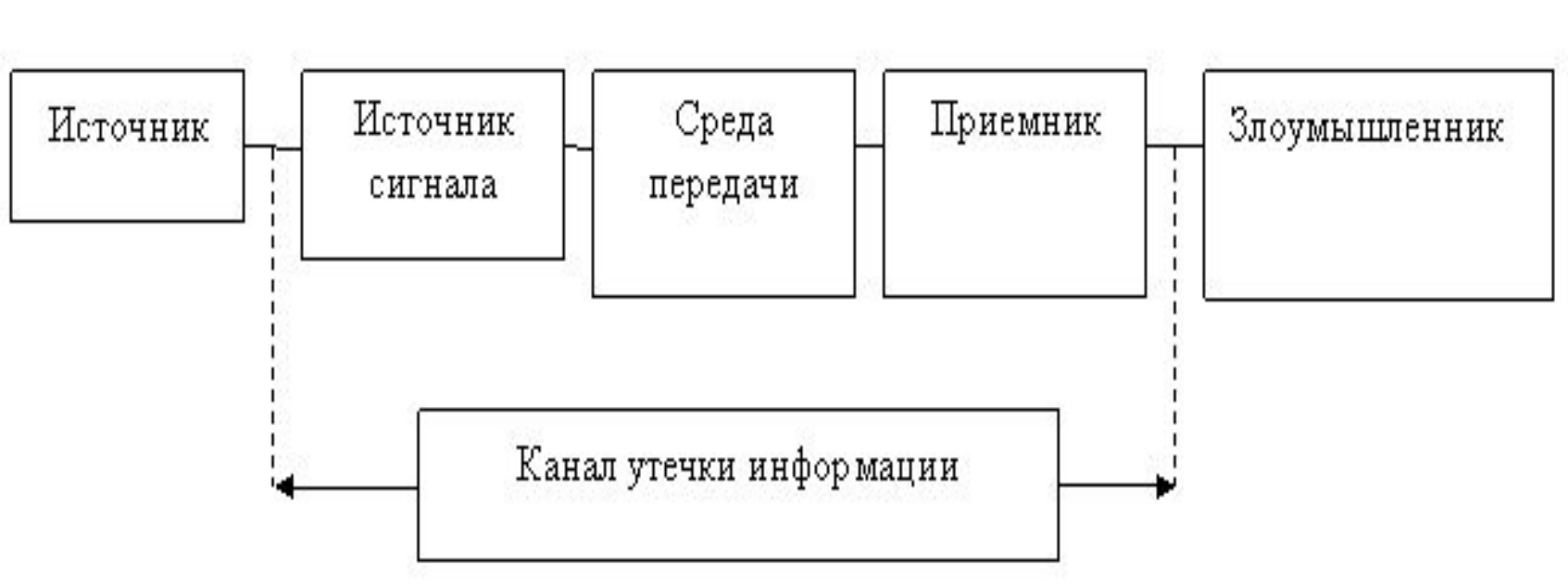
Технические каналы утечки информации *подразумевают использование специальных технических средств для несанкционированного доступа к защищаемой информации.*

1. Вопрос
Понятие и структура технического канала утечки информации

Физический путь переноса информации от ее источника к несанкционированному получателю называется каналом утечки.

Канал, несанкционированный перенос информации в котором осуществляется с использованием технических средств, называется

Структура технического канала утечки информации.



Источник сигнала:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн.

Функции передатчика сигнала:

- производит запись информации на носитель;
- усиливает мощность сигнала (носителя с информацией);
- обеспечивает передачу сигнала в среду распространения в заданном секторе пространства.

Параметры среды распространения

- **физические препятствия для субъектов и материальных тел:**
- **мера ослабления сигнала на единицу длины;**
- **частотная характеристика;**
- **вид и мощность помех для сигнала.**

Форма и носители защищаемой информации

Информация может быть представлена в разной форме и на различных физических носителях. Основными формами информации, представляющими интерес с точки зрения защиты, являются три следующие:

1. **Документальная форма**, которая обычно представляет информацию:

- в графическом или буквенно-цифровом виде на бумажном носителе или
- в электронном виде на магнитных, оптических и других носителях.

Особенность документальной информации в том, что она в сжатом виде содержит сведения, подлежащие защите.

2. Речевая форма информации возникает в процессе:

- ведения разговоров,
- при работе систем звукоусиления и звуко-воспроизведения.

Носителем речевой информации являются акустические колебания (механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины).

Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200...300 Гц до 4...6 кГц.

3. Телекоммуникационная форма информации циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче.

Носителем информации при ее обработке техническими средствами являются:

- электрический ток — при передаче по проводным каналам связи,
- электромагнитные волны —при передаче по радио и оптическим каналам.

Объекты защиты информации (или объект ТСПИ)

К числу **основных объектов** защиты информации относятся:

1) **информационные ресурсы** (ИР), содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

2) **основные технические средства и системы** (ОТСС):

- ***средства автоматизированные систем*** (вычислительные комплексы, сети и системы);
- ***средства изготовления и размножения документов***;
- ***аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода***;
- ***системы видеозаписи и видеовоспроизведения;***

3) **вспомогательные технические средства и системы** (ВТСС), размещенные в помещениях, в которых обрабатывается секретная и конфиденциальная информация. К ним относятся ***технические средства*** :

- открытой телефонной и громкоговорящей связи,
- системы пожарной и охранной сигнализации,
- радиотрансляции и часофикации,
- электробытовые приборы и т.д.

Объектом ТСПИ является совокупность ИР, ОТСС, ВТСС, а также помещений, в которых они размещены и где обрабатывается информация ограниченного доступа.

- При обработке информации с помощью ТСПИ возникает побочное электромагнитное излучение (ПЭМИ), перехватив которое становится возможным получение обрабатываемой информации без прямого доступа к устройству пользователя.
- Устройство, осуществляющее прием сигнала ПЭМИ, называется техническим средством разведки - ТСР

- Средой распространения ПЭМИ может быть воздушная среда и случайные антенны (посторонние проводники и соединительные линии ВТСС), выходящие за пределы **контролируемой зоны – КЗ**
- КЗ – территория, на которой исключено появление лиц и транспорта без постоянных и временных пропусков.
- Если ТСР, находясь за пределами КЗ, может перехватить сигнал и возможна расшифровка перехвата, то говорят, что ТСР находится в опасной зоне.

- Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется опасной **зоной 1**.
- Пространство вокруг ТСПИ, в котором возможен перехват ПЭМИ (без случайных антенн) и последующая расшифровка, называется опасной **зоной 2.**

Таким образом, **ТКУИ** это совокупность:

- объекта разведки (в данном случае — объекта атак ТСР),
- физической среды, в которой распространяется информационный сигнал,
- технического средства разведки (ТСР), с помощью которого информация добывается за пределами КЗ:
  - в пределах опасной **зоны 1** (при наличии случайных антенн) или
  - в пределах опасной **зоны 2** (при отсутствии случайных антенн).

2 Вопрос
Классификация технических каналов утечки информации

Оптический

- **Носителем информации в оптическом канале является электромагнитное поле (фотоны). Оптический диапазон подразделяется на:**
- **дальний инфракрасный поддиапазон 100 – 10 мкм (3 – 30 ТГц);**
- **средний и ближний инфракрасный поддиапазон 10 – 0,76 мкм (30 – 400 ТГц);**
- **видимый диапазон (сине-зелёно-красный) 0,76 – 0,4 мкм (400 – 750 ТГц).**

Радиоэлектронный

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала занимает полосу частот от десятков ГГц до звукового.

Он подразделяется на:

- **низкочастотный 10 – 1 км (30 – 300 кГц);**
- **среднечастотный 1 км – 100 м (300 кГц – 3МГц);**
- **высокочастотный 100 – 10 м (3 – 30 МГц);**
- **ультравысокочастотный 10 – 1м (30 – 300 МГц);**
- **и т.д. до сверхвысокочастотного 3 – 30 ГГц (10 – 1 см).**

Акустический

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Здесь различают:

- **инфразвуковой диапазон 1500 – 75 м (1 – 20 Гц);**
- **нижний звуковой 150 – 5 м (1– 300 Гц);**
- **звуковой 5 – 0,2 м (300 – 16000 Гц);**
- **ультразвуковой от 16000 Гц до 4 МГц.**

Материально-вещественный

Утечка информации производится путем несанкционированного распространения вещественных носителей с защищаемой информацией.

В качестве вещественных носителей выступают: черновики документов и использованная копировальная бумага, образцы материалов, детали и т.д..

Информативность канала оценивается ценностью информации, которая передается по каналу.

- информативные
- малоинформативные
- неинформативные

По времени

- постоянные
- периодические
- эпизодические

В постоянном канале утечка информации носит достаточно регулярный характер. К эпизодическим каналам относятся каналы, утечка информации в которых имеет случайный разовый характер.

По структуре каналы утечки информации делят на:

- одноканальные
- составные

ВОПРОС 3. Технические каналы утечки информации. Модель и способы утечки.

- **АКУСТИЧЕСКИЙ (РЕЧЕВОЙ)**
- **РАДИОЭЛЕКТРОННЫЙ и ЭЛЕКТРИЧЕСКИЙ**
- **ОПТИЧЕСКИЙ (ВИДОВОЙ)**
- **МАТЕРИАЛЬНО-ВЕЩЕСТВЕННЫЙ**

Модель и способы утечки по акустическому каналу

- Акустический канал утечки информации состоит из трех составляющих: источник опасного сигнала, физической среды его распространения и технического средства его приема, определяющих физический путь, по которому злоумышленник обеспечивает ее несанкционированное получение.
- **Источником образования** акустического канала утечки информации являются вибрирующие, колеблющиеся тела и механизмы, такие как голосовые связки человека, движущиеся элементы машин, телефонные аппараты, звукоусилительные системы и т.д.
- В зависимости от физической природы возникновения речевых сигналов, среды их распространения и способов перехвата технические каналы утечки речевой информации можно разделить на *акустические, виброакустические, акустоэлектрические, параметрические, и оптико-электронный*.

Акустические каналы утечки речевой информации.

Для перехвата информации по данному каналу используются *направленные микрофоны и миниатюрные высокочувствительные микрофоны*. Последние используются в качестве чувствительного элемента в *портативных диктофонах и акустических закладочных устройствах (акустических закладках)* – устройствах, в которых микрофон конструктивно объединен с миниатюрным передатчиком.

Акустические каналы утечки речевой информации.

Диктофоны представляет собой устройства для записи, или для записи и воспроизведения устной речи с целью ее последующего прослушивания.

Направленные микрофоны применяются в том случае, когда отсутствует возможность проникновения на контролируемый объект или если конфиденциальный разговор происходит вне помещения (например, на улице или на открытой местности).

Акустические каналы утечки речевой информации.

Акустические закладки представляют собой миниатюрные устройства, конструктивно объединяющие чувствительный элемент и передатчик. При перехвате акустической информации, распространяющейся в воздушных и водных средах, используются акустические закладки микрофонного типа. Чувствительным элементом в этих устройствах являются миниатюрные микрофоны, которые преобразуют перехватываемый акустический сигнал в электрический.

Акустическое закладочное устройство микрофонного типа с передачей перехваченной информации по радиоканалу называется *радиозакладкой.*

Устройства перехвата информации по акустическому каналу

а) направленный микрофон

б) радиозакладка, закамуфлированная под коробок спичек

Виброакустические каналы утечки речевой информации

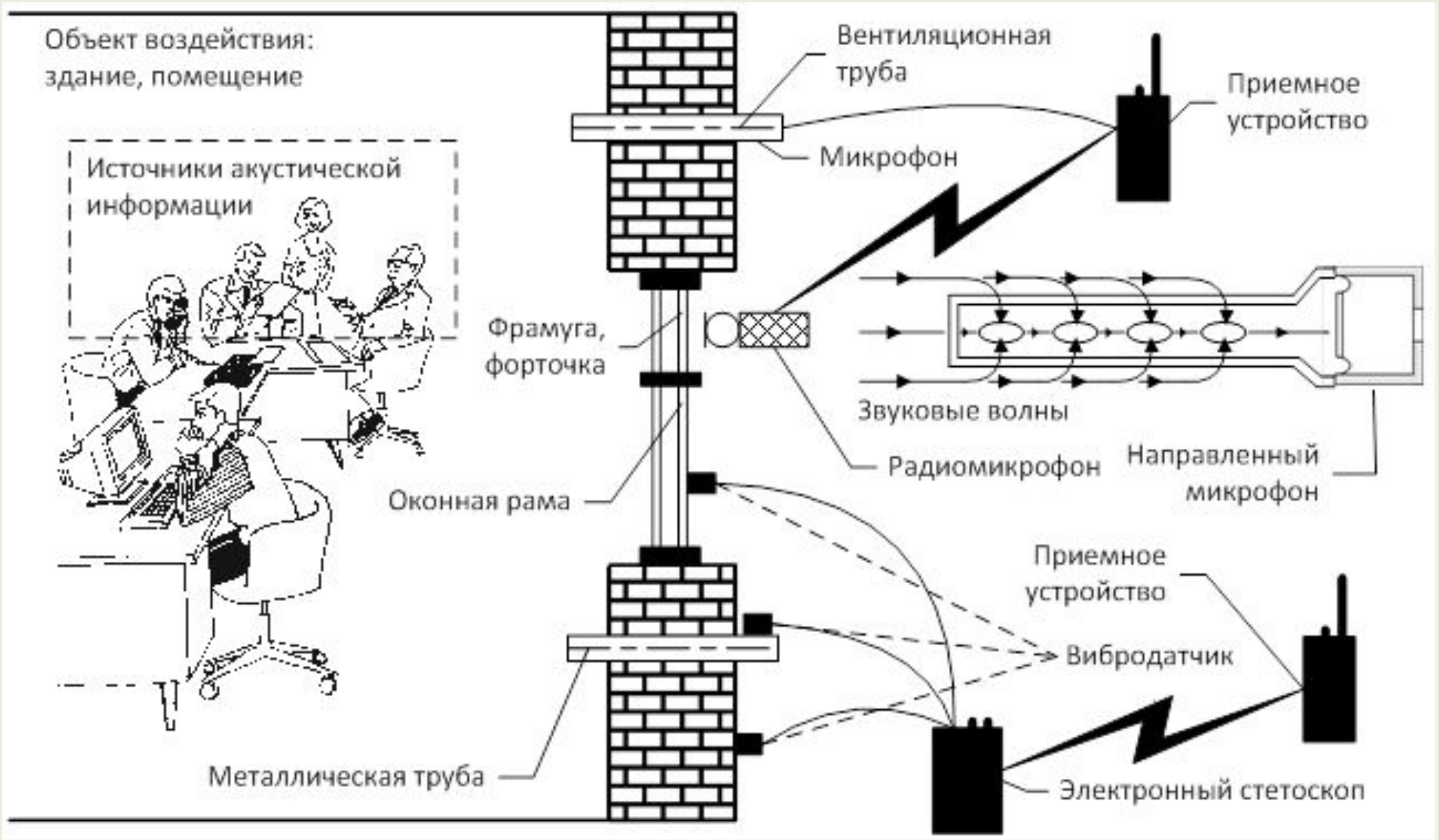
Электронный стетоскоп

Электронные стетоскопы - специальные устройства которые преобразуют акустические колебания в твердых телах в электрические сигналы.

Виброакустические каналы утечки речевой информации

Электронные стетоскопы применяются в том случае, если имеется возможность беспрепятственного проникновения в смежное с контролируемым помещение. В том случае, если возможность беспрепятственного проникновения в смежное помещение отсутствует, вибродатчик оснащается средствами передачи перехваченного акустического сигнала по проводным, радио- и другим возможным каналам передачи информации. На практике для этих целей обычно используется радиоканал, а вибродатчик, оснащенный средствами передачи акустического сигнала по радиоканалу, называется *радиостетоскопом.*

Схема утечки речевой информации по акустическому и виброакустическому каналам



Акустоэлектрические каналы утечки речевой информации

Перехват информации в данных каналах утечки информации осуществляется путем использования устройств, реализующих принцип *высокочастотного навязывания*. Под высокочастотным навязыванием (ВЧ-навязыванием) понимают способ несанкционированного получения речевой информации, основанный на зондировании мощным ВЧ-сигналом заданной области пространства.

Прослушивание помещения через телефон можно осуществить, используя «микрофонный эффект», основанный на том, что детали и узлы телефона (в частности, его вызывная цепь) могут работать как микрофон и наводить в линию достаточно сильный сигнал, который после его усиления пригоден для записи и прослушивания.

Параметрические каналы утечки речевой информации.

Электронные устройства, установленные в помещениях, в процессе работы создают в окружающем пространстве высокочастотные излучения, параметры которых могут меняться в случае воздействия на них какого-либо акустического сигнала, например, ведущимся в помещении разговором (поэтому этот канал утечки информации и называется параметрическим), то есть их модуляции информационным сигналом. Модулированные таким образом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и декодированы с помощью специального оборудования.

Дальность перехвата подобных сигналов, как правило, невелика, но иногда может превышать 100 метров.

Параметрические каналы утечки речевой информации.

Еще одним способом перехвата акустической информации по параметрическому каналу является использование *полуактивных закладных устройств* (или аудиотранспондеров). Работать *аудиотранспондер* начинает только при облучении его мощным высокочастотным зондирующим сигналом, который активизирует устройство. Этот сигнал выделяется приемником аудиотранспондера и модулируется сигналом, поступающим либо непосредственно с микрофона, либо с микрофонного усилителя полуактивного закладного устройства. После чего про модулированный высокочастотный сигнал переизлучается, при этом его частота смещается относительно несущей частоты зондирующего сигнала.

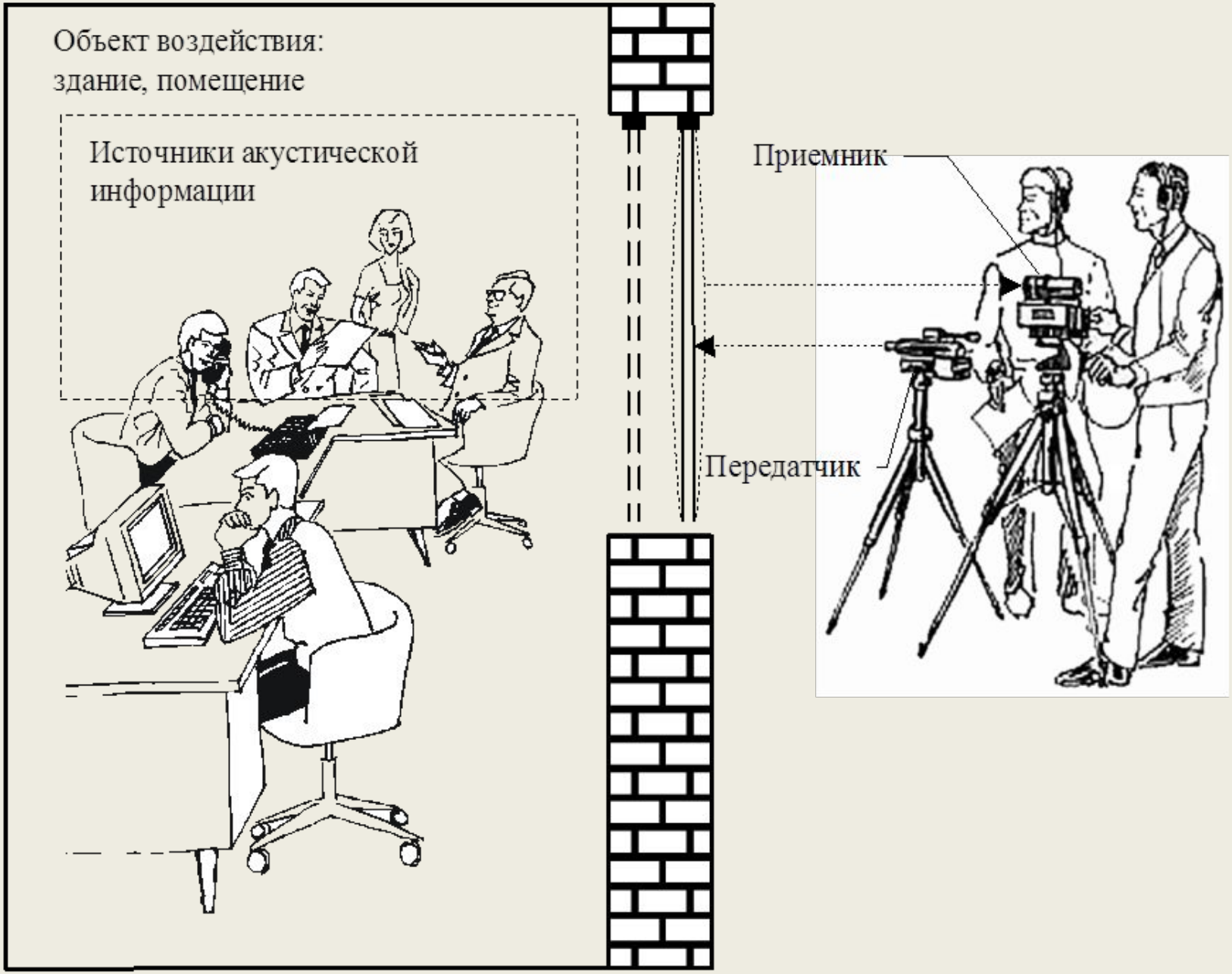
Параметрические каналы утечки речевой информации.

В 1945 году американскому послу в Москве Авереллу Гарриману пионерами «Артека» был подарен деревянный герб Соединенных Штатов из ценных пород дерева. Растроганный посол повесил подарок детишек у себя в кабинете. И лишь через восемь лет американцы узнали, что в гербе было установлено подслушивающее устройство. В гербе находился полый металлический цилиндр без источников питания, торец которого был закрыт тонкой металлической мембраной. Под клювом орла было просверлено отверстие, позволявшее звуковым волнам достигать мембраны. Из соседнего здания в сторону этого подслушивающего устройства, установленного в гербе, направлялось излучение высокой частоты. Звуковые волны, сопровождавшие разговоры в кабинете американского посла, вызывали колебания мембраны, закрывающей металлический цилиндр. В результате изменялась электрическая емкость между этой мембраной и специальным настроечным винтом. Эти изменения приводили к модуляции отраженного излучения указанным звуковым сигналом. В приемном пункте этот сигнал принимался и обрабатывался. Устройство оказалось настолько чувствительным, что была прекрасно слышна не только речь, но и звуки поворота ключа в дверном замке.

Оптико-электронный канал утечки речевой информации

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

Схема утечки информации по оптико-электронному каналу

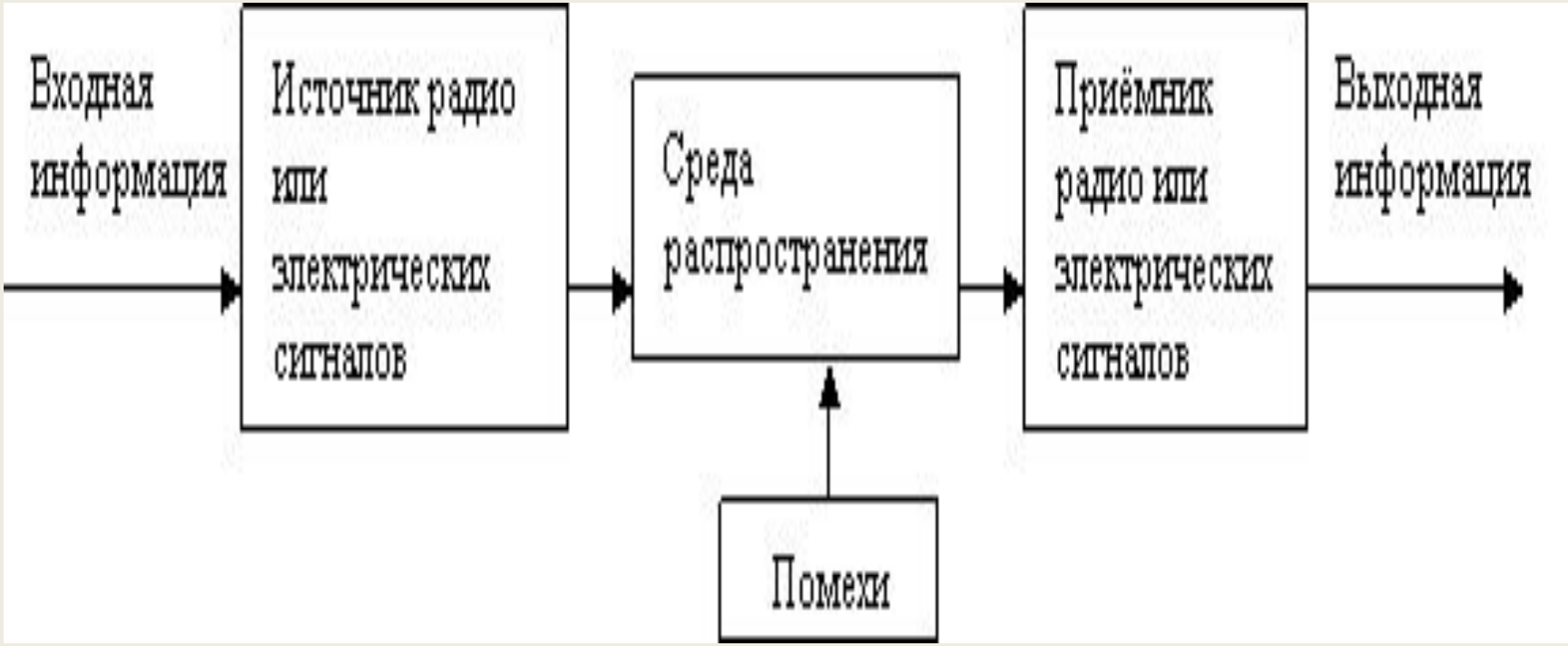


Радиоэлектронные каналы утечки информации

В радиоэлектронном канале передачи носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц.

- Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:
- - независимость функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;
- - высокая достоверность добываемой информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев дезинформации);
- - большой объем добываемой информации; - оперативность получения информации вплоть до реального масштаба времени;
- - скрытность перехвата сигналов и радиотеплового наблюдения.

Структура радиоэлектронного канала утечки информации в общем виде



Электрические ТКУИ, основанные на съеме наводок ПЭМИ:

а) с посторонних проводников;

б) с цепей заземления и линий электропитания;

в) с аппаратных закладок (мини-передатчики, излучение которых модулируется информационным сигналом).

Модель и способы утечки оптической информации

Оптическая информация - информация, получаемая в виде изображений объектов или документов.

Миниатюрные видеокамеры

Модель и способы утечки по материально-вещественным каналам

К материально-вещественному каналу утечки информации относится снятие информации непосредственно с носителя информации.

Основными источниками информации вещественного канала утечки информации являются следующие:

- черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследова тельских и опытно-конструкторских работ, ведущихся в орга низации;
- отходы делопроизводства и издательской деятельности в организации, в том числе использованная копировальная бумага, за
  бракованные листы при оформлении документов и их размножении;
- отходы промышленного производства опытного и серийного выпуска продукции, содержащей защищаемую информацию в газообразном, жидком и твердом виде;
- содержащие защищаемую информацию дискеты и жесткие дис ки ПЭВМ, нечитаемые из-за их физических дефектов и искаже ний загрузочных или других секторов;
- бракованная продукция и ее элементы;

ВОПРОС 4 Основные меры защиты информации от утечки по техническим каналам.

Обеспечение защиты информации от утечки обеспечивается реализацией целого комплекса мер, ключевую роль в котором играют мероприятия организационного и технического характера.

Организационные меры защиты: временные ограничения, территориальные ограничения.

Мероприятия

- определение границ контролируемой зоны;
- привлечение к проведению работ по защите информации организаций, имеющих лицензию на ТЗКИ;
- категорирование и аттестация объектов ОТСС и выделенных для проведения закрытых мероприятий помещений по выполнению требований обеспечения защиты информации;
- использование на объекте сертифицированных ОТСС и ВТСС;
- организация контроля и ограничение доступа к ИС и в защищаемые помещения;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- отключение на период закрытых мероприятий технических средств, имеющих элементы, выполняющие роль электроакустических преобразователей, от линий связи и т.д.

Техническое мероприятие - это мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений.

Технические мероприятия осуществляются с использованием активных и пассивных средств.

Пассивные средства защиты информации ослабляют уровень информативного сигнала, который может перехватить злоумышленник, активные уменьшают отношение сигнал/шум на входе аппаратуры злоумышленника

Пассивные средства

контроль и ограничение доступа к ИС и в выделенные помещения с помощью технических средств и систем;

локализация излучений:

1. экранирование ОТСС и их соединительных линий;
2. заземление ОТСС и экранов их соединительных линий;
3. звукоизоляция выделенных помещений.

развязывание информационных сигналов:

4. установка специальных средств защиты в ВТСС, обладающих "микрофонным эффектом" и имеющих выход за пределы контролируемой зоны;
5. установка специальных диэлектрических вставок в оплетки кабелей электропитания, труб систем отопления, водоснабжения и канализации, имеющих выход за пределы контролируемой зоны;
6. установка автономных или стабилизированных источников электропитания ОТСС;
7. установка устройств гарантированного питания ОТСС (например, мотор-генераторов);
8. установка в цепях электропитания ОТСС, а также в линиях осветительной и розеточной сетей выделенных помещений помехоподавляющих фильтров.

- **Экранирование** - локализация электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами
- **Заземление** состоит из заземлителя и заземляющего проводника, соединяющего заземляемое устройство с заземлителем.
- **Звукоизоляция** локализует источники излучения в замкнутом пространстве с целью снижения до предела отношения сигнал/шум до предела, исключающего или значительно затрудняющего съем акустической информации.

К техническим мероприятиям с использованием активных средств относятся:

- **пространственное зашумление:**
  - **пространственное электромагнитное зашумление с использованием генераторов шума или создание прицельных помех;**
  - **создание акустических и вибрационных помех с использованием генераторов акустического шума;**
  - **подавление диктофонов в режиме записи с использованием подавителей диктофонов.**
- **линейное зашумление:**
  - **линейное зашумление линий электропитания;**
  - **линейное зашумление посторонних проводников и соединительных линий ВТСС, имеющих выход за пределы контролируемой зон.**
- **уничтожение закладных устройств:**
  - **уничтожение закладных устройств, подключенных к линии, с использованием специальных генераторов импульсов (выжигателей "жучков").**

Выявление закладных устройств

Выявление портативных электронных устройств перехвата информации — **закладных устройств** на объектах ТСПИ и в выделенных помещениях осуществляется проведением:

- **специальных обследований** путем их визуального осмотра без применения технических средств,
- **специальных проверок** с использованием пассивных или активных технических средств.

В ходе использования **пассивных средств** осуществляется:

- установка в выделенных помещениях средств и систем обнаружения лазерного облучения (подсветки) оконных стекол;
- установка в выделенных помещениях стационарных обнаружителей диктофонов;
- поиск закладных устройств с использованием индикаторов поля, интерсепторов, частотомеров, сканерных приемников и программно-аппаратных комплексов контроля;
- организация радиоконтроля (постоянно или на время проведения конфиденциальных мероприятий) и побочных электромагнитных излучений ТСПИ.

В ходе использования **активных средств** реализуются специальные проверки:

- выделенных помещений с помощью *нелинейных локаторов*;
- выделенных помещений, ТСПИ и вспомогательных технических средств с помощью *рентгеновских комплексов*.

1. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993)
2. Указ Президента РФ от 30.11.1995 N 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне».
3. Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера».
4. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне».
5. Федеральный закон от 28.12.2010 N 390-ФЗ "О безопасности".
6. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ.
7. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ.
8. «Гражданский кодекс Российской Федерации» от 30 ноября 1994 года N 51-ФЗ.

9. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».
11. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне".
12. Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 05.12.2017) "О связи".
13. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи».
14. Федеральный закон от 7.02.2011, № 3-ФЗ «О полиции».
15. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

16. Доктрина информационной безопасности Российской Федерации (Утверждена указом Президента РФ от 5 декабря 2016 г. № 646).

17. Постановление Правительства РФ от 06.02.2010 N 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».

18. Инструкция по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации (Утверждена приказом МВД России от 6 июля 2012 г. № 678).

19. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы".

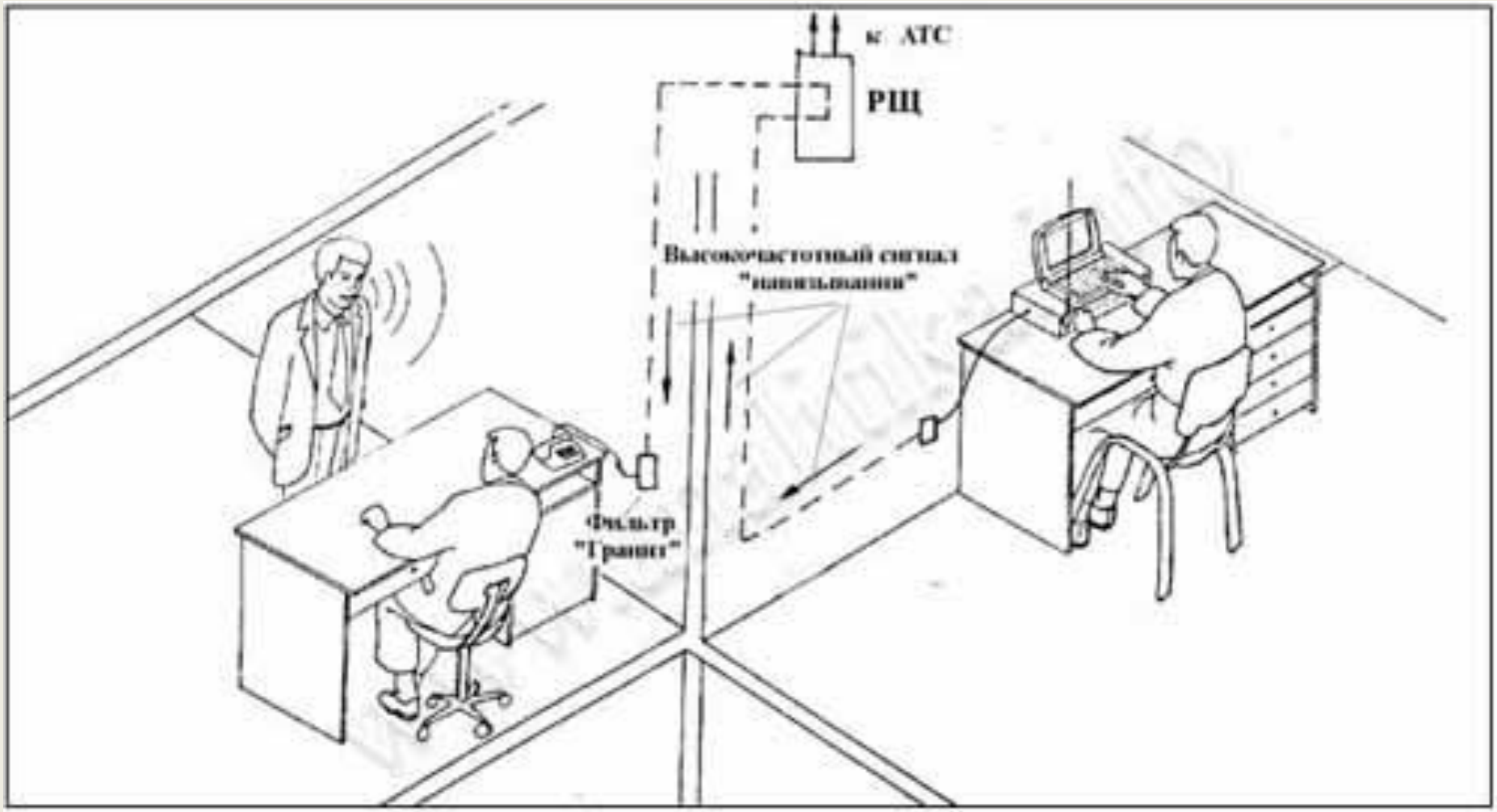


Рис. 1.1. Установка специальных фильтров типа «Гранит» в соединительных линиях вспомогательных технических средств, обладающих "микрофонным эффектом" и имеющих выход за пределы контролируемой зоны

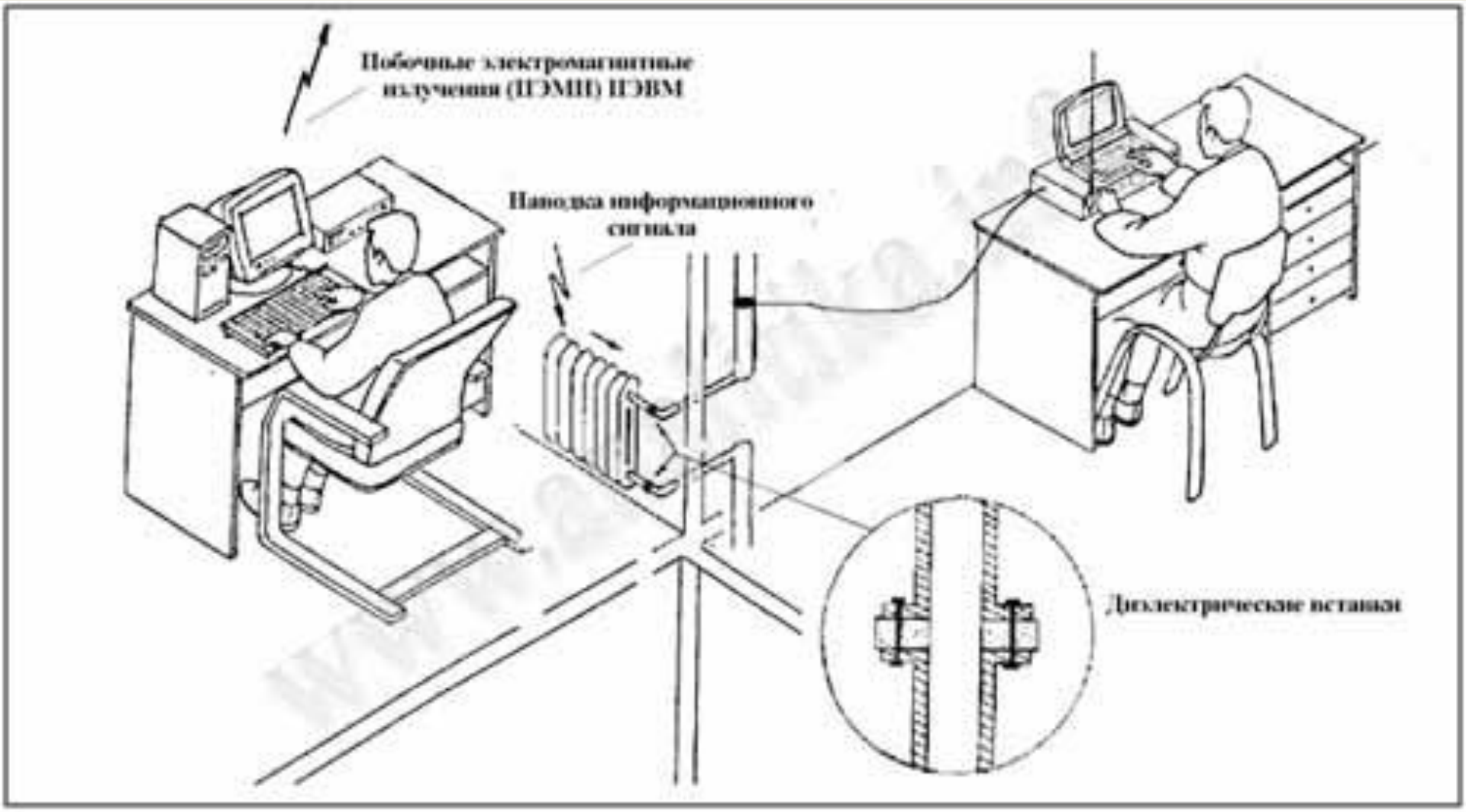


Рис. 1.2. Установка специальных диэлектрических вставок в трубы систем отопления и водоснабжения, имеющих выход за пределы контролируемой зоны

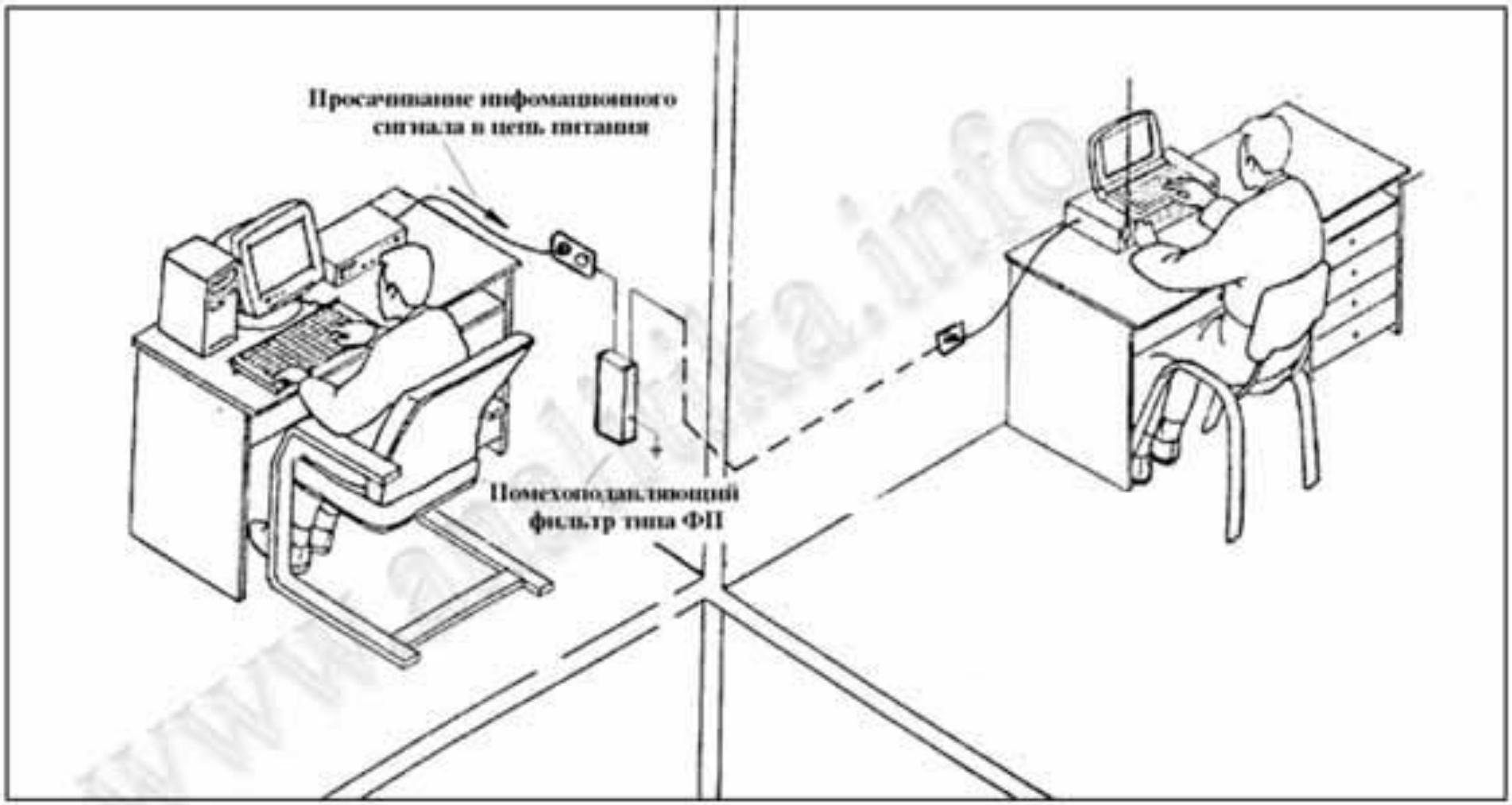


Рис. 1. 3. Установка в цепях электропитания ТСПИ помехоподавляющих фильтров типа ФП

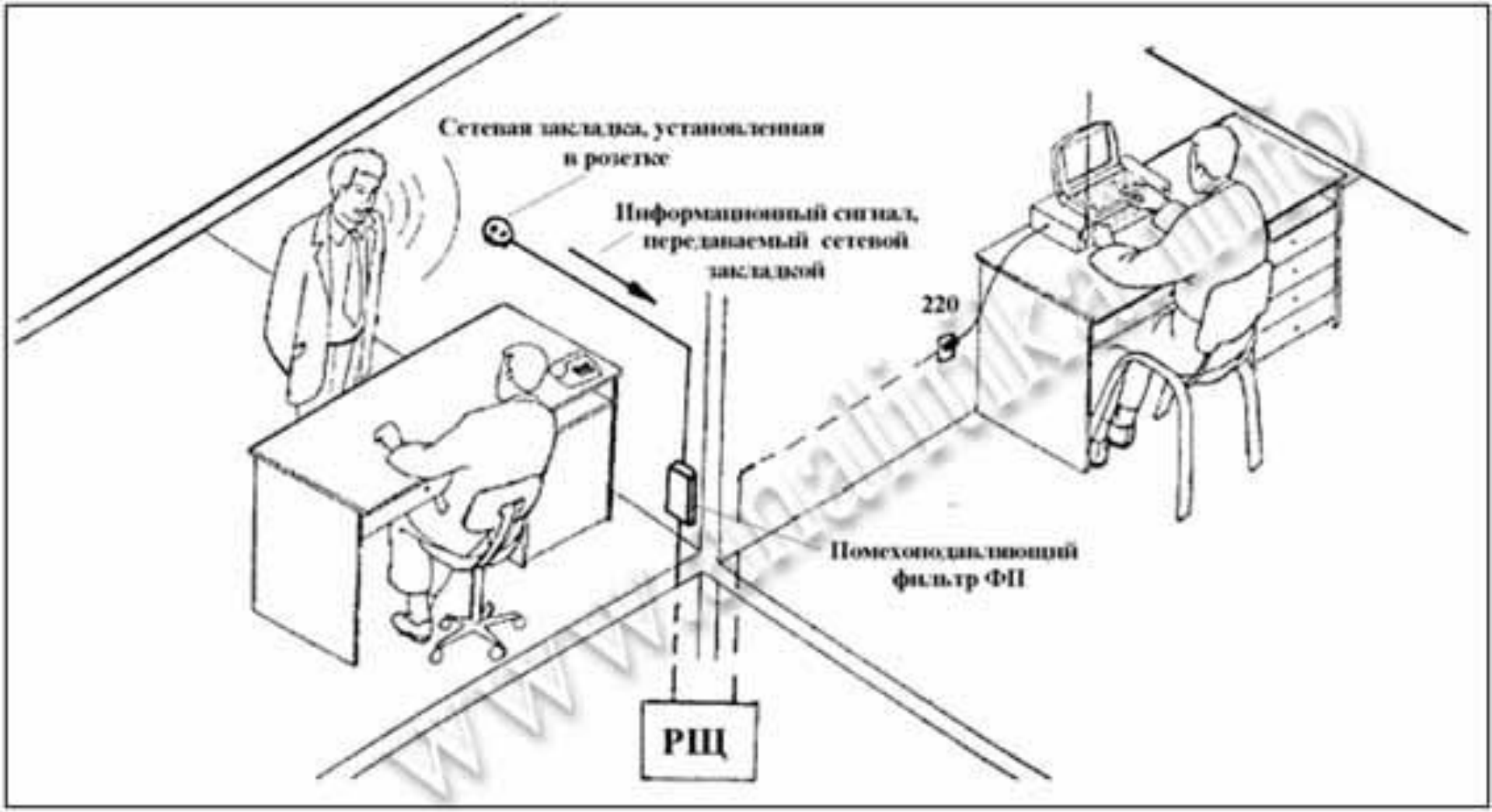


Рис. 1.4. Установка в осветительной и розеточных сетях электропитания выделенных помещений помехоподавляющих фильтров типа ФП

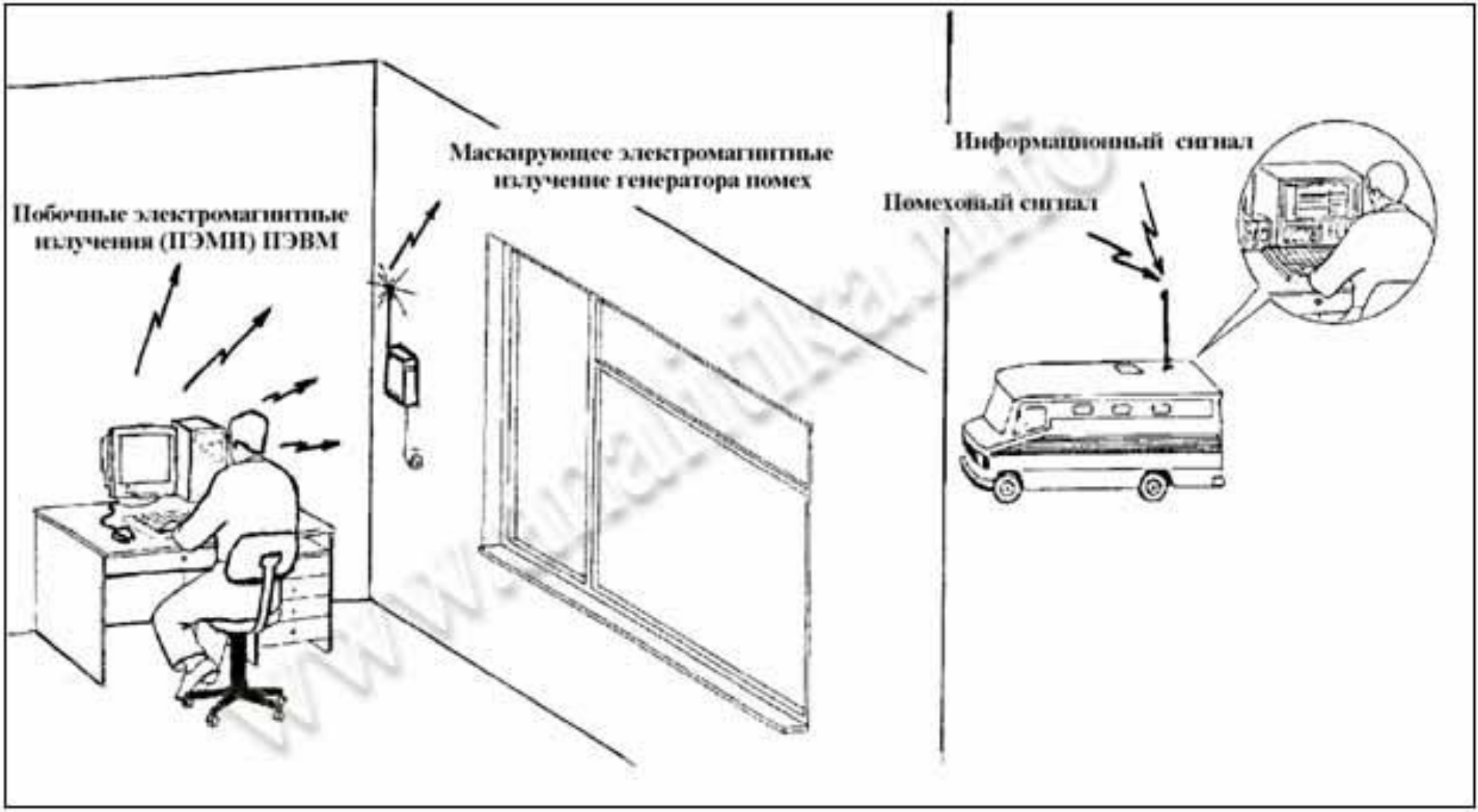


Рис. 1.5. Пространственное электромагнитное зашумление побочных электромагнитных излучений ПЭВМ с использованием генератора шума

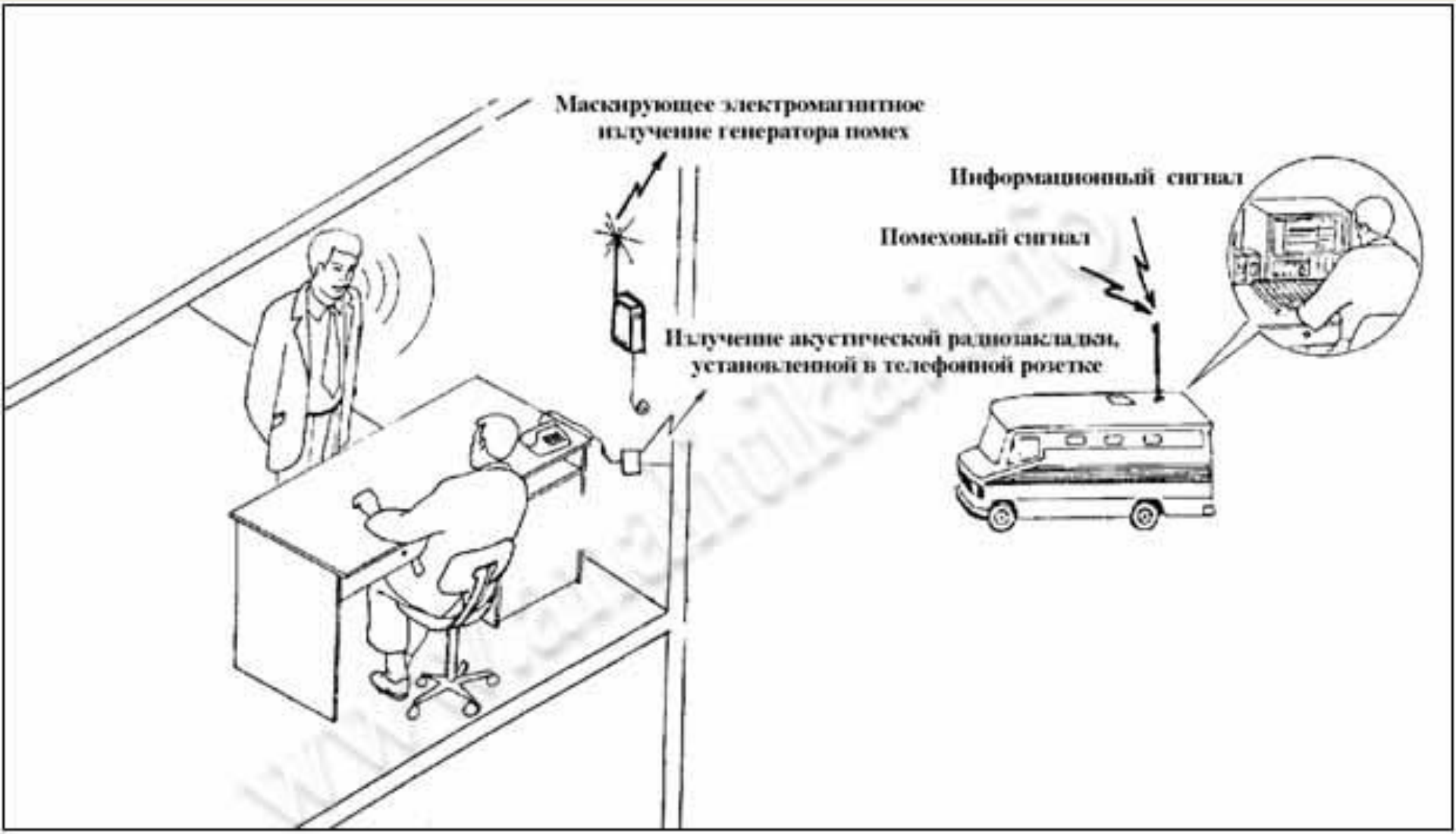


Рис. 1.6. Создание прицельных маскирующих радиопомех в каналах передачи информации закладными устройствами

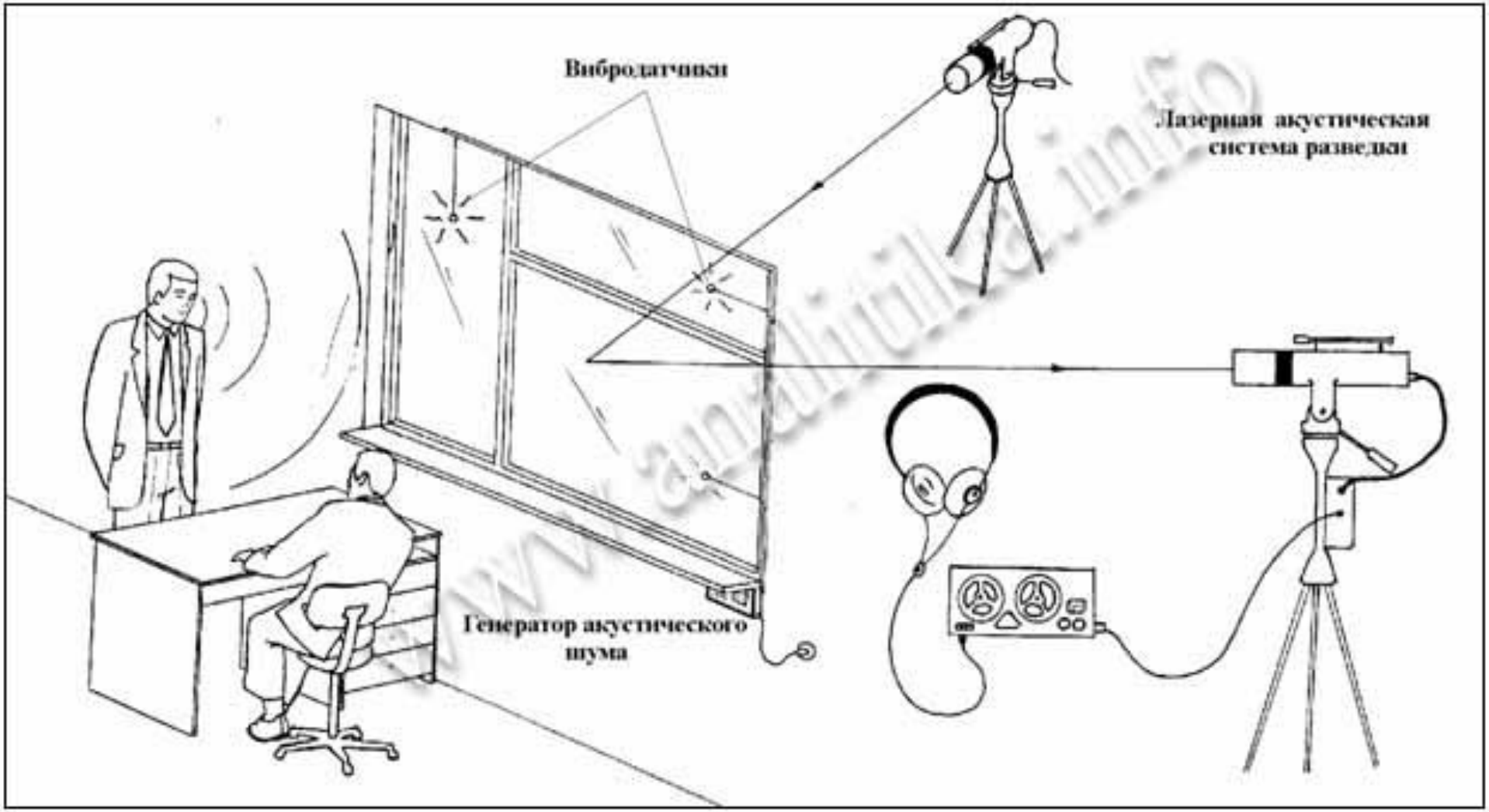


Рис. 1. 7. Создание вибрационных помех с использованием генераторов акустического шума с целью противодействия лазерным акустическим системам разведки

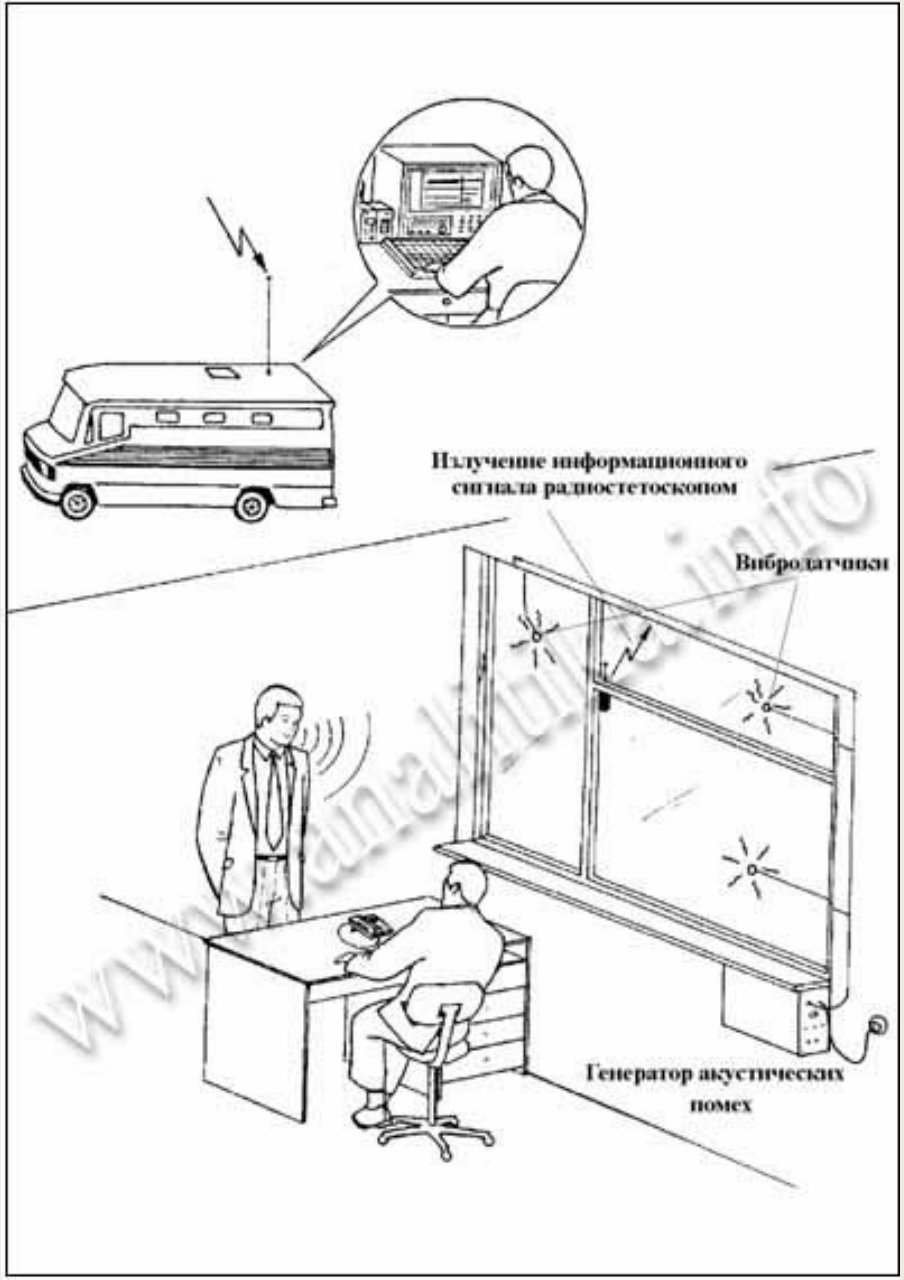


Рис. 1.8. Создание вибрационных помех с использованием генераторов акустического шума с целью подавления средств съема информации по виброакустическому каналу

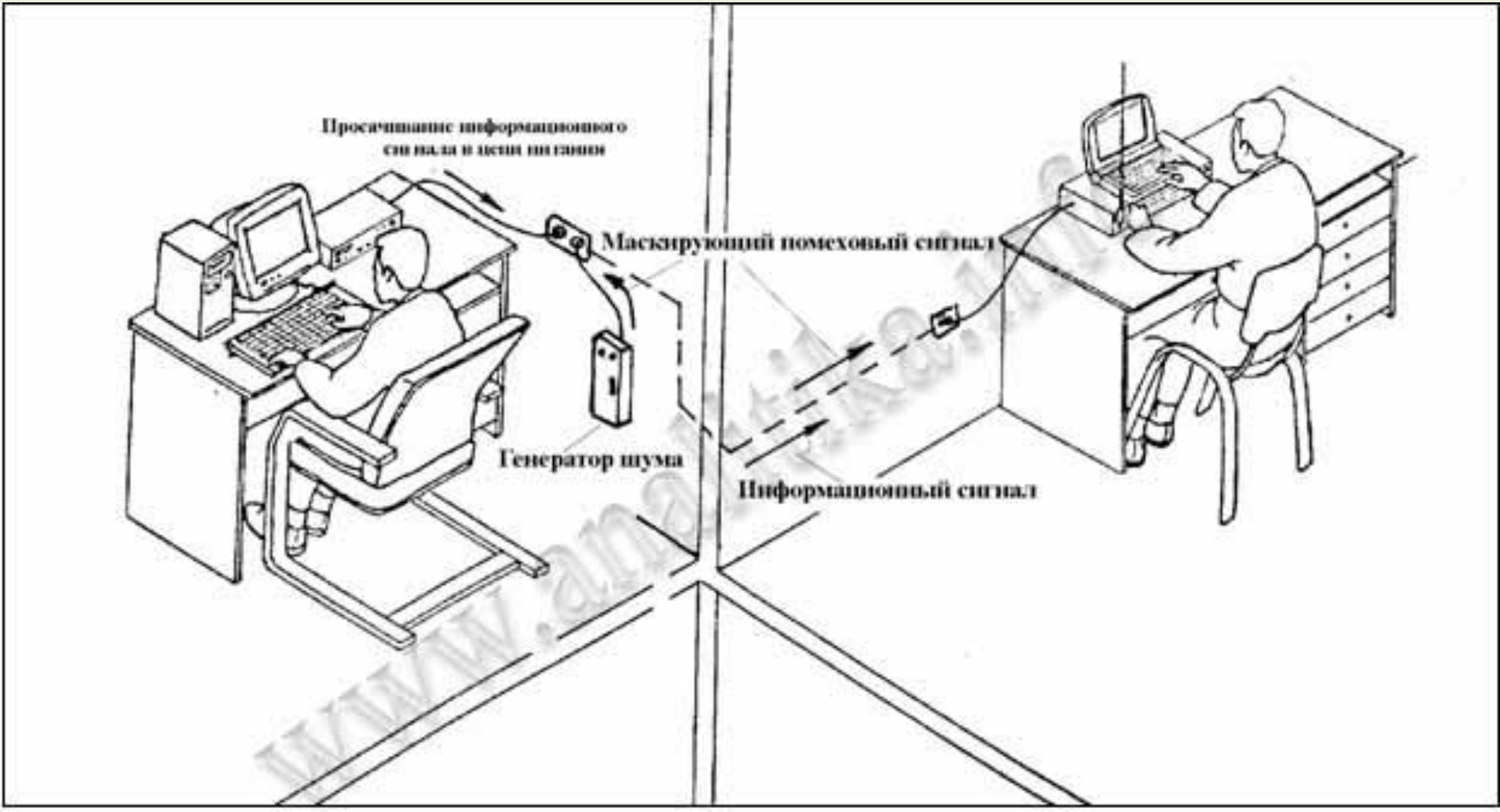


Рис. 1. 9. Линейное зашумление линий электропитания ТСПИ

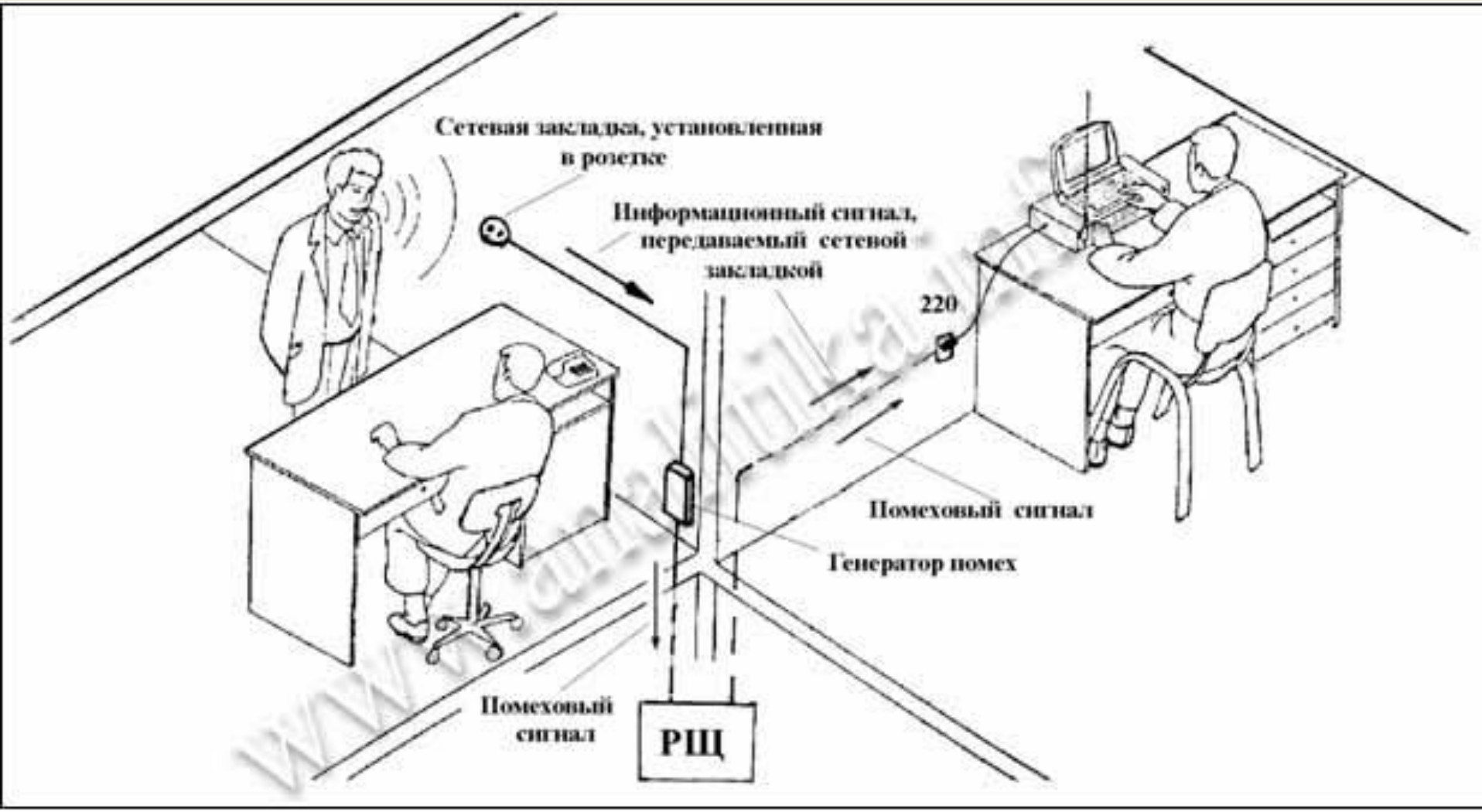
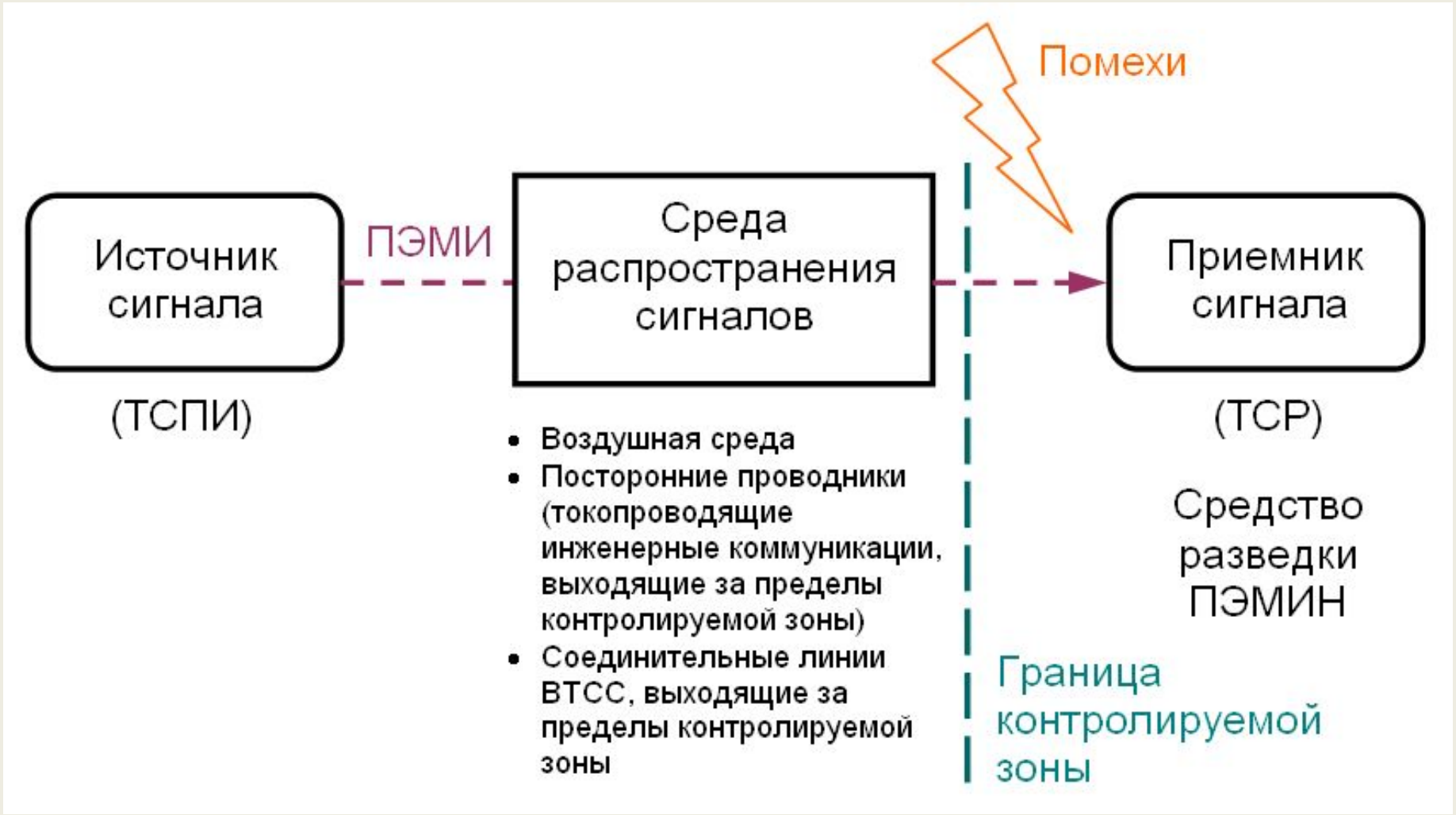
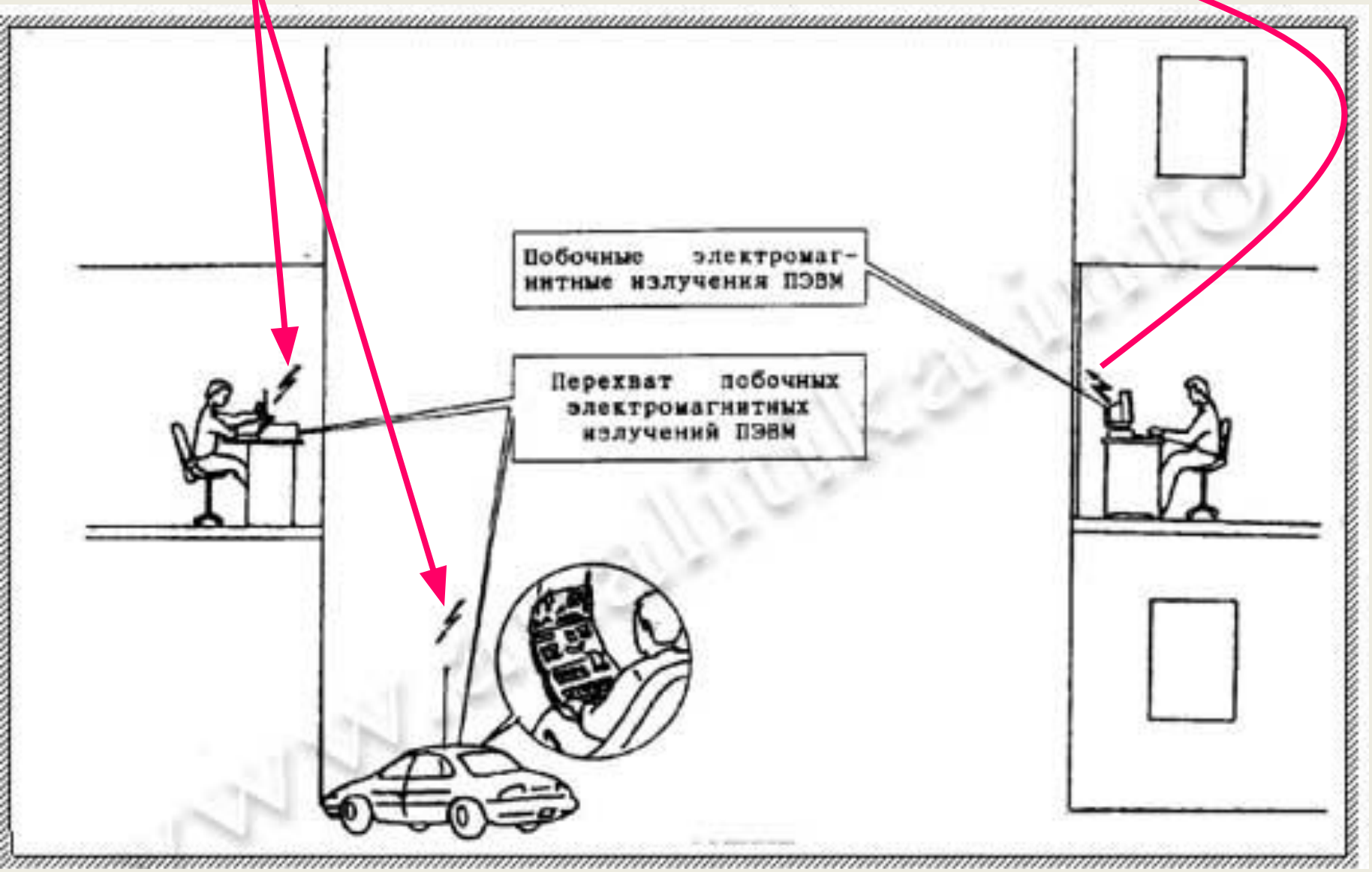


Рис.1.10. Линейное зашумление линий электропитания осветительной и розеточных сетей выделенных помещений

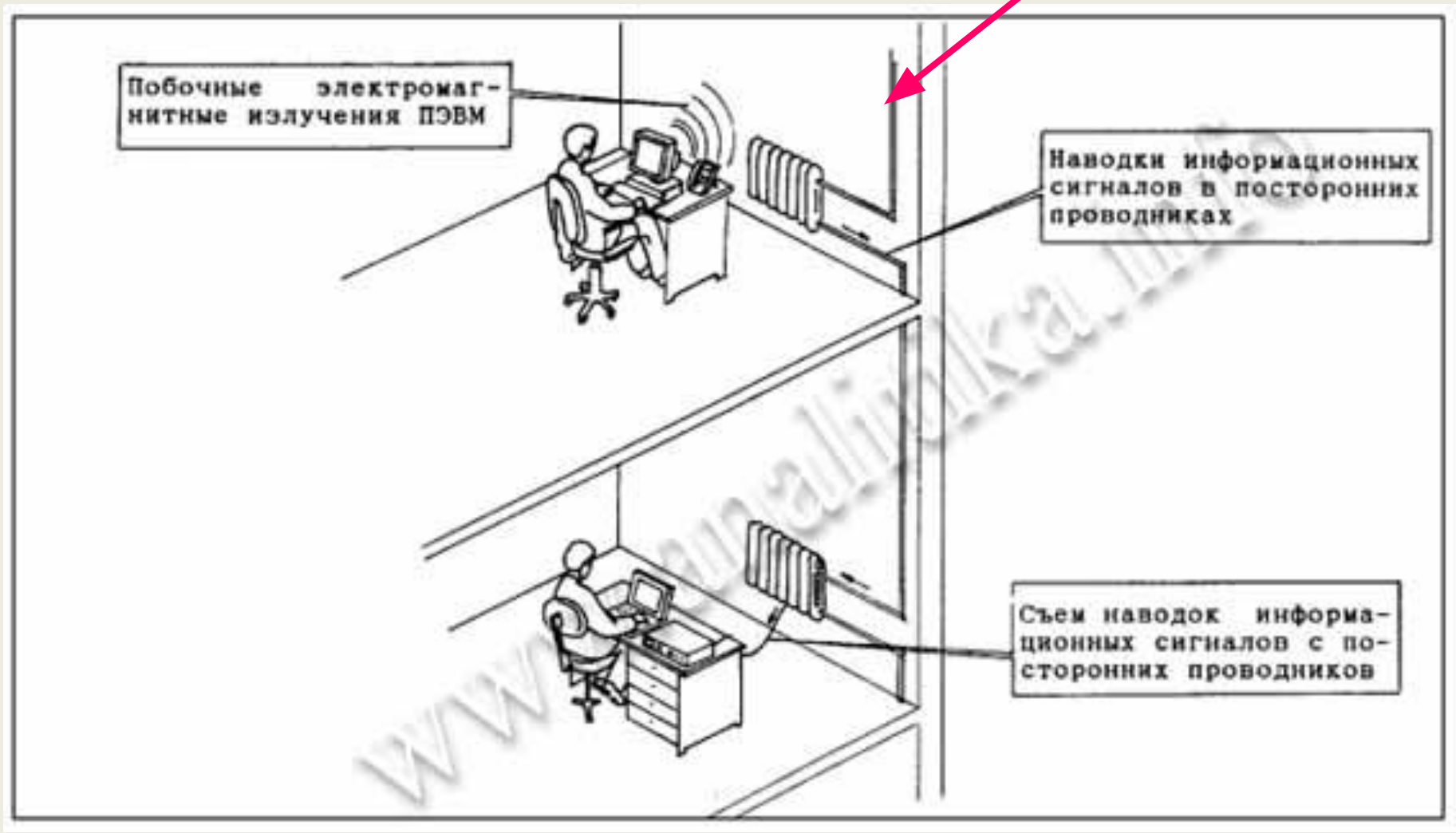
Схема технического канала утечки информации (ТКУИ)



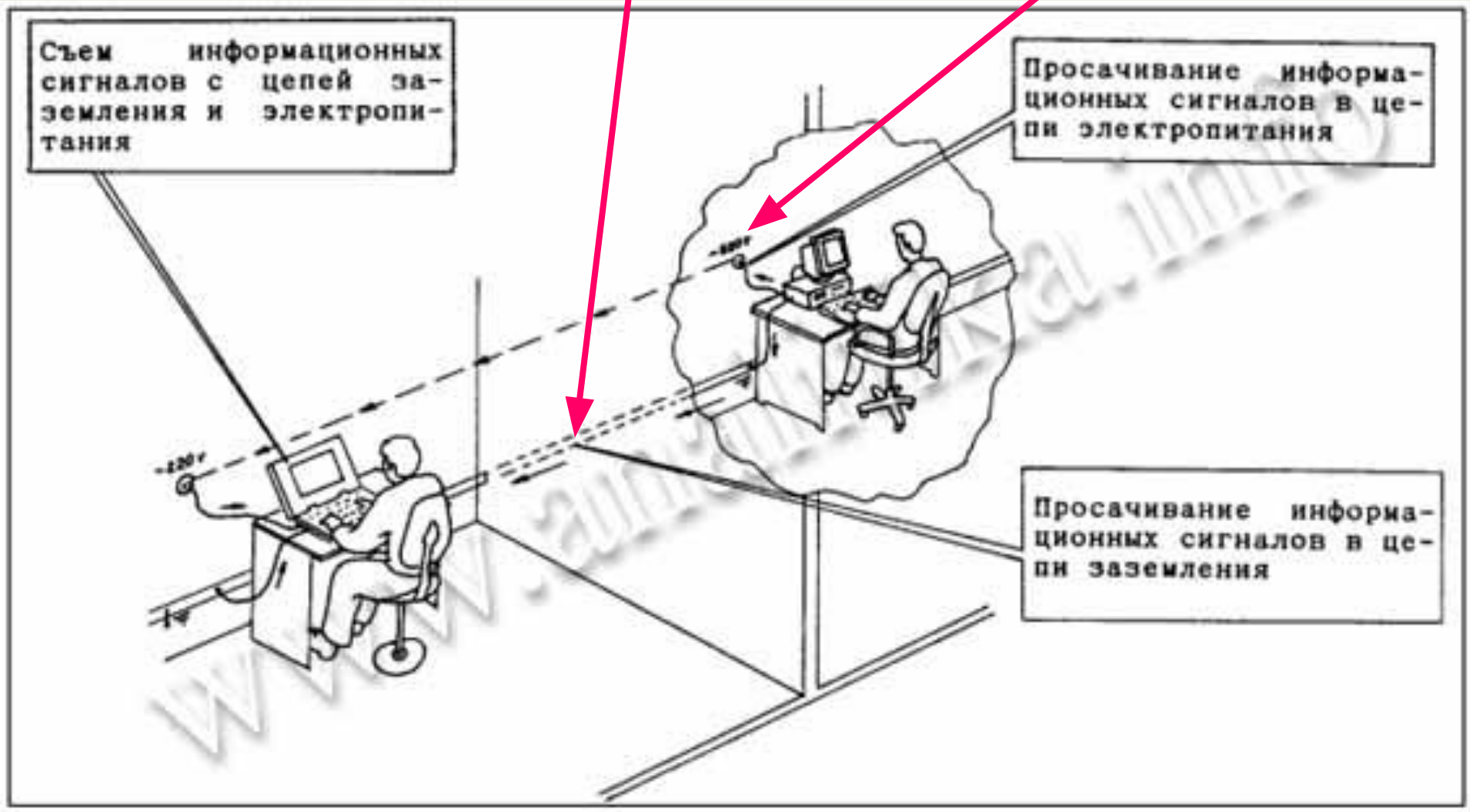
Перехват побочных электромагнитных излучений (ПЭМИ)



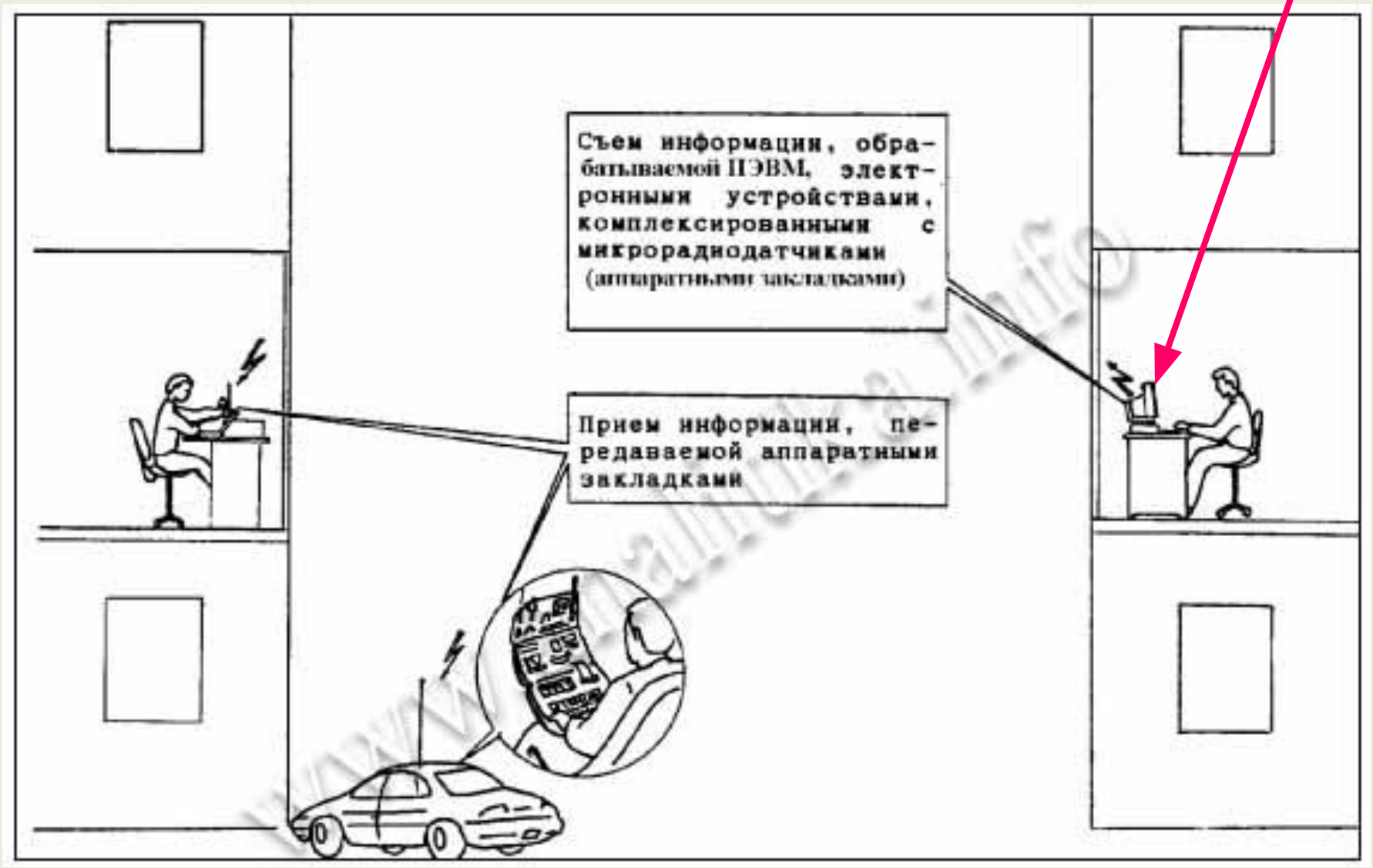
Съем наводок с посторонних проводников



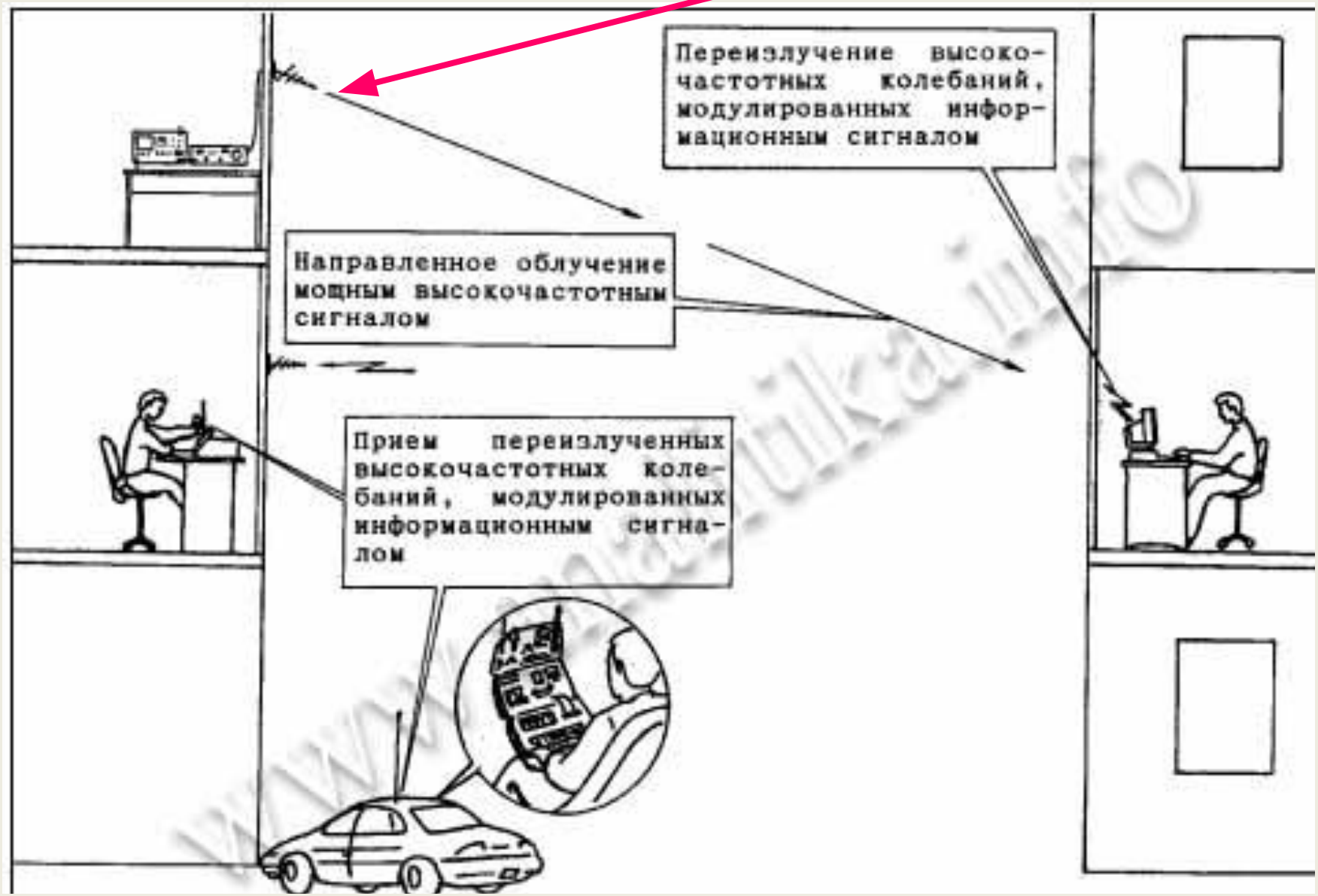
Съем наводок с заземления и электропитания



Съем информации с аппаратных закладок



Перехват информации «высокочастотным облучением»



Перехват информации микрофонами с устр. звукозаписи

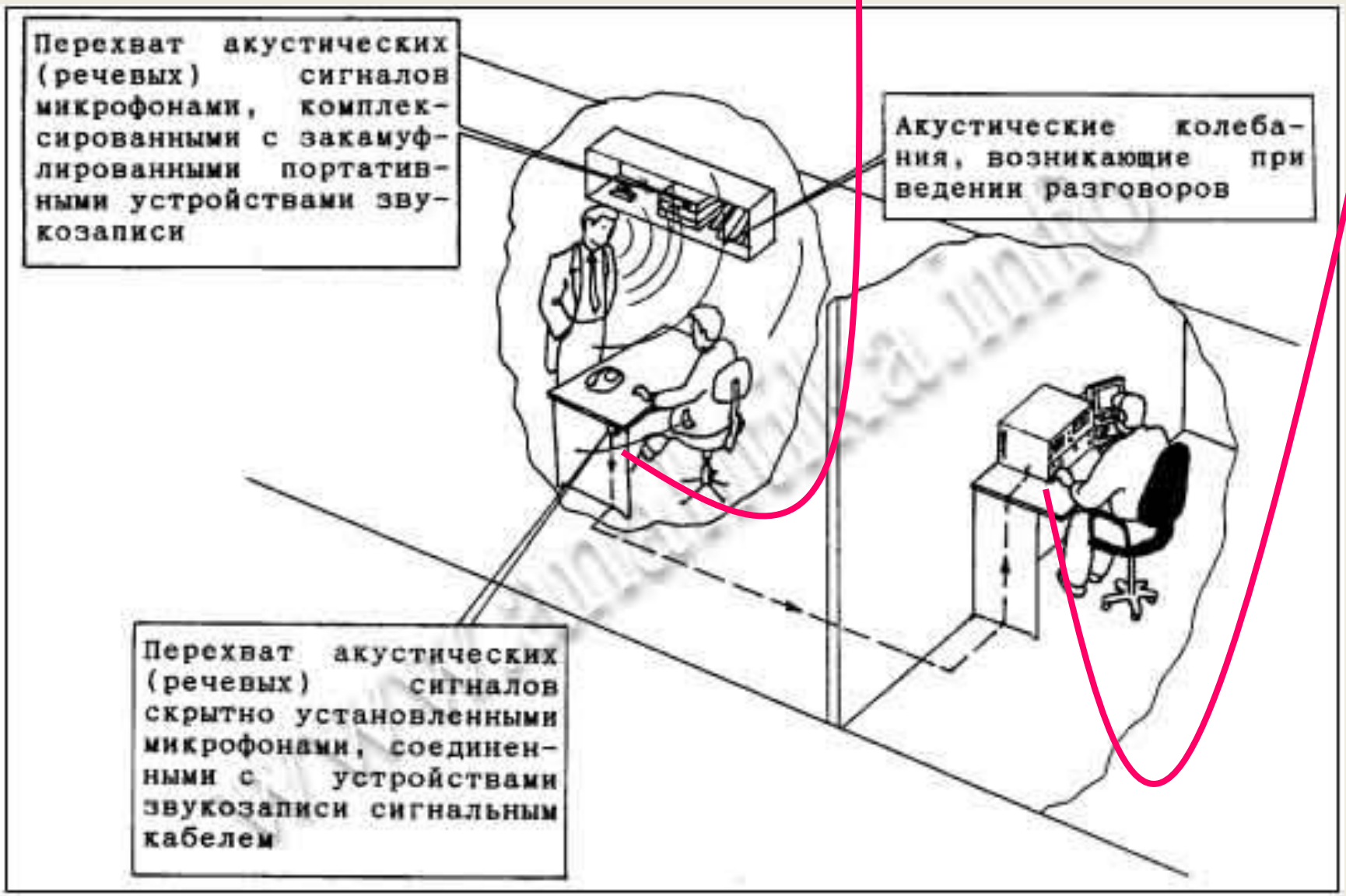


Рис. 1.8. Перехват акустических сигналов микрофонами, комплексированными с портативными устройствами звукозаписи

Перехват информации направленными микрофонами

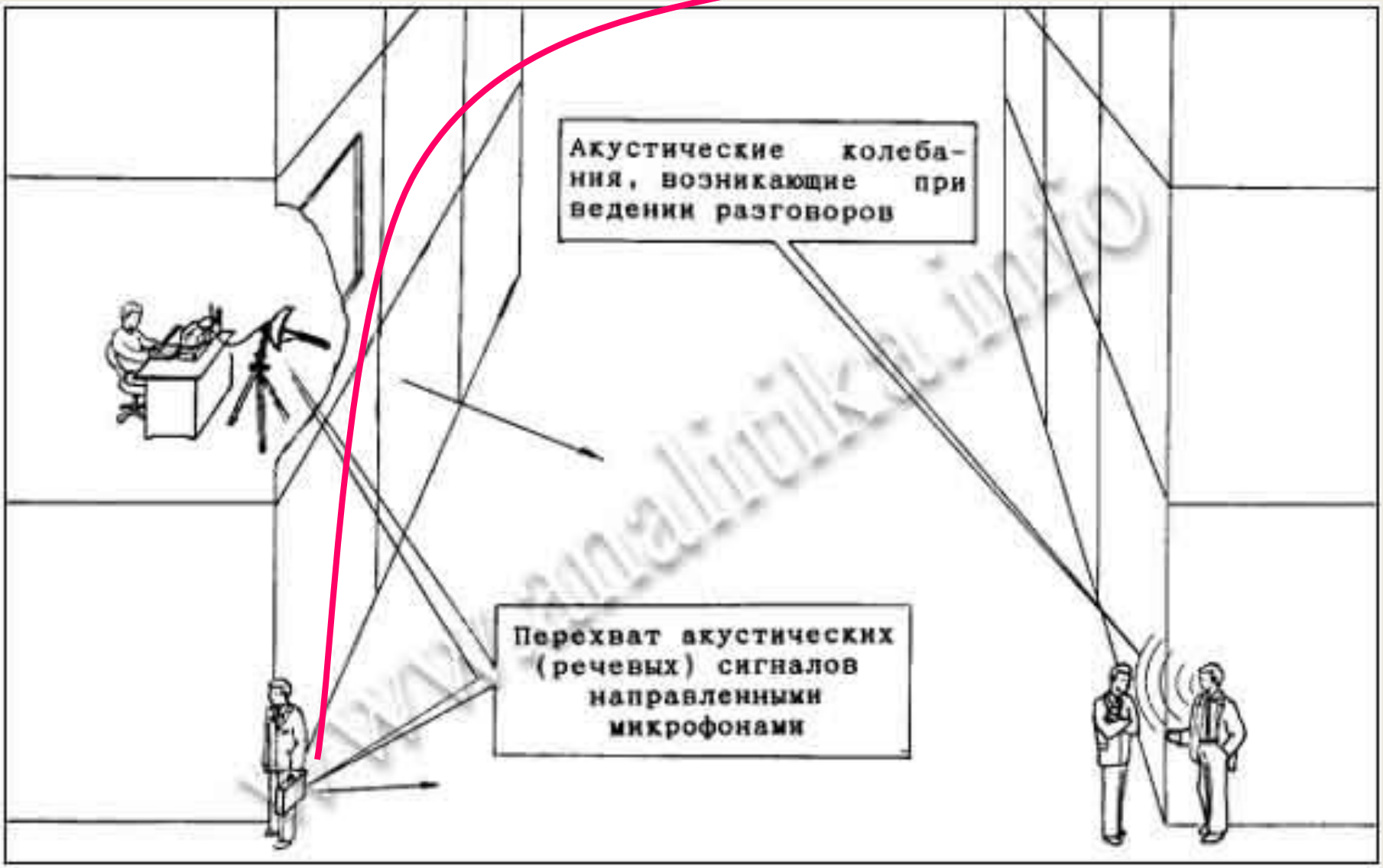


Рис. 1.9. Перехват акустических сигналов направленными микрофонами

Перехват информации радиозакладками

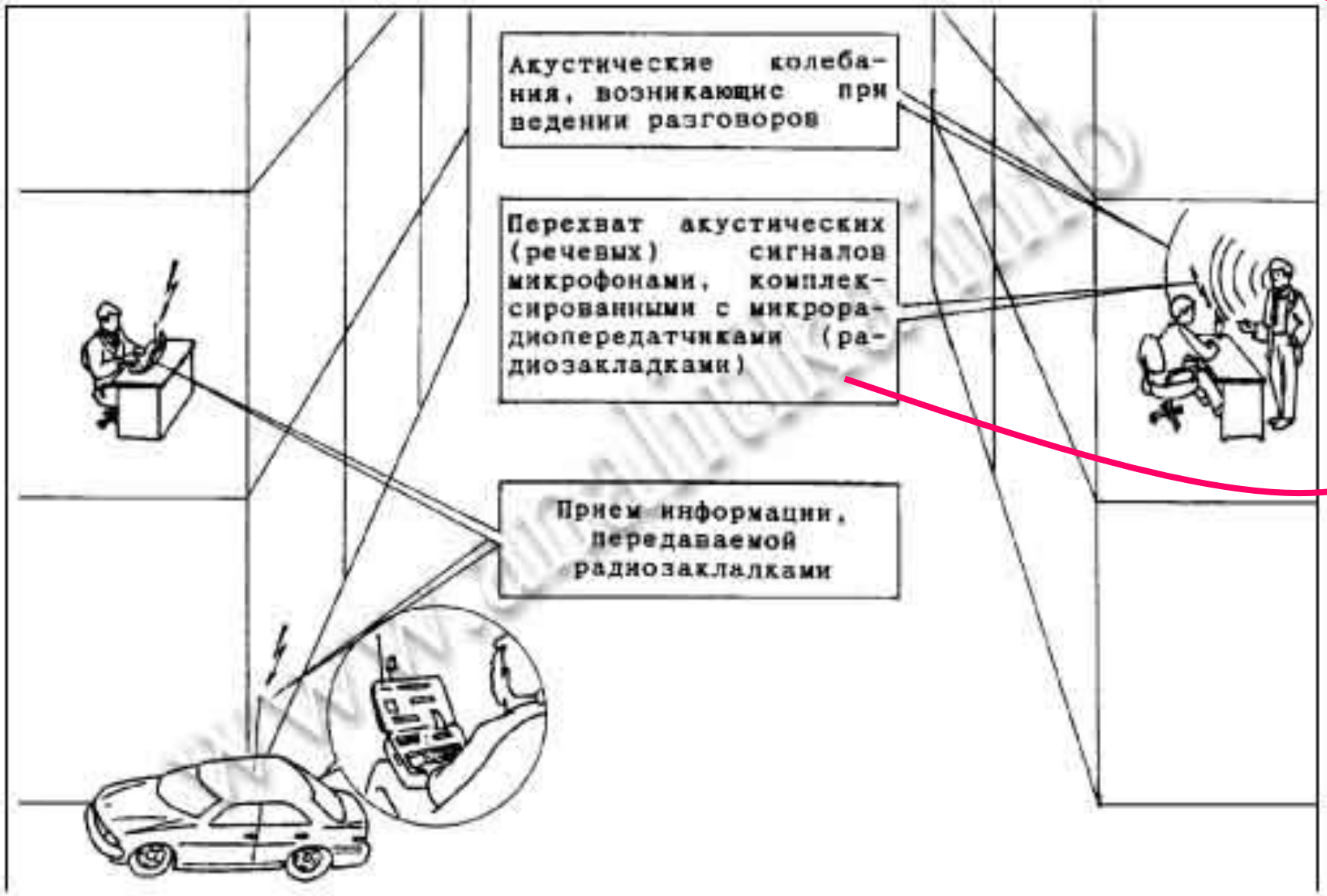


Рис. 1.10. Перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по радиоканалу

Перехват информации по оптическому каналу

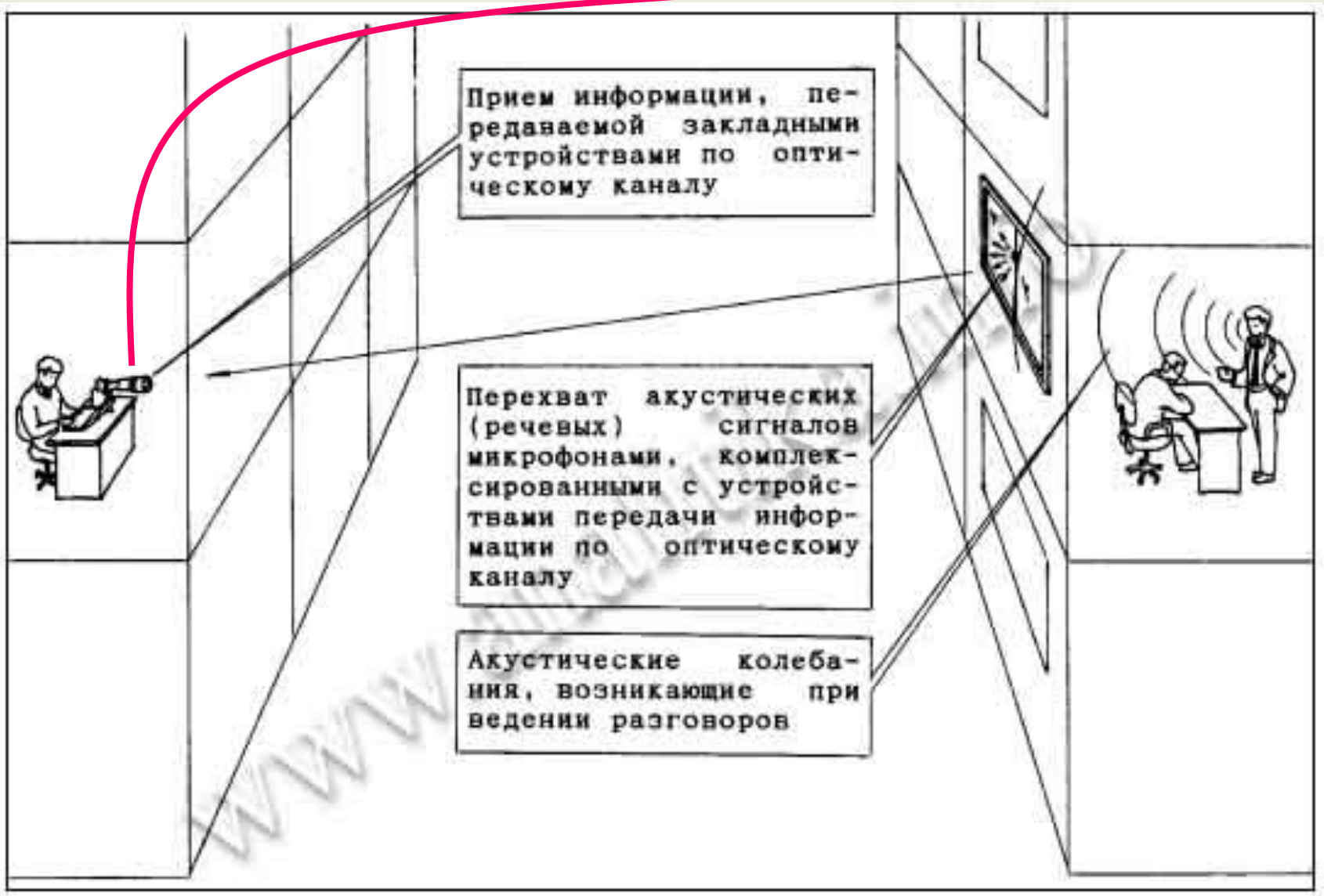


Рис. 1.11. Перехват акустических сигналов микрофонами (в том числе контактными), комплексированными с устройствами передачи информации по оптическому каналу

Перехват информации по электросети 220 в

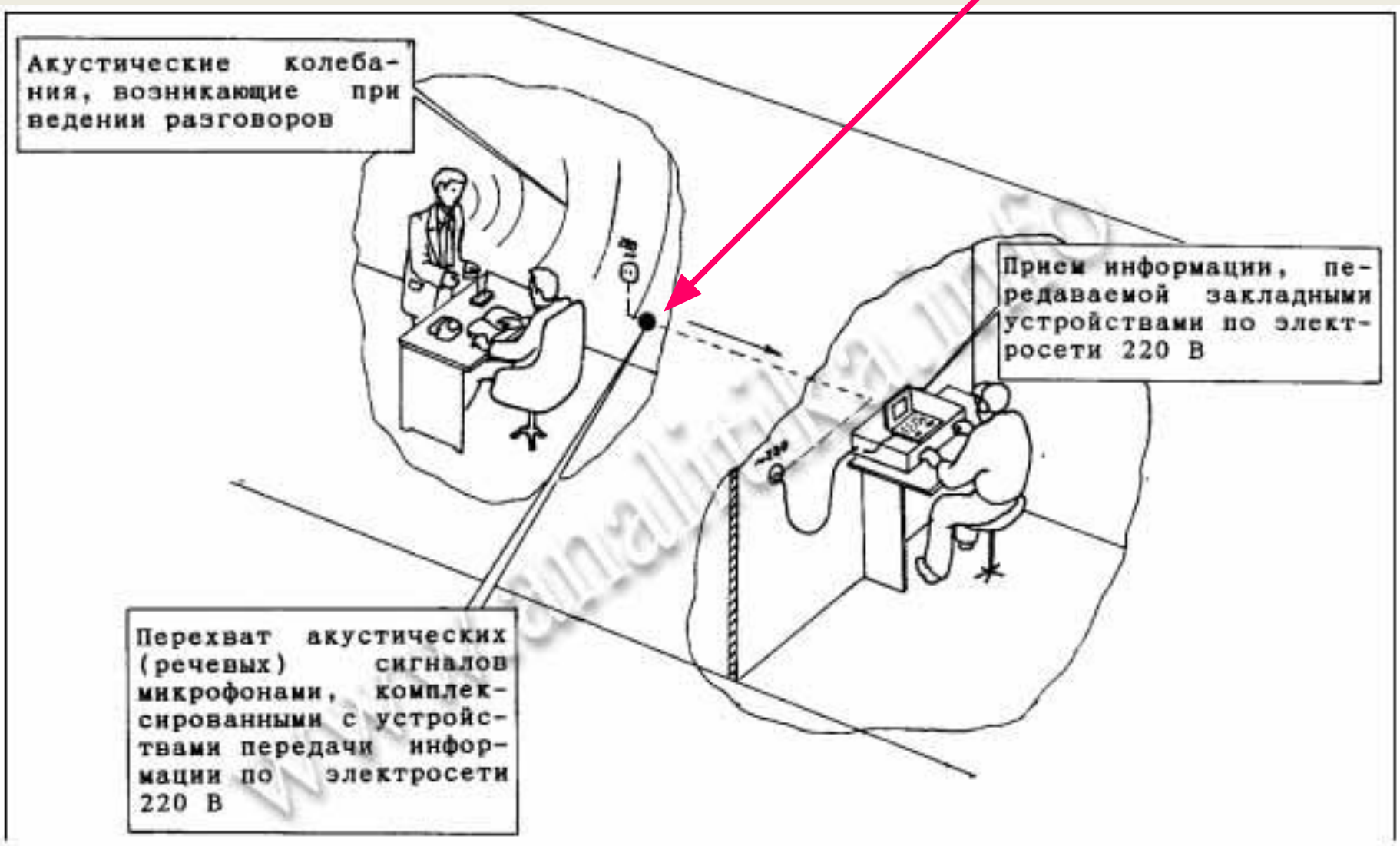


Рис. 1.12. Перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по электросети

Перехват информации по телефону-наблюдателю

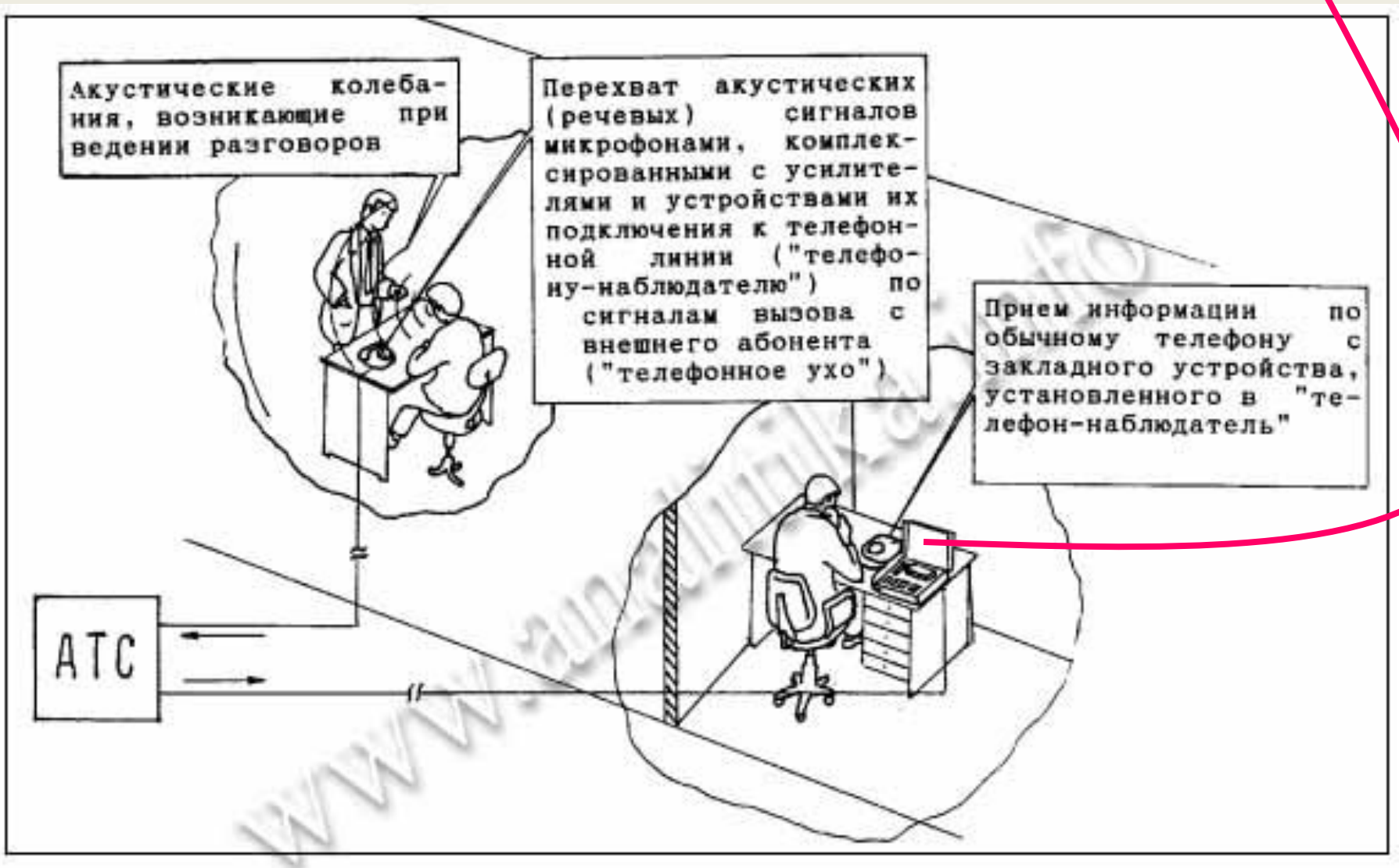


Рис. 1.13. Перехват акустических сигналов микрофонами, комплексированными с устройствами их подключения к телефонной линии ("телефону-наблюдателю") по сигналам вызова от внешнего абонента

Перехват информации по стетоскопу

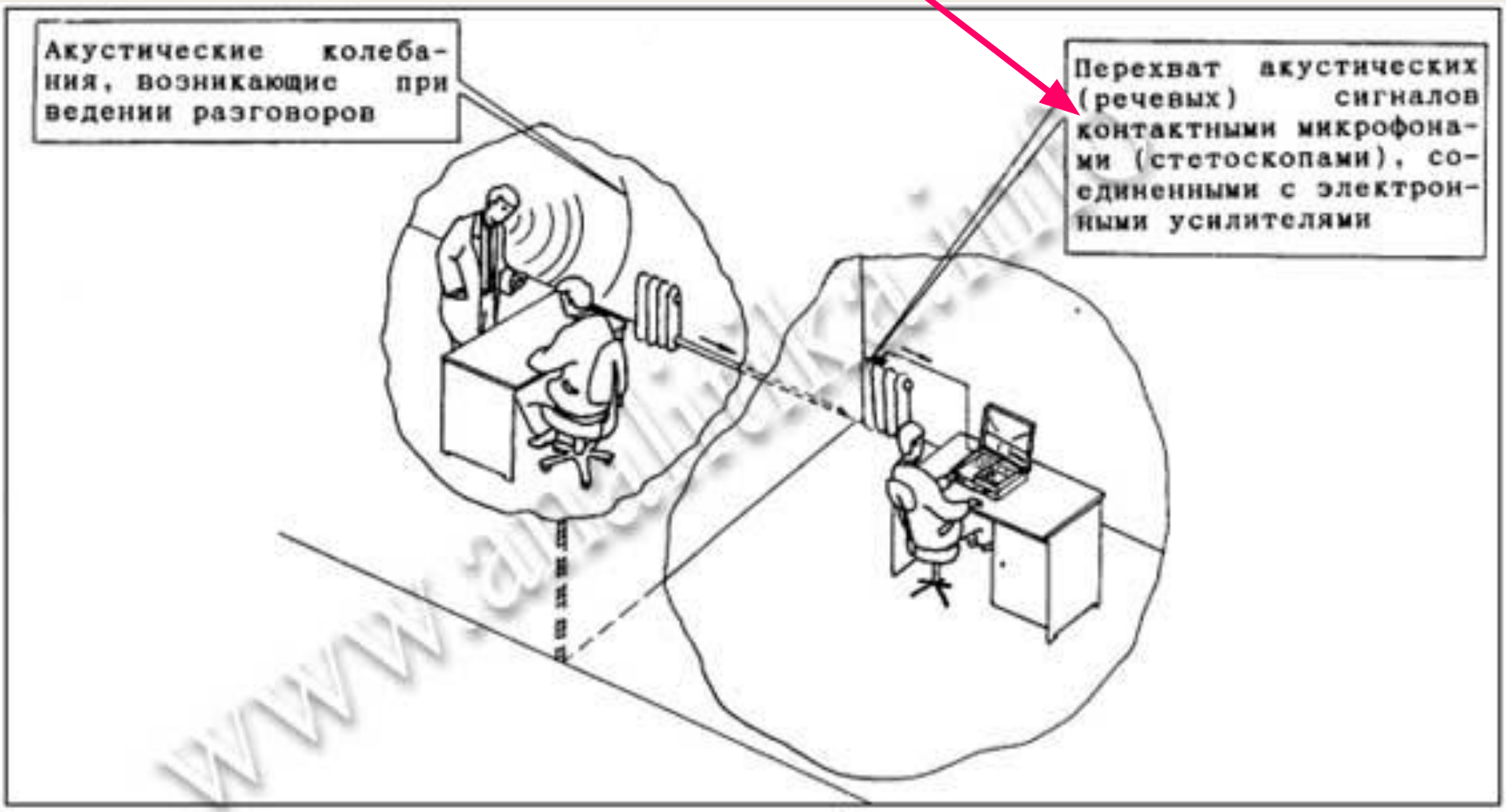


Рис. 1.14. Перехват акустических (речевых) сигналов электронными стетоскопами

Перехват информации по радиостетоскопу

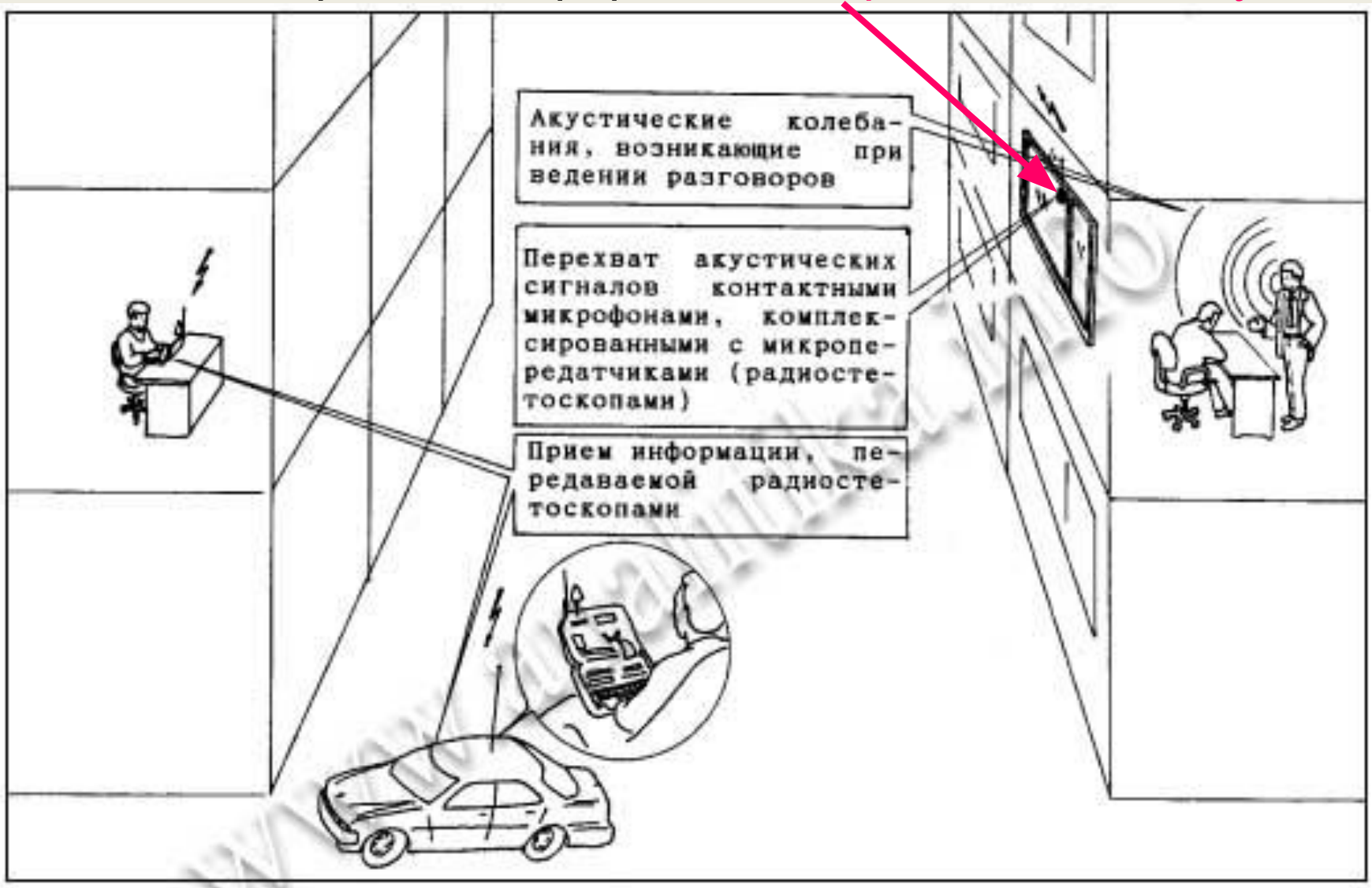


Рис. 1.15. Перехват акустических (речевых) сигналов электронными стетоскопами, комплексированными с устройствами передачи информации по радиоканалу (радиостетоскопами)

Перехват через ВТСС, обладающих “микрофонным эффектом”

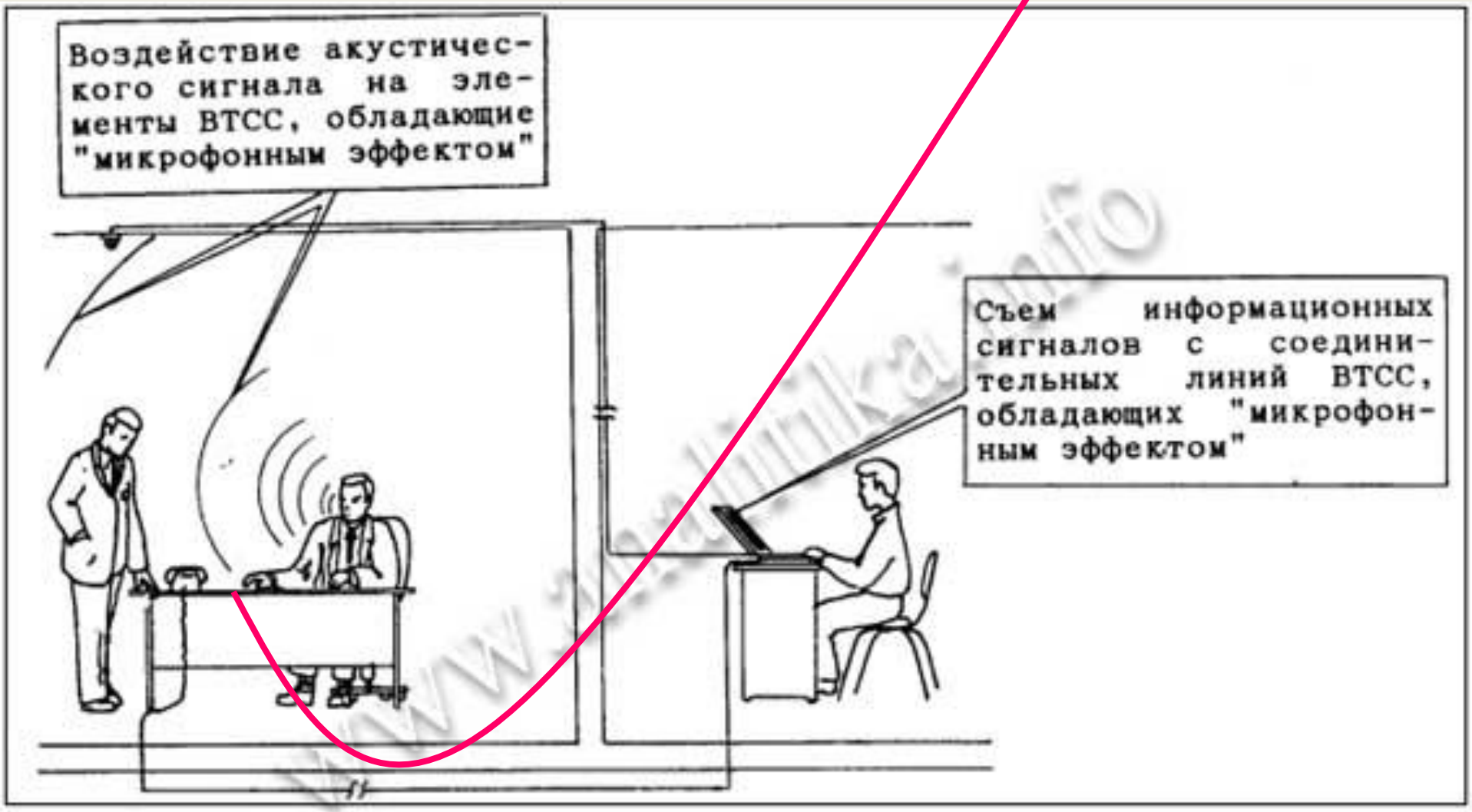


Рис. 1.16. Перехват акустических (речевых) сигналов через ВТСС, обладающие "микрофонным эффектом"

Перехват информации путем “высокочастотного навязывания”

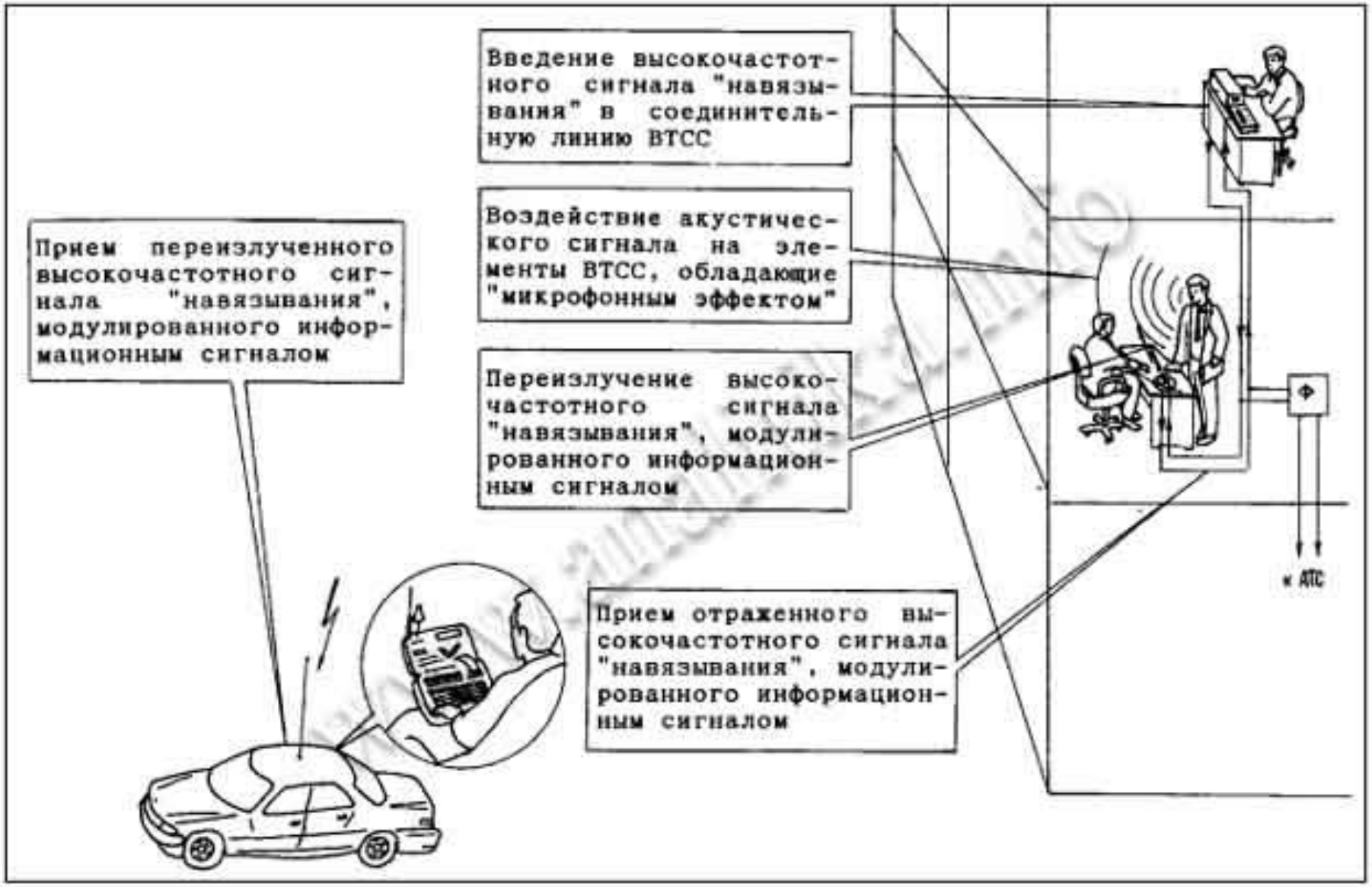


Рис. 1.17. Перехват акустических (речевых) сигналов через ВТСС путем "высокочастотного навязывания"

Перехват информации путем лазерного зондирования

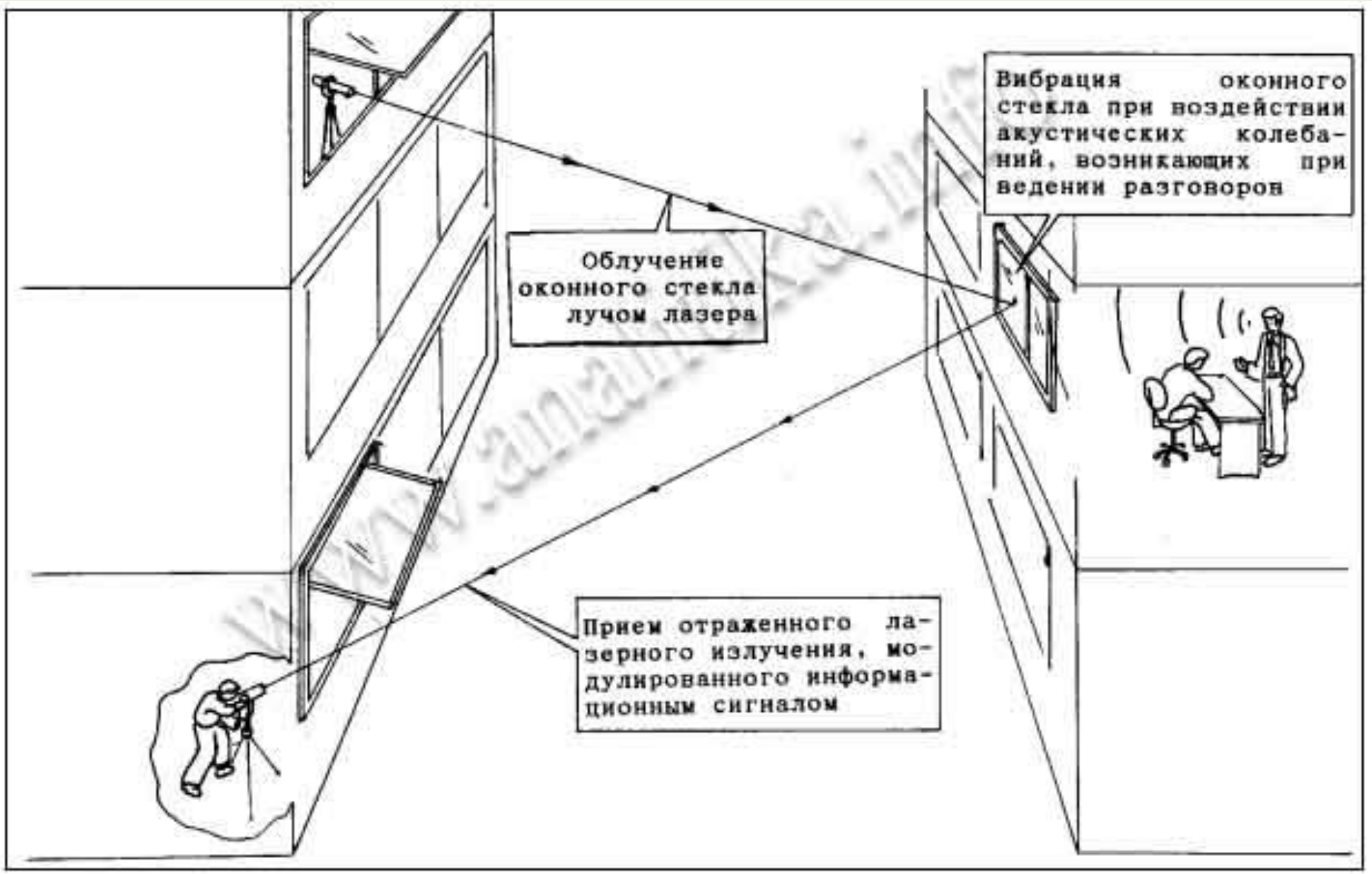


Рис. 1.18. Перехват акустических (речевых) сигналов путем лазерного зондирования оконных стекол

Перехват информации путем детектирования побочных излучений модулированных информационным сигналом

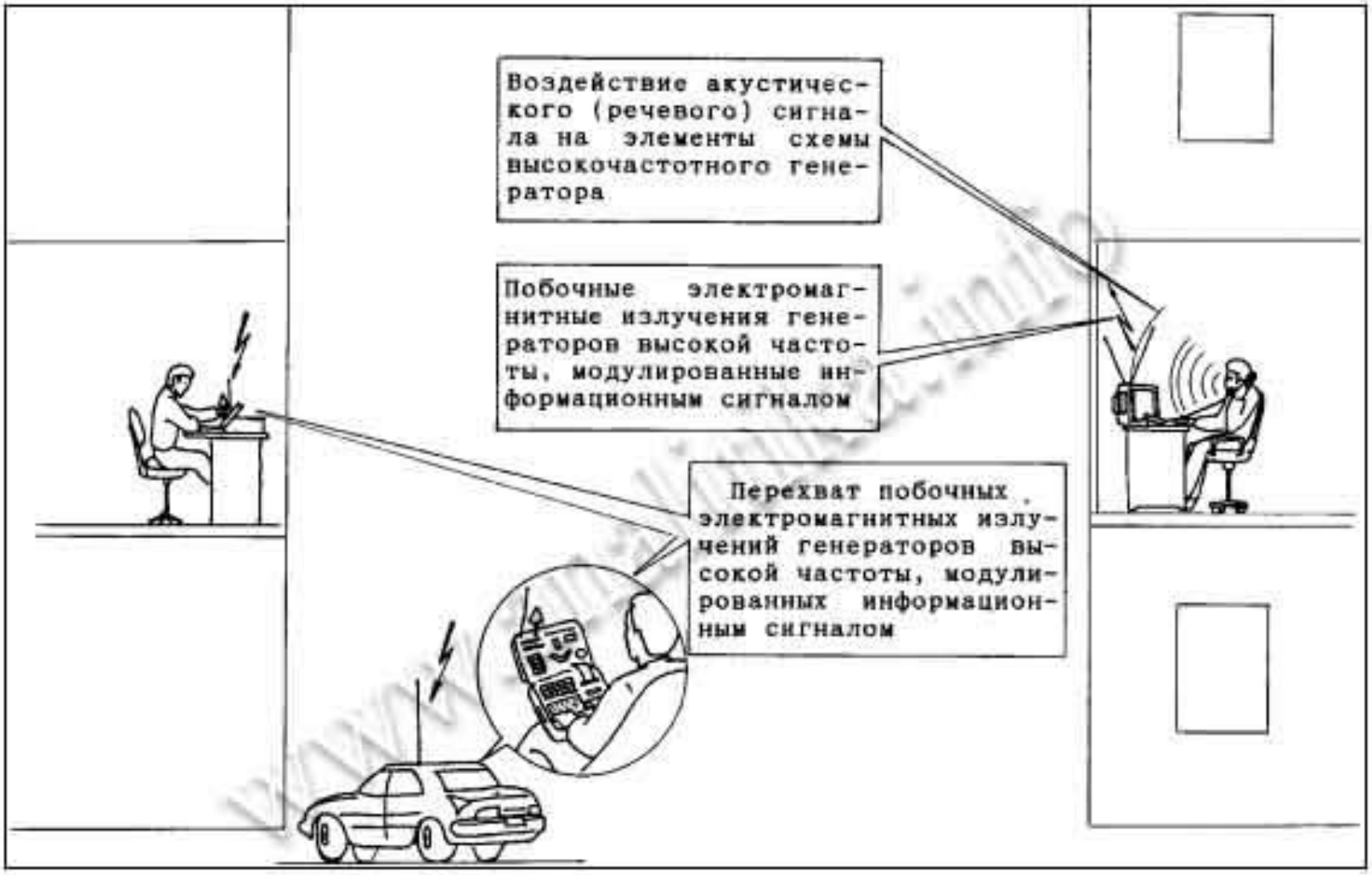


Рис. 1.19. Перехват акустических (речевых) сигналов путем приема и детектирования побочных электромагнитных излучений (на частотах работы высокочастотных генераторов ТСПИ и ВТСС), модулированных информационным сигналом

Перехват информации путем “высокочастотного облучения” закладных устройств

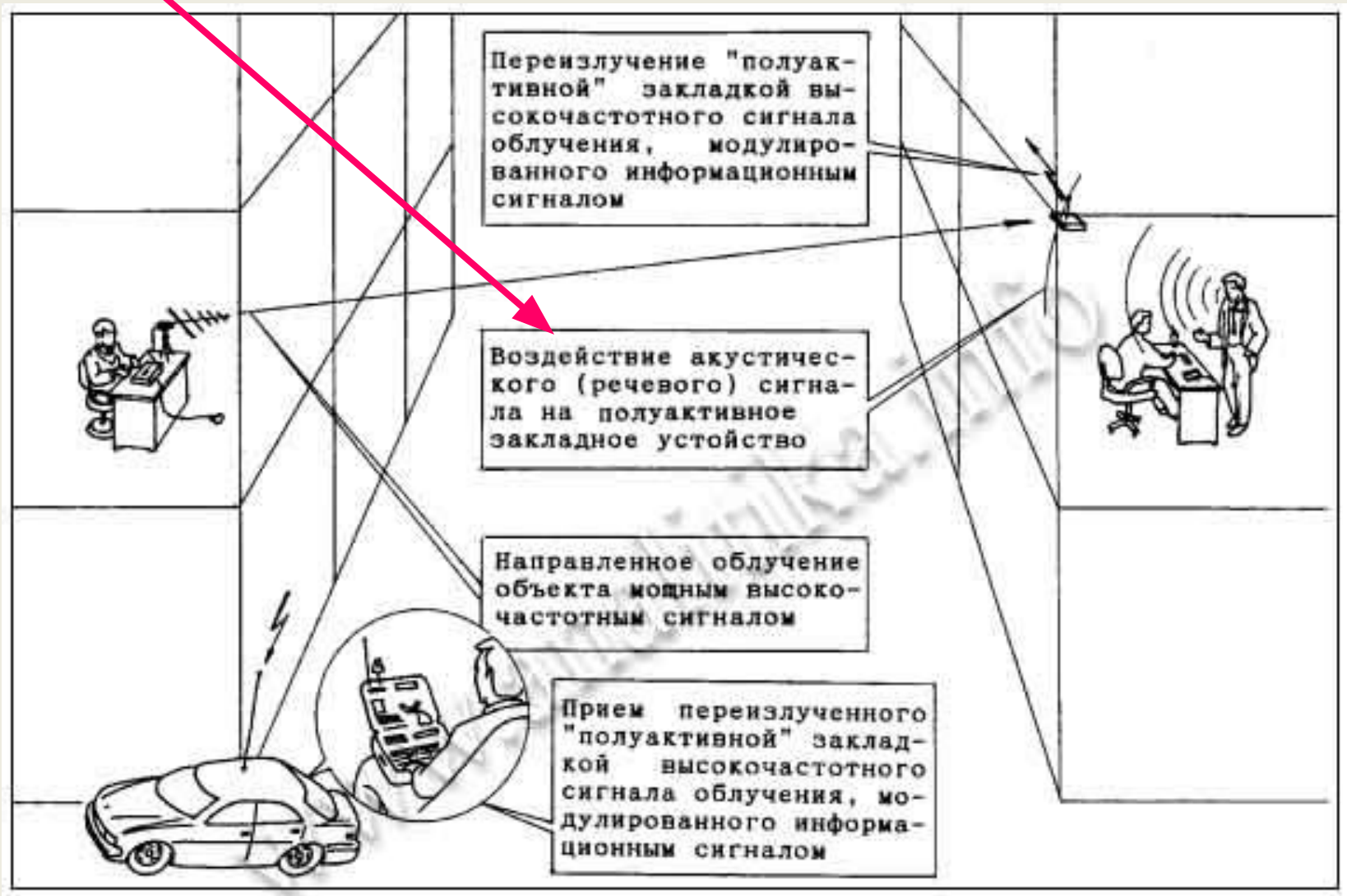


Рис. 1.20. Перехват акустических (речевых) сигналов путем "высокочастотного облучения" полуактивных закладных устройств

Вопросы к семинару:

1. Понятие и структура технического канала утечки информации.

2. Классификация технических каналов утечки информации.

3. Объясните понятие утечки по радиоканалу.

4. Объясните понятие утечки по электрическому каналу.

5. Акустический канал утечки информации, методы и средства защиты.

6. Виброакустический канал утечки информации, методы и средства защиты.

7. Акустоэлектрический и параметрический канал утечки информации, методы и средства защиты.

8. Оптико-электронный канал утечки информации, методы и средства защиты.

9. Объясните понятие утечки по каналу ПЭМИН.