

Методы защиты речевой информации от утечки по техническим каналам

- 1. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам и каналы перехвата информации техническими средствами**
- 2. Специально создаваемые технические каналы утечки информации**
- 3. Электронные устройства для поиска устройств перехвата информации**
- 4. Снятие информации со стекла и борьба с ним (схема для защиты)**
- 5. Использование ИК-диапазона для снятия информации с оконного стекла и схема для защиты**
- 6. Глушилка частот, как способ защиты от прослушки.**

Таблица 1. Потенциальные технические каналы утечки речевой информации

Технические каналы утечки информации	Специальные технические средства речевой разведки, используемые для перехвата информации
<p>Прямой акустический (через щели, окна, двери, технологические проемы, вентиляционные каналы и т. д.)</p>	<p><i>Направленные микрофоны, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны.</i></p> <p><i>Специальные высокочувствительные микрофоны, установленные в воздуховодах или в смежных помещениях, принадлежащих другим организациям.</i></p> <p><i>Электронные устройства перехвата речевой информации с датчиками микрофонного типа, установленные в воздуховодах, при условии неконтролируемого доступа к ним посторонних лиц.</i></p> <p><i>Прослушивание разговоров, ведущихся в выделенном помещении, без применения технических средств посторонними лицами (посетителями, техническим персоналом), при их нахождении в коридорах и смежных с выделенным помещениях (непреднамеренное прослушивание).</i></p>
<p>Акустовибрационный (через ограждающие конструкции, трубы инженерных коммуникаций и т. д.)</p>	<p><i>Электронные стетоскопы, установленные в смежных помещениях, принадлежащих другим организациям.</i></p> <p><i>Электронные устройства перехвата речевой информации с датчиками контактного типа, установленные на инженерно-технических коммуникациях (трубы водоснабжения,</i></p>

	отопления, канализации, воздуховоды и т. п.) и внешних ограждающих конструкциях (стены, потолки, полы, двери, оконные рамы и т. п.) выделенного помещения, при условии неконтролируемого доступа к ним посторонних лиц.
Акустооптический (через оконные стекла)	<i>Лазерные акустические локационные системы, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны.</i>
Акустоэлектрический (через соединительные линии ВТСС)	<i>Специальные низкочастотные усилители, подключаемые за пределами контролируемой зоны к соединительным линиям ВТСС, имеющим в своем составе элементы, обладающие «микрофонным» эффектом.</i> <i>Аппаратура «высокочастотного навязывания», подключаемая за пределами контролируемой зоны к соединительным линиям ВТСС, имеющим в своем составе элементы, обладающие «микрофонным» эффектом.</i>
Акустоэлектромагнитный (параметрический)	<i>Специальные радиоприемные устройства, устанавливаемые в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны, перехватывающие ПЭМИ ВТСС на частотах работы высокочастотных генераторов, входящих в их состав.</i> <i>Аппаратура «высокочастотного облучения» ВТСС, устанавливаемая в ближайших строениях, находящихся за пределами контролируемой зоны.</i>

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 можно 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

**Таблица 5. Критерии эффективности защиты
выделенных помещений**

Цель защиты	Потенциальные технические каналы утечки информации	Критерий эффективности защиты
Скрытие факта ведения переговоров в выделенном помещении	Прямой акустический, акустовибрационный, акустооптический, акустоэлектрический, акустоэлектромагнитный	$W_n < 10 \%$
Скрытие предмета переговоров в выделенном помещении	Прямой акустический, акустовибрационный, акустооптический, акустоэлектрический, акустоэлектромагнитный	$W_n < 20 \%$
Скрытие содержания переговоров в выделенном помещении	Прямой акустический, акустовибрационный, акустооптический, акустоэлектрический, акустоэлектромагнитный	$W_n < 30 \%$
Скрытие содержания переговоров в выделенном помещении	Прямой акустический без применения технических средств (непреднамеренное прослушивание)	$W_n < 40 \%$

Способы перехвата информации обрабатываемой техническими средствами



Рис. 17. Классификация способов перехвата информации, обрабатываемой техническими средствами

Подробнее о каналах утечки

- **Электромагнитные каналы утечки информации**
- В электромагнитных каналах утечки информации носителем информации являются различного вида побочные электромагнитные излучения (ПЭМИ), возникающие при работе технических средств, а именно:
 - побочные электромагнитные излучения, возникающие вследствие протекания по элементам ТСОИ и их соединительным линиям переменного электрического тока;
 - побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав ТСОИ;
 - побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСОИ.

Электрические каналы утечки информации

•

Причинами возникновения электрических каналов утечки информации являются наводки информационных сигналов, под которыми понимаются токи и напряжения в токопроводящих элементах, вызванные побочными электромагнитными излучениями, емкостными и индуктивными связями [2].

Наводки информационных сигналов могут возникать:

- в линиях электропитания ТСОИ;
- в линиях электропитания и соединительных линиях ВТСС;
- цепях заземления ТСОИ и ВТСС;
- посторонних проводниках (металлических трубах систем отопления, водоснабжения, металлоконструкциях и т. д.).

Специально создаваемые технические каналы утечки информации

- Наряду с пассивными способами перехвата информации, обрабатываемой ТСОИ, рассмотренными выше, возможно использование и активных способов, в частности способа «высокочастотного облучения» (рис. 13 и 14), при котором ТСОИ облучается мощным высокочастотным гармоническим сигналом (для этих целей используется высокочастотный генератор с направленной антенной, имеющей узкую диаграмму направленности). При взаимодействии облучающего электромагнитного поля с элементами ТСОИ происходит модуляция вторичного излучения информационным сигналом. Переизлученный сигнал принимается приемным устройством средства разведки и детектируется.

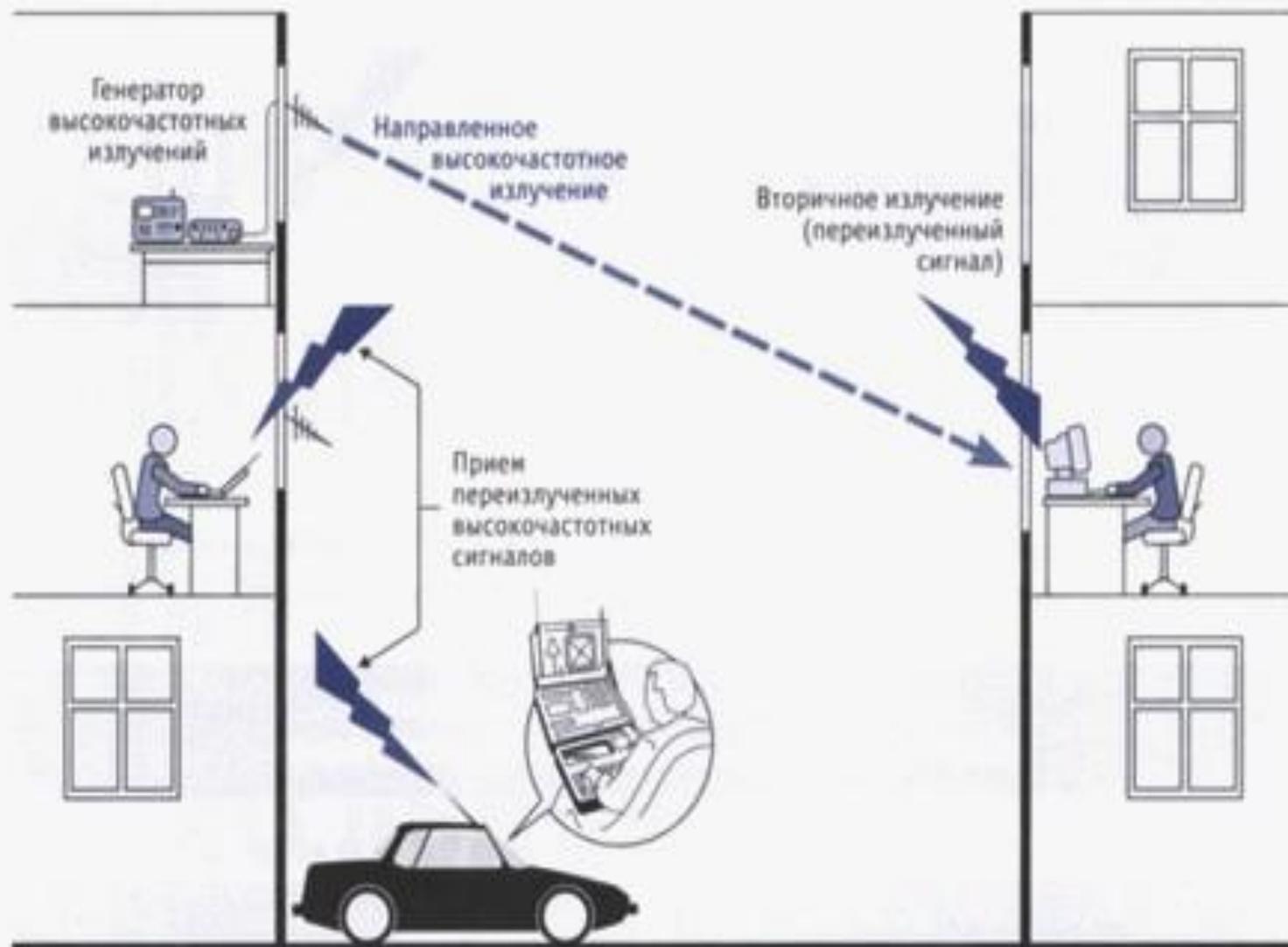


Рис. 13. Перехват информации, обрабатываемой ТСОИ, методом «высокочастотного облучения»

- Для перехвата информации, обрабатываемой ТСОИ, также возможно использование электронных устройств перехвата информации (закладных устройств), скрытно внедряемых в технические средства и системы

- Закладные устройства, внедряемые в ТСОИ, по виду перехватываемой информации можно разделить на:
 - аппаратные закладки для перехвата изображений, выводимых на экран монитора;
 - аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ;
 - аппаратные закладки для перехвата информации, выводимой на периферийные устройства (например, принтер);

Электронные устройства для поиска устройств перехвата информации

- Для поиска радиозакладок в сложной электромагнитной обстановке (например, в городах с множеством радиоэлектронных средств) используются индикаторы поля ближней зоны (дифференциальные индикаторы поля). Такие индикаторы поля измеряют не абсолютное значение напряженности электромагнитного поля, а разность значений напряженности поля в двух близлежащих точках или скорость ее изменения.

Принцип работы приборов основан на особенностях распространения электромагнитного поля в ближней и дальней зонах. В дальней зоне напряженность электрической составляющей электромагнитного поля убывает обратно пропорционально расстоянию до источника излучения, в ближней зоне - обратно пропорционально квадрату расстояния до источника излучения.

- Другим методом идентификации сигнала, источник которого находится в ближней зоне, является сравнение уровней сигналов, принимаемых магнитной и электрической антеннами. Метод основан на особенностях распространения в ближней зоне электрической и магнитной составляющих электромагнитного поля. В ближней зоне магнитная составляющая электромагнитного поля убывает обратно пропорционально кубу расстояния от источника сигнала ($H \sim 1/r^3$), а электрическая составляющая - обратно пропорционально квадрату расстояния от источника сигнала ($E \sim 1/r^2$).

Идентификаторы поля

- По назначению индикаторы поля можно разделить на поисковые, сторожевые (пороговые) и комбинированные
- ***Поисковые индикаторы поля*** предназначены для выявления (писка) закладных устройств, внедренных в защищаемые помещения, и выпускаются в обычном исполнении. Отличительными особенностями поисковых приборов являются индикатор уровня сигнала или звуковой генератор с изменяющейся в зависимости от уровня принимаемого сигнала частотой и сравнительно большой динамический диапазон.

Наиболее простые индикаторы поля



*Рис. 3. Индикаторы поля:
bug detector (Grsystem) (а)
и ST-006 (б)*



*Рис. 4. Индикаторы поля:
EH-1 (а) и Protect -1206 (б)*



*Рис. 5. Индикаторы поля:
Sig-Net (а) и Delta V ECM (б)*

- Более сложные индикаторы поля позволяют измерить не только уровень, но и частоту сигнала, а также идентифицировать сигналы типа GSM, DECT, W-LAN, Bluetooth



а *б*
Рис. 6. Индикаторы поля:
РИЧ-3 (а) и РИЧ-8 (б)



а *б*
Рис. 7. Индикаторы поля:
АПП-7М (а) и ST-007 (б)

- ***Сторожевые (пороговые) индикаторы*** поля предназначены для контроля электромагнитной обстановки в выделенных помещениях. При превышении принимаемым сигналом установленного порога индикатор выдает сигнал тревоги (звуковой, вибрационный или световой). Уровень порога устанавливается оператором либо в качестве такового принимается измеренное при включении индикатора поля значение уровня фона



Рис. 10. Подключение сканирующего приемника к радиочастотомеру Scout



а б

Рис. 11. Индикаторы поля, встроенные в корпус пейджера SEL SP-71/М «Оберег» (а) и в авторучку Protect-1205 (б)



а б

Рис. 12. Индикаторы поля, встроенные в картину (а) и в настольные часы (б)



а б

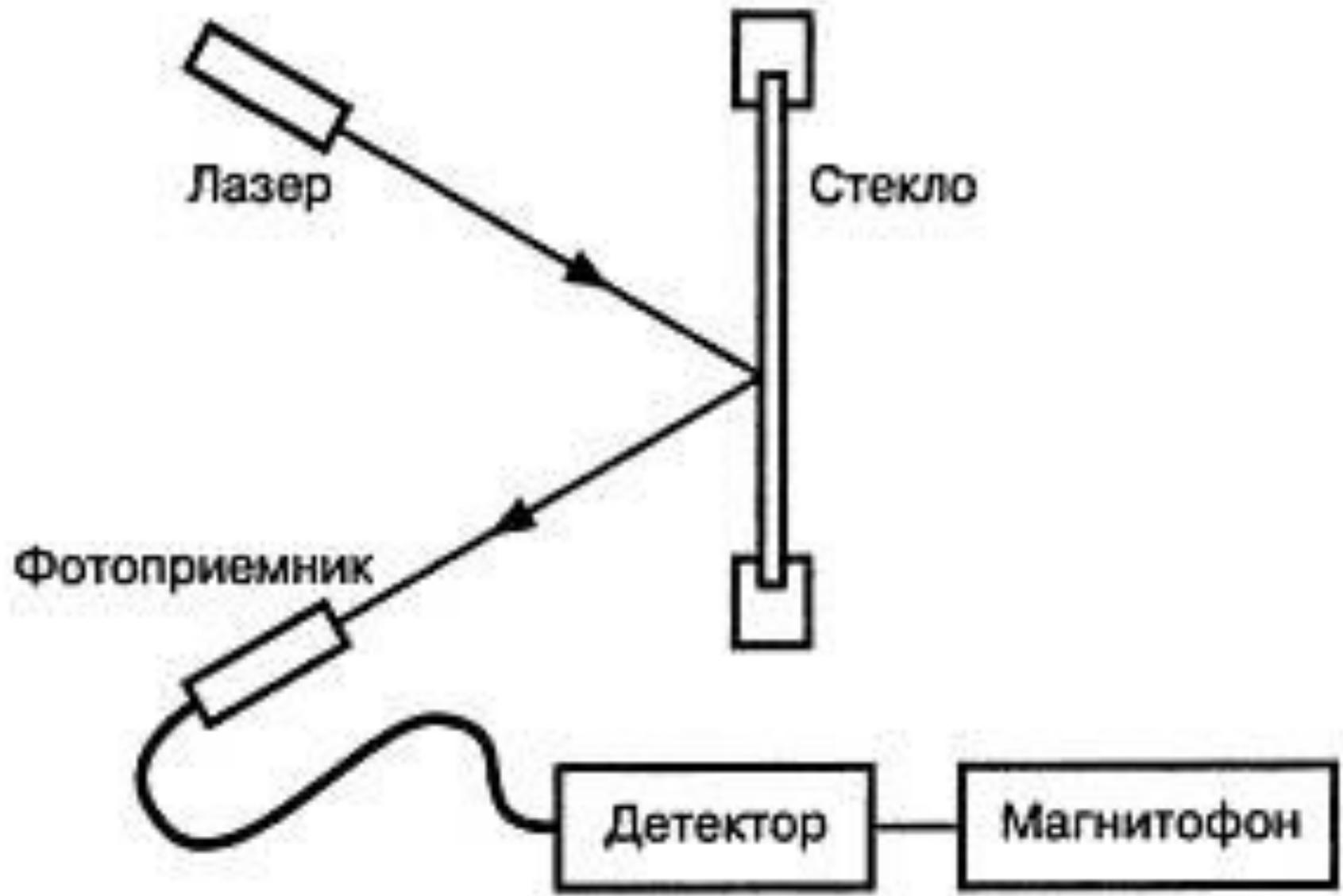
Рис. 13. Индикаторы поля, встроенные в брелоки: «Блик» (а) и «Сигнал-6» (б)

- ***К комбинированным индикаторам*** поля относятся поисковые индикаторы, обладающие сторожевым режимом работы. К ним относятся индикаторы поля

Снятие информации со стекла и борьба с ним

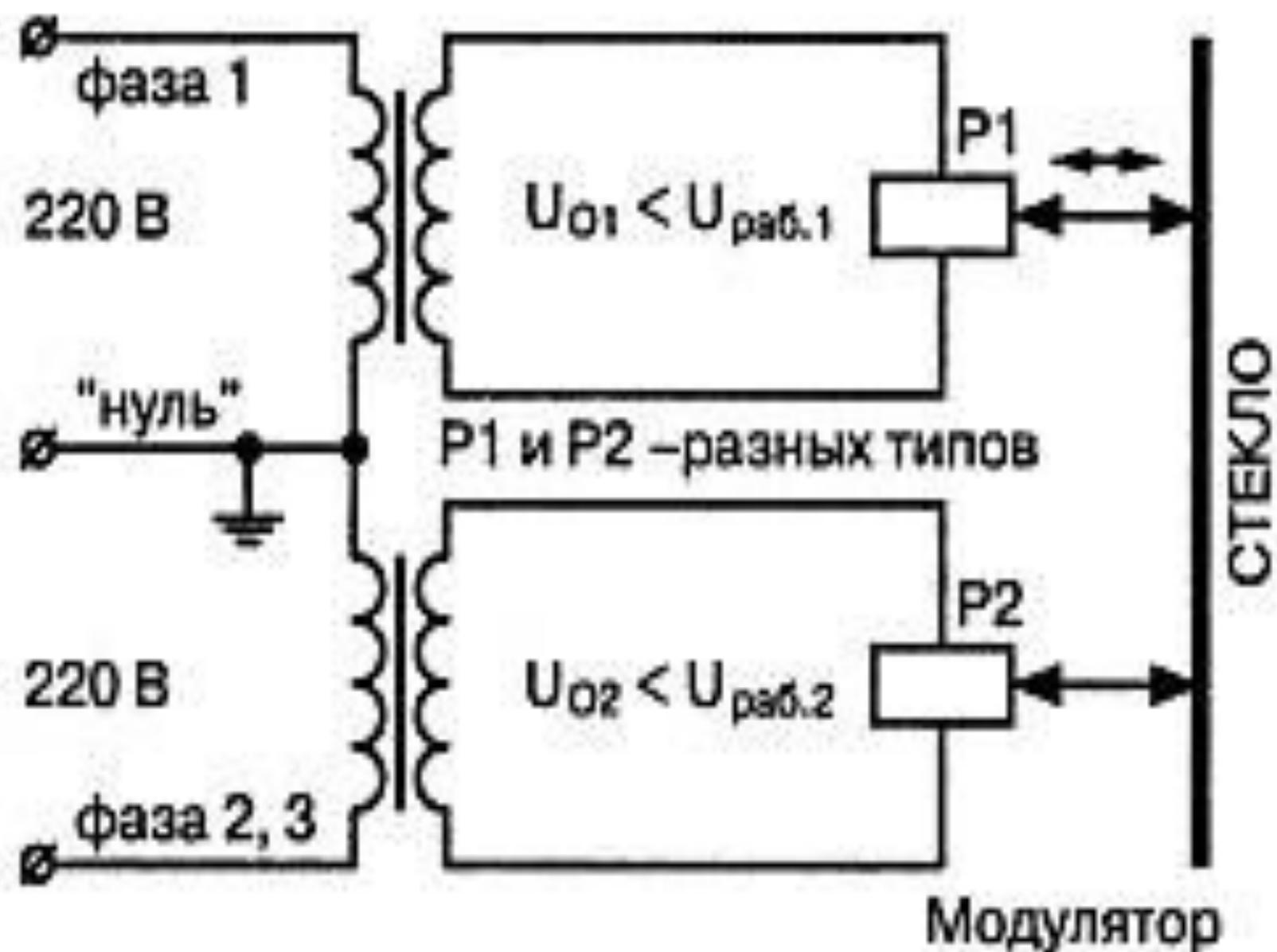
- В последние годы появилась информация, что спецслужбы различных стран для несанкционированного получения речевой информации все чаще используют дистанционные порты средства акустической разведки.
- Самыми современными и эффективными считаются лазер акустической разведки, которые позволяют воспроизводить речь, любые другие звуки и акустические шумы при лазерно-локационном зондировании оконных стекол и других отражающих поверхностей.

- Рассмотрим кратко физические процессы, происходящие при перехвате речи с помощью лазерного микрофона. Зондируемый объект — обычно оконное стекло — представляет собой своеобразную мембрану, которая колеблется со звуковой частотой, создавая фонограмму разговора.
- Генерируемое лазерным передатчиком излучение, распространяясь в атмосфере, отражается от поверхности оконного стекла и модулируется акустическим сигналом, а затем воспринимается фотоприёмником, который и восстанавливает разведываемый сигнал.



простая схема срыва прослушивания

- В качестве модулятора с частотой 50 Гц используется обычное малогабаритное реле постоянного тока РЭС 22, РЭС 9.
- Выводы обмотки подключаются к переменному току напряжением чуть ниже порога срабатывания. Реле жестко крепится к стеклу клеем ЭПД.



Так же можно попробовать совсем элементарную схему для защиты от ЛСАР

- **Примечание**

- Все мы знаем закон физики — «Угол падения равен углу отражения». Это значит, что надо находиться строго перпендикулярно окну прослушиваемого помещения. Из квартиры напротив вы вряд ли поймаете отраженный луч, так как стены здания обычно, я уж не говорю об окнах, немного кривоваты и отраженный луч пройдет мимо.
-
- Перед важным совещанием приоткройте окно, и пока шпионы бегают по соседним зданиям и ищут отраженный луч, вы, наверняка, успеете обсудить все важные моменты, а если менять положение окна каждые 5—10 мин. (приоткрыть, закрыть), то все желание прослушивать вас после такого марафона пройдет

Противодействие электронным приборам утечки речевой информации

- **Глушение** — целенаправленное создание активных помех для ухудшения качества сигнала путём снижения его отношения сигнал/шум. Глушение может быть направлено на определенный узкий диапазон, либо на широкий создавая помехи практически для всех средств связи.
-
- Если для перехвата информации используется устройство считывающее речевую информацию в помещении и передающие информацию по некоторой частоте, например GSM или FM то эффективно будет заглушить широкий диапазон частот в помещении. Так же такая глушилка будет содействовать ускоренному разряду батареи возможных жучков, так как они непрерывно будут пытаться установить сигнал.
-
- Для глушения можно использовать прибор с такой схемой:

Для глушения Fm частот

