Технические каналы утечки информации

Нежелательные излучения технических средств обработки информации (ТСОИ)

Примеры ТСОИ:

- ✔ электронно-вычислительная техника,
- ✔ режимные АТС,
- ✔ системы оперативно-командной и громкоговорящей связи,
- ✔ системы звукоусиления, звукового сопровождения и звукозаписи и т.д.

В цепях различных устройств протекают переменные электрические токи, порождающие электромагнитные поля, излучаемые в окружающее пространство. Структура и параметры электромагнитных полей, создаваемых токоведущими элементами, определяются конструктивными особенностями систем и средств информатизации и связи, а также условиями их размещения и эксплуатации. Такие электромагнитные излучения являются потенциальными носителями опасного сигнала.

Возможные каналы утечки информации образуются:

- низкочастотными электромагнитными полями, возникающими при работе технических средств передачи информации (ТСПИ) и вспомогательных технических средств и систем (ВТСС);
- при воздействии на ТСПИ и ВТСС электрических, магнитных и акустических полей;
- при возникновении паразитной высокочастотной (ВЧ) генерации (паразитные и обратные связи);
- при прохождении информативных (опасных) сигналов в цепи электропитания;
- при взаимном влиянии цепей;
- при прохождении информативных (опасных) сигналов в цепи заземления;
- при паразитной модуляции высокочастотного сигнала;
- вследствие ложных коммутаций и несанкционированных действий.

Информативные (опасные) сигналы могут возникать на элементах технических средств, чувствительных к воздействию:

- электрического поля (неэкранированные провода и элементы технических средств);
- магнитного поля (микрофоны, громкоговорители, головные телефоны, трансформаторы, катушки индуктивности, дроссели, электромагнитные реле);
- акустического поля (микрофоны, громкоговорители, головные телефоны, трансформаторы, катушки индуктивности, дроссели, электромагнитные реле).

При наличии в технических средствах элементов, способных преобразовывать эти поля в электрические сигналы, возможна утечка информации по незащищенным цепям абонентских линий связи, электропитания, заземления, управления, сигнализации.

Побочные излучения ТСОИ могут иметь место в различных участках частотного диапазона. Низкочастотными излучателями электромагнитных колебаний являются, например, усилительные устройства различного функционального назначения. На более высоких частотах наблюдаются излучения гетеродинов радио-приемных устройств, измерительных генераторов, генераторов тактовых частот электронно-вычислительной техники и т.д.

Нежелательные излучения различных устройств могут содержать опасные сигналы. В процессе функционирования технических средств обработки информации элементы генераторов, усилителей и других излучающих электромагнитные поля устройств могут оказаться в зоне действия электромагнитных полей опасных сигналов. Воздействие электромагнитного поля опасного сигнала на рассматриваемые устройства может привести к изменению параметров отдельных элементов генератора или усилителя. Результатом такого изменения является паразитная модуляция опасным сигналом нежелательных излучений технических средств. Следствием этого является появление в окружающем пространстве нежелательных излучений, модулированных опасными сигналами, т.е. создаются предпосылки для утечки информации, обрабатываемой техническими средствами.

В отдельных технических средствах, например в усилительных каскадах, могут возникать паразитные излучения, обусловленные их самовозбуждением за счет паразитных положительных обратных связей. Причины возникновения нежелательных обратных связей в усилителях могут быть различными. Параметры элементов радиоэлектронной аппаратуры — конденсаторов, резисторов, катушек индуктивности, отрезков соединительных линий — вне полосы рабочих частот существенно отличаются от соответствующих параметров на рабочих частотах. Наличие конечной индуктивности выводов элементов, различных паразитных емкостей, проявление свойств цепей с распределенными параметрами, различные межэлементные соединения образуют большое количество паразитных колебательных систем и обратных связей, свойства которых невозможно предусмотреть и учесть заранее.

Причины возникновения нежелательных обратных связей в усилителях можно разделить на две группы.

- ✔ Первая группа причин связана с наличием внутренних обратных связей через усилительный прибор.
- ✔ Ко второй группе относят внешние обратные связи через паразитные индуктивности, емкости, цепи питания, регулировок и т.д.

К таким каналам можно отнести все виды обратной связи между входной и выходной цепями, в пределах каждого отдельного каскада, в пределах двух, трех и более каскадов.

Основные виды внешних обратных связей:

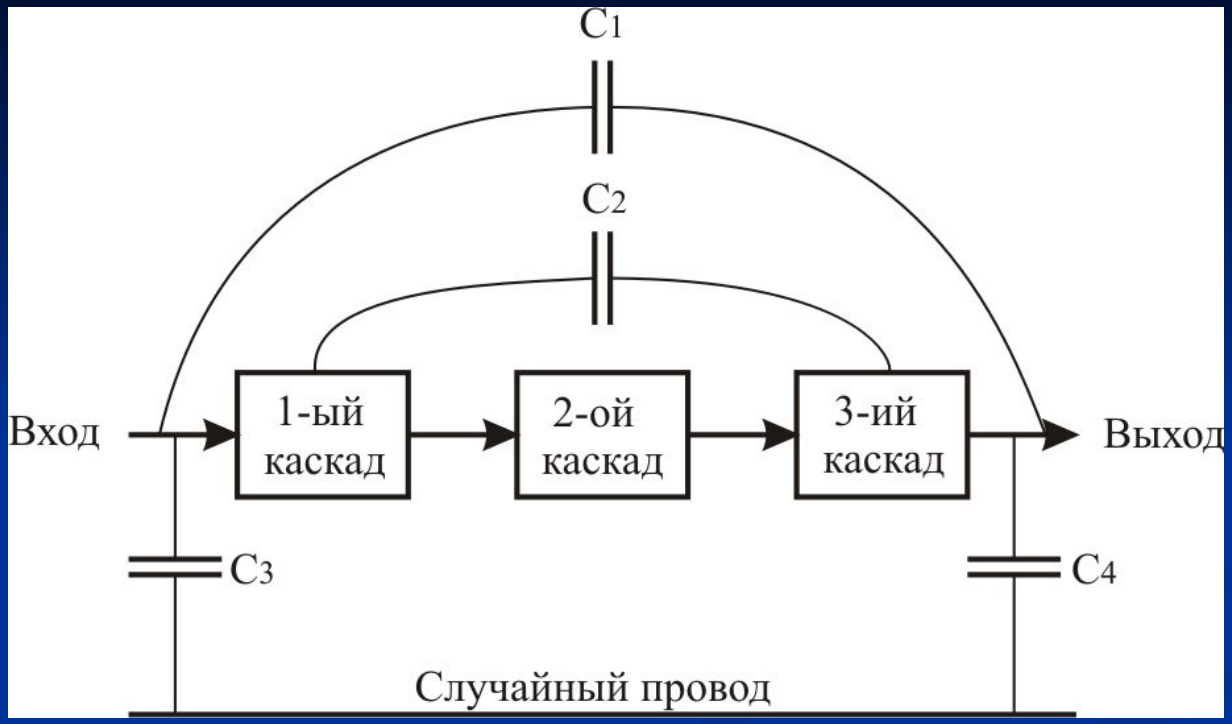
— через взаимоиндуктивности между выходным и входным контурами избирательного усилителя;

— через провода питания активных элементов усилителя;

— через провода регулировок, подключенные к различным точкам усилительных каскадов;

— через шасси и корпус усилителя, являющиеся общим проводом, соединяющим ряд его точек;

— через емкость между выходной и входной цепями усилителя. Этот вид связи имеет место в тех случаях, когда провода входной цепи проходят рядом с проводами выходной цепи (емкость C_1), когда отсутствуют экраны между каскадами или когда они недостаточно экранированы (емкость C_2), когда среди монтажных проводов имеются провода, не имеющие отношения к высокоточным цепям, но связанные с ними емкостями (емкости C_3 и C_4).



Образование паразитной емкостной обратной связи в многокаскадном усилителе

В определенных условиях нежелательная обратная связь может оказаться положительной, а условия самовозбуждения - выполненными. Это приводит к возникновению паразитной генерации устройства на этой частоте, предсказать которую заранее практически невозможно.

Для персонального компьютера **потенциально-информативными** паразитными электромагнитными излучениями (ПЭМИ) являются излучения, формируемые следующими цепями:

- ✔ цепь, по которой передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате;
- ✔ цепи, по которым передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора;
- ✔ цепи, формирующие шину данных системной шины компьютера;
- ✔ цепи, формирующие шину данных внутри микропроцессора, и т. д.

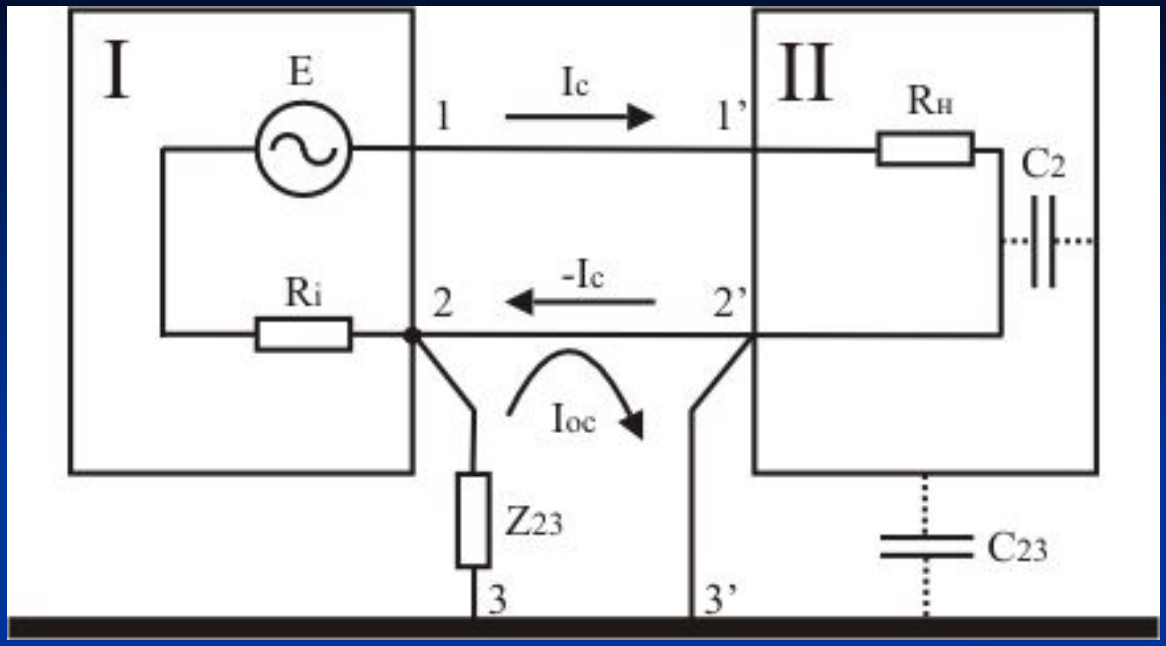
Применение **многоразрядного параллельного кода** в большинстве случаев (в зависимости от разрядности кода, формата представления информации) делает **невозможным** восстановление информации при перехвате ПЭМИ.

Утечка информации по цепям заземления

Заземлением называется преднамеренное соединение объекта с заземляющим устройством, осуществляемое путем создания системы проводящих поверхностей и электрических соединений, предназначенных для выполнения различных функций.

Одной из причин попадания опасного сигнала в систему заземления является наличие электромагнитного поля — носителя опасного сигнала в местах расположения элементов системы. Это электромагнитное поле будет наводить в расположенной поблизости системе заземления ток опасного сигнала.

Проникновение опасного сигнала в цепи заземления может быть связано с образованием так называемых **контуров заземления**. Рассмотрим два устройства, соединенные парой проводников, один из которых является сигнальным, а другой служит для протекания обратных токов.



Образование контуров заземления между двумя устройствами

Пусть возвратный проводник соединен с корпусом первого (I) устройства, а корпус – с землей. Если этот проводник соединен с корпусом второго (II) устройства, также имеющего электрический контакт с землей (соединение 2'-3'), то образуется замкнутый проводящий контур 2-2'-3'-3-2.

Внешнее электромагнитное поле источника опасного сигнала наводит в этом контуре ЭДС, вызывая протекание тока $I_{ос}$, который, в свою очередь, создает на участке 2-3 падение напряжения $U_{ос}$ (опасного сигнала) равное:

$$U_{ос} = I_{ос} \cdot Z_{23}$$

где Z_{23} — сопротивление участка цепи 2-3.

Если отсутствует проводник 2'-3' или соединение проводника 2-2' с корпусом второго устройства, то возможность образования контура заземления полностью не исключается. В этих случаях контур может состоять из проводников 2-2', 3-3', земляной шины и паразитных емкостей между сигнальной цепью и корпусом второго устройства C_2, а также между корпусом второго устройства и землей C_{23}.

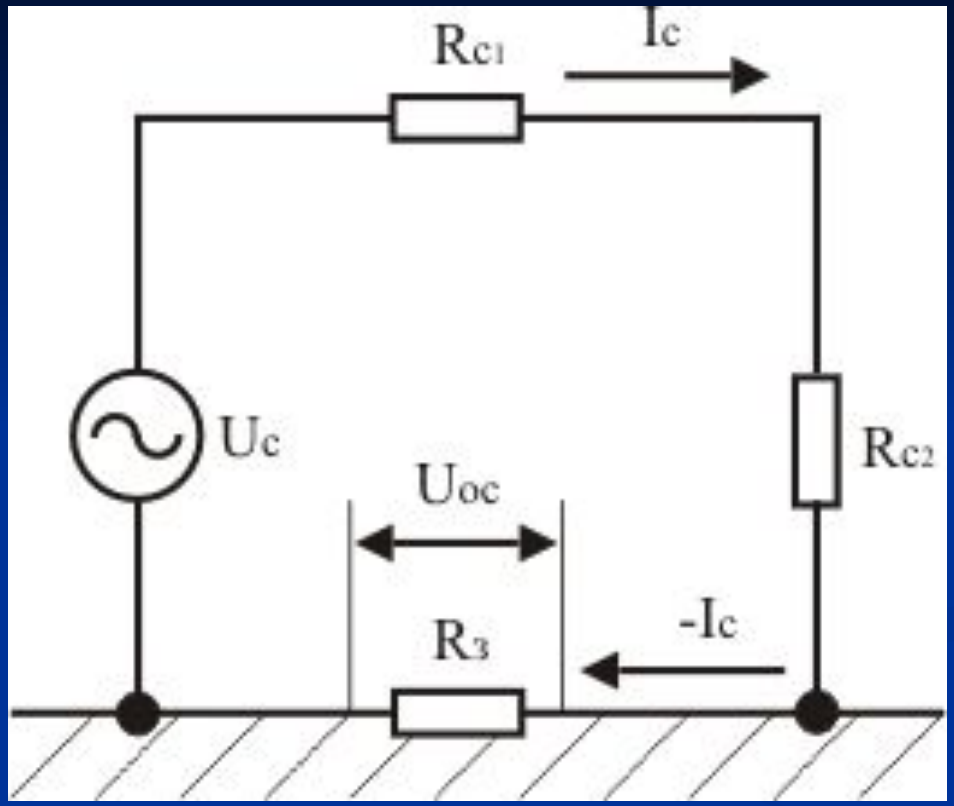
Еще одна причина появления опасного сигнала в цепи заземления связана с конечным значением величины сопротивления заземляющих проводников. По заземляющему проводнику протекает обратный электрический ток опасного сигнала.

Из-за конечного сопротивления $R_З$ земляной шины на этом сопротивлении создается падение напряжения:

$$U_{ос} = \frac{U_в \cdot R}{R_{С1} + R_{С2} + R}$$

где $U_С$ – напряжение источника сигнала; $R_{С1}$, $R_{С2}$ — внутреннее сопротивление источника сигнала и сопротивление нагрузки соответственно.

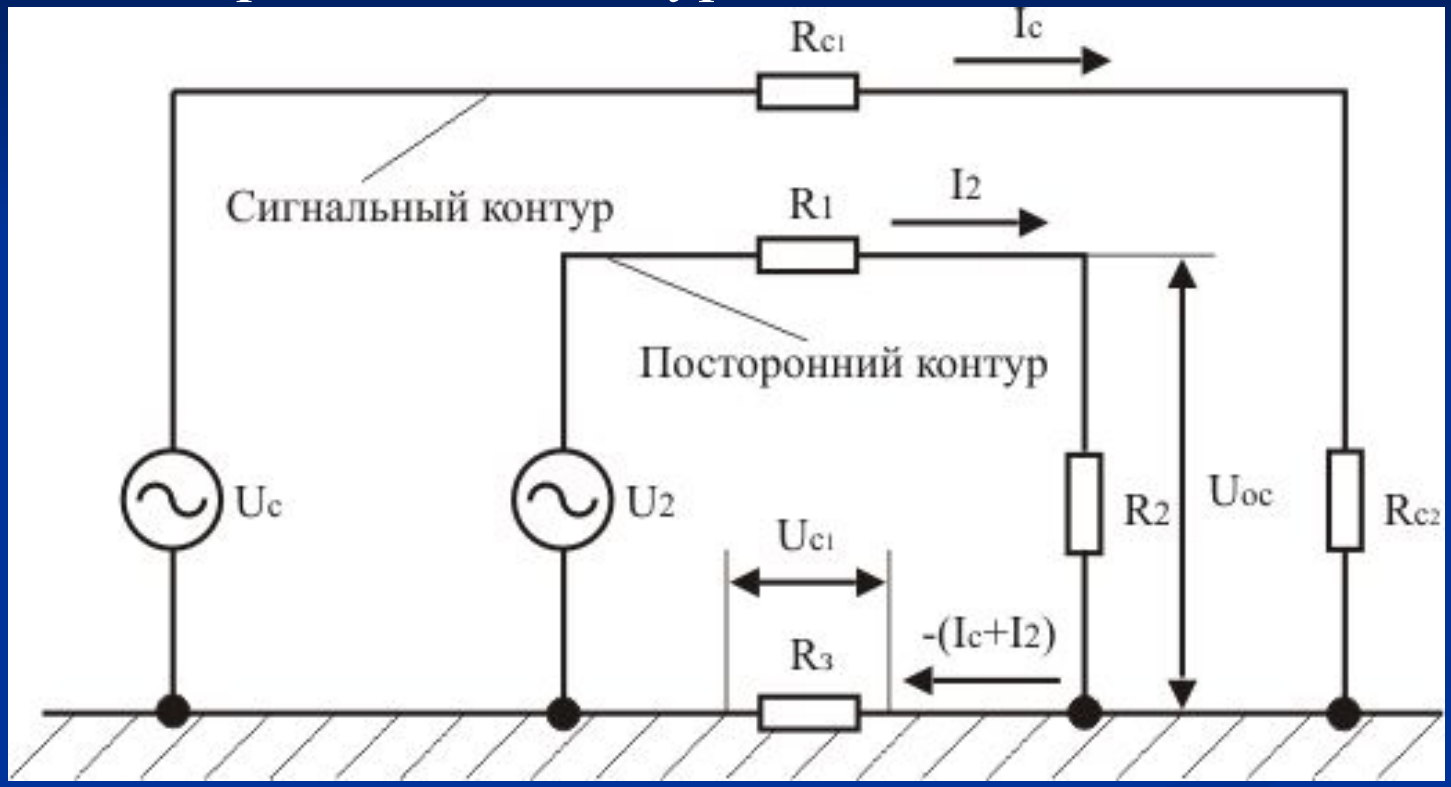
$$При \;\; R_{С1} + R_{С2} >> R \qquad U_{ос} = \frac{U_в \cdot R}{R_{С1} + R_{С2}}$$



Утечка информации за счет падения напряжения на сопротивлении заземляющего устройства.

Напряжение опасного сигнала в цепи заземления будет тем больше, чем больше величина сопротивления R_3

Утечка информации по цепям заземления может также происходить вследствие того, что общая земля служит обратным проводом для различных контуров.



В этом случае для двух различных контуров — сигнального и постороннего — общая земля является обратным проводом с эквивалентным сопротивлением $R_З$.

На эквивалентном сопротивлении земли R_3 возникает падение напряжения за счет протекания обратного тока опасного сигнала I_C, равное:

$$U_{C1} = \frac{U_C \cdot R_3}{R_{C1}^{C1} + R_{C2}^{C2} + R_3} \approx \frac{U_C \cdot R_3}{R_{C1} + R_{C2} + R_3}, \text{при } R_3 << R_{C1} + R_{C2}$$

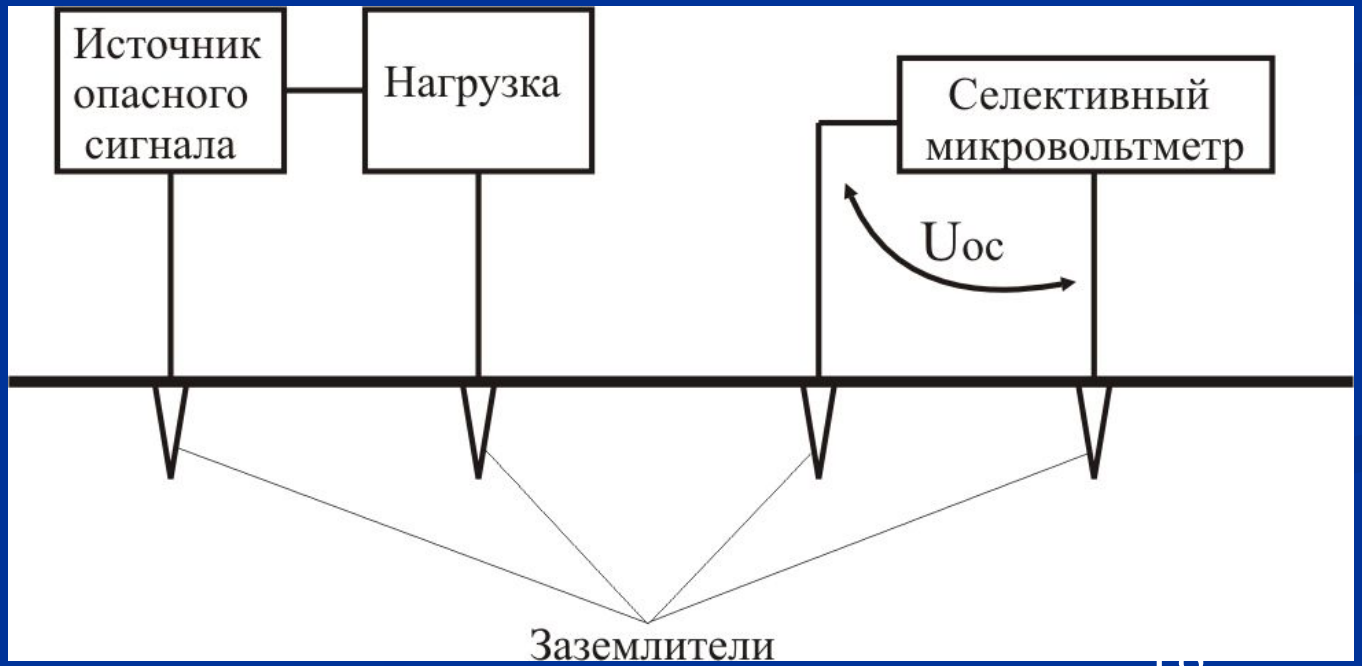
где R_{C1}, R_{C2} — внутреннее сопротивление источника опасного сигнала U_C и сопротивление нагрузки в цепи сигнального контура.

На сопротивлении нагрузки R_2 постороннего контура имеет место падение напряжения U_{OC}, вызванное протеканием обратного тока опасного сигнала - I_C по общей цепи заземления, которое равно:

$$U_{oc} = \frac{U_{C1} \cdot R_2}{R_1 + R_2}, \text{при } R_3 << R_1 + R_2$$

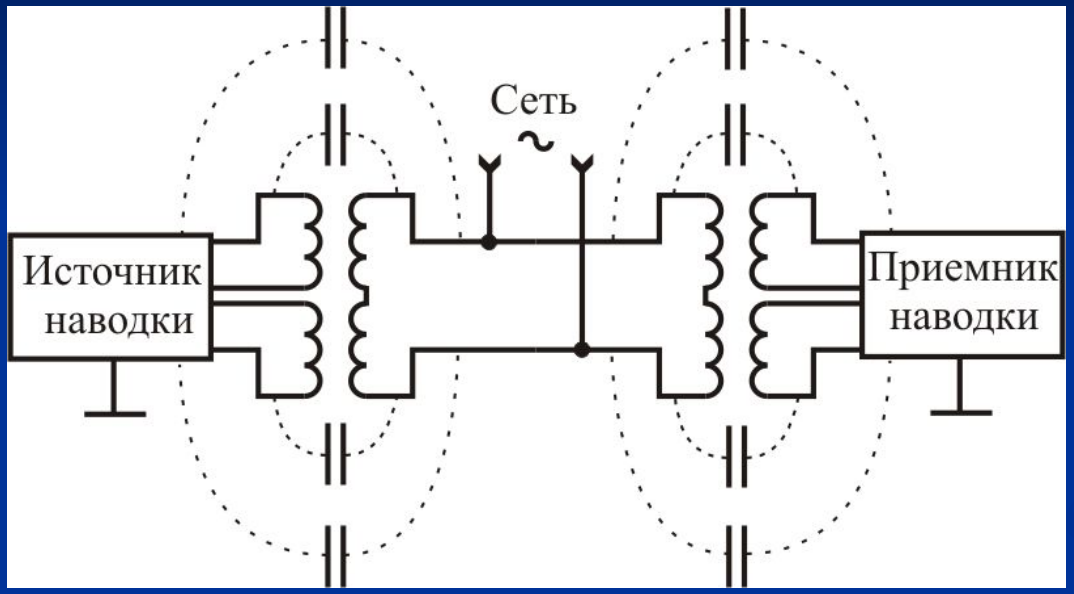
где R_1 — внутреннее сопротивление источника напряжения U_2 в цепи постороннего контура.

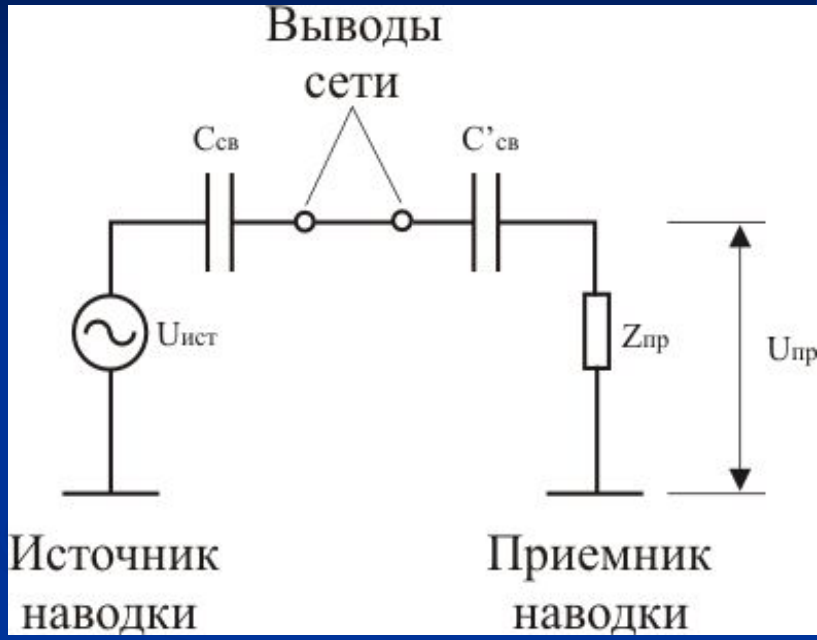
Возможность утечки информации, связанная с цепями заземления, обусловлена также наличием электромагнитного поля опасного сигнала в грунте вокруг заземлителя. Из-за большого затухания, вносимого грунтом, магнитное поле в землю практически не проникает. Электрическое поле в земле определяется величиной потенциала заземлителя и параметрами грунта, где происходит растекание тока опасного сигнала. С помощью дополнительных заземлителей можно осуществить перехват опасного сигнала.



Утечка информации по цепям электропитания

Как правило, провода общей сети питания распределяются по различным помещениям, где расположены технические системы, и соединены с различными устройствами. Вследствие этого образуется нежелательная связь между отдельными техническими средствами. Кроме того, провода сети питания являются линейными антеннами, способными излучать или воспринимать электромагнитные поля. На практике значительная часть нежелательных наводок между удаленными друг от друга устройствами происходит с участием сети питания. При этом возможны различные ситуации. В случае асимметричной наводки, когда провода сети питания прокладываются вместе и имеют одинаковые емкости относительно источников и приемников наводки, в них наводятся напряжения, одинаковые по величине и по фазе относительно земли и корпуса приборов.

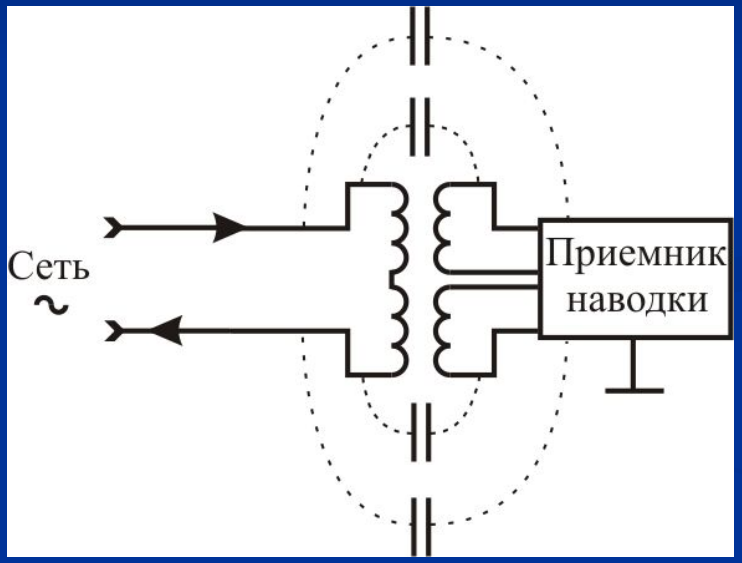




Действительная Эквивалентная

Схемы нежелательной асимметричной связи двух устройств

Симметричное распространение наводки имеет место в тех случаях, когда на проводах сети индуцируются различные напряжения относительно земли. Тогда между проводами образуется высокочастотная разность потенциалов, и по проводам сети проходят токи наводки в разных направлениях.



Вследствие этого в приемнике наводки индуцируются равные по величине обратные по знаку напряжения. Поэтому симметрично распространяющаяся наводка не может проникнуть в высокочастотную часть приемника наводки.

Проникновение симметричной наводки через силовой трансформатор путем передачи напряжения, наведенного в первичной обмотке, во вторичную маловероятно вследствие существенных отличий частот сети питания и сигнала наводки. Симметричное распространение наводки опасно только при асимметрии приемника наводки относительно проводов сети питания. Например, если в один из проводов сети питания ввести предохранитель, то провода сети будут иметь разные емкости относительно приемника наводки. Через них будут передаваться напряжения, разность которых приведет к наводке в приемнике.

При наличии в составе технических средств усилительных каскадов токи усиливаемых в них сигналов замыкаются через вторичный источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, изменяющееся в соответствии с законом изменения усиливаемого (опасного) сигнала.

При недостаточном затухании в фильтре источника питания это напряжение может быть обнаружено в питающей линии.

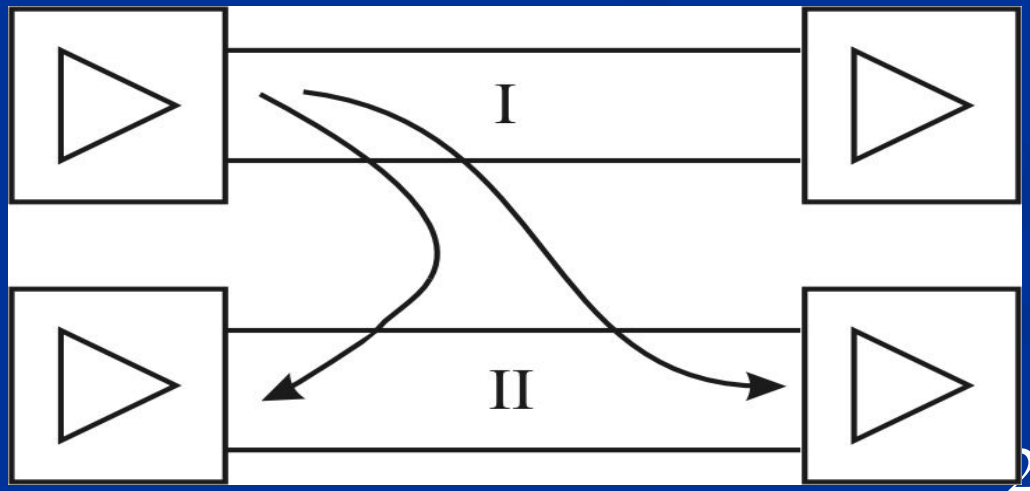
Взаимные влияния в линиях связи

С целью рассмотрения результатов влияния друг на друга параллельно проложенных линий связи приняты следующие основные определения:

— влияющая цепь — цепь, создающая первичное влияющее электромагнитное поле (цепь I);

— цепь, подверженная влиянию, — цепь, на которую воздействует влияющее электромагнитное поле (цепь II*);*

— непосредственное влияние — сигналы, индуцированные непосредственно электромагнитным полем влияющей цепи, в цепи, подверженной влиянию.



В зависимости от структуры влияющего электромагнитного поля и конструкции цепи, подверженной влиянию, различают влияния:

- ✔ систематические
- ✔ случайные.

К систематическим влияниям относятся взаимные наводки, возникающие по всей длине линии.

К случайным относятся влияния, возникающие вследствие ряда случайных причин и не поддающиеся точной оценке.

Существуют реальные условия наводок с одного неэкранированного провода на другой, параллельный ему провод той же длины, когда оба они расположены над "землей".

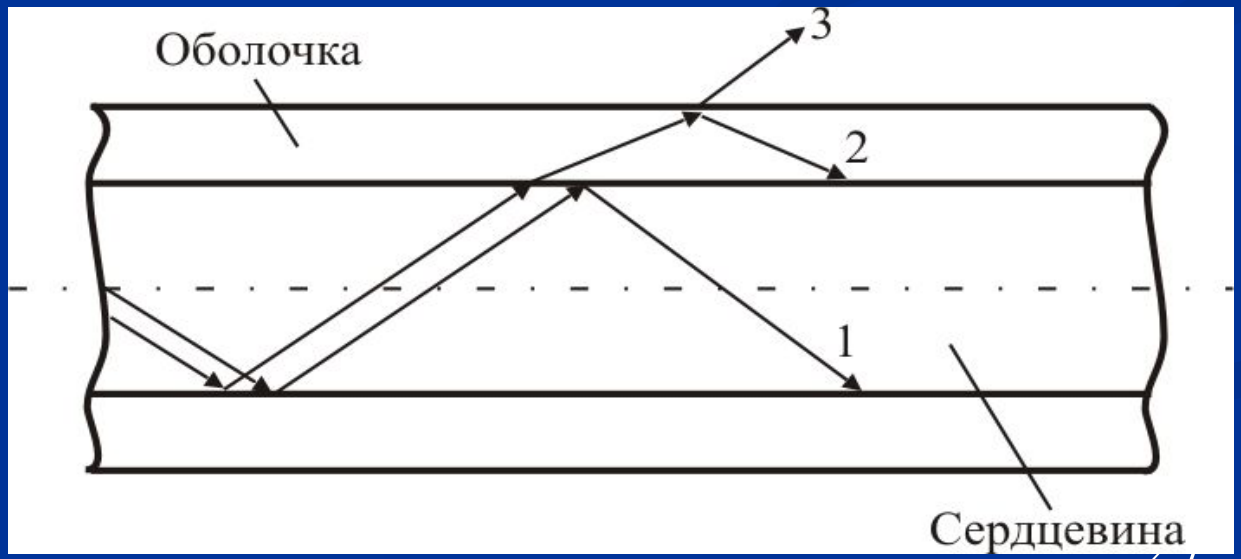
Тип линии	Преобладающее влияние	Меры защиты
Воздушные линии связи	Систематическое влияние, возрастающее с увеличением частоты	Скрещивание цепей оптимальное расположение цепей
Коаксиальный кабель	Систематическое влияние через третьи цепи (ослабляется с повышением частоты)	Экранирование и ограничение диапазона рабочих частот снизу
Симметричный кабель	Систематическое и случайное влияние, возрастающее с частотой	Оптимизация шагов скрутки кабеля, экранирование
Оптический кабель	Систематическое и случайное влияние (от частоты сигнала практически не зависит)	Экранирование оптических волокон, пространственное разделение

Утечка информации в волоконно-оптических линиях связи

Основные причины утечки информации в волоконно-оптических линиях связаны с излучением световой энергии в окружающее пространство. Причины этого излучения обусловлены процессами, происходящими при вводе (выводе) излучения в оптический волновод и распространении волн в диэлектрическом волноводе. Кроме того, утечка информации за счет оптического излучения может иметь место из-за наличия постоянных и разъемных соединений оптических волокон, а также изгибов и повреждений этих волокон.

Рассеивание излучения при вводе оптического сигнала в волновод связано с тем, что пучок излучения источника имеет заметно большую ширину, чем толщина сердцевины волновода. Увеличение эффективности ввода излучения достигается применением оптического клея, микролинз и других средств фокусировки излучения.

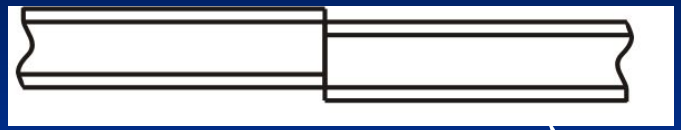
В диэлектрическом волноводе толщиной порядка длины распространяющейся в нем волны (l-10 мкм) в зависимости от соотношения показателей преломления волноводного слоя (сердцевины), оболочки и покровного слоя, а также от угла падения световой волны на границе раздела волна может либо распространяться вдоль волокна путем многократных отражений от границы сердцевина—оболочка (луч 1), либо проникать в оболочку, распространяться вдоль нее и далее выходить в окружающую среду (лучи 2, 3).



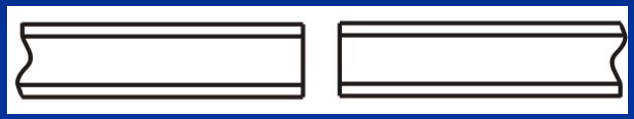
В прямолинейных световодах излучение в окружающую среду незначительно. Однако в местах изгибов волноводов интенсивность излучения в оболочку или воздух увеличивается, и тем больше, чем сильнее эти изгибы. Интенсивность излучения в окружающее пространство увеличивается и при повреждении оболочки световода.

Постоянные соединения отрезков оптических волокон между собой осуществляют свариванием, сплавлением или склеиванием в юстировочном устройстве. Оптические разъемы (соединители) должны допускать многократные соединения—разъединения оптических волокон. Рассогласование волокон возникает из-за имеющихся различий в числовой апертуре, профиле показателя преломления, диаметре сердцевины или из-за погрешностей во взаимной ориентации волокон при их соединении.

Основными причинами излучения световой энергии в окружающее пространство в местах соединения оптических волокон являются:

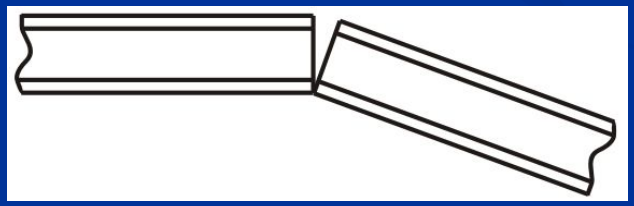


— смещение (осевое несовмещение) стыкуемых волокон

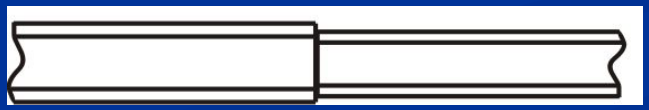


— наличие зазора между торцами стыкуемых волокон

— непараллельность торцевых поверхностей волокон



— угловое рассогласование осей стыкуемых волокон



— различие в диаметрах стыкуемых волокон

Наиболее интенсивное излучение в окружающее пространство наблюдается при наличии сдвига соединяемых волокон относительно друг друга.

Еще одна причина утечки информации в волоконно-оптических линиях может быть связана с возможным воздействием внешнего акустического поля (поля опасного сигнала) на волоконно-оптический кабель. Звуковое давление акустической волны может вызвать изменение геометрических размеров (толщины) или смещение соединяемых концов световодов в разъемном устройстве относительно друг друга. Вследствие этого может осуществляться амплитудная модуляция опасным сигналом излучения, проходящего по волокну. Глубина модуляции определяется силой звукового давления, конструкцией и свойствами волокна.

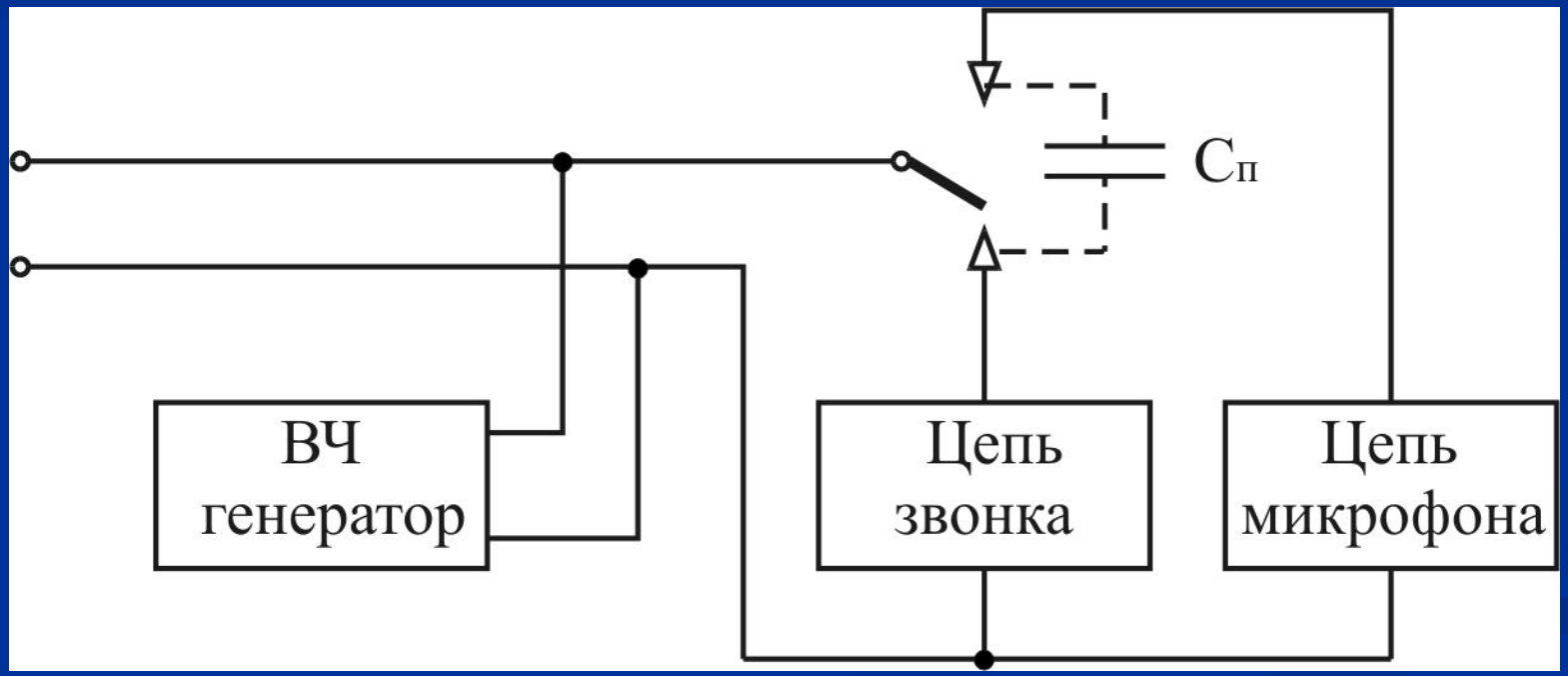
Высокочастотное навязывание

Перехват обрабатываемой техническими средствами информации может осуществляться путем специальных воздействий на элементы технических средств. Одним из методов такого воздействия является высокочастотное навязывание, т.е. **воздействие на технические средства высокочастотных сигналов**. В настоящее время используются два способа высокочастотного навязывания:

1. Посредством контактного введения высокочастотного сигнала в электрические цепи, имеющие функциональные или паразитные связи с техническим средством.
2. Путем излучения высокочастотного электромагнитного поля.

Возможность утечки информации при использовании высокочастотного навязывания связана с наличием в цепях технических средств нелинейных или параметрических элементов. Навязываемые высокочастотные колебания воздействуют на эти элементы одновременно с низкочастотными сигналами, возникающими при работе этих средств и содержащими конфиденциальные сведения. В результате взаимодействия на таких элементах высокочастотные навязываемые колебания оказываются промодулированными низкочастотными опасными сигналами. Распространение высокочастотных колебаний, модулированных опасными сигналами, по токоведущим цепям или излучение их в свободное пространство создают реальную возможность утечки закрытой информации.

Схема иллюстрирует принцип реализации высокочастотного навязывания в телефонном аппарате при положенной микротелефонной трубке (т.е. в ситуации, когда телефонный разговор не ведется и цепь питания микрофона разомкнута).



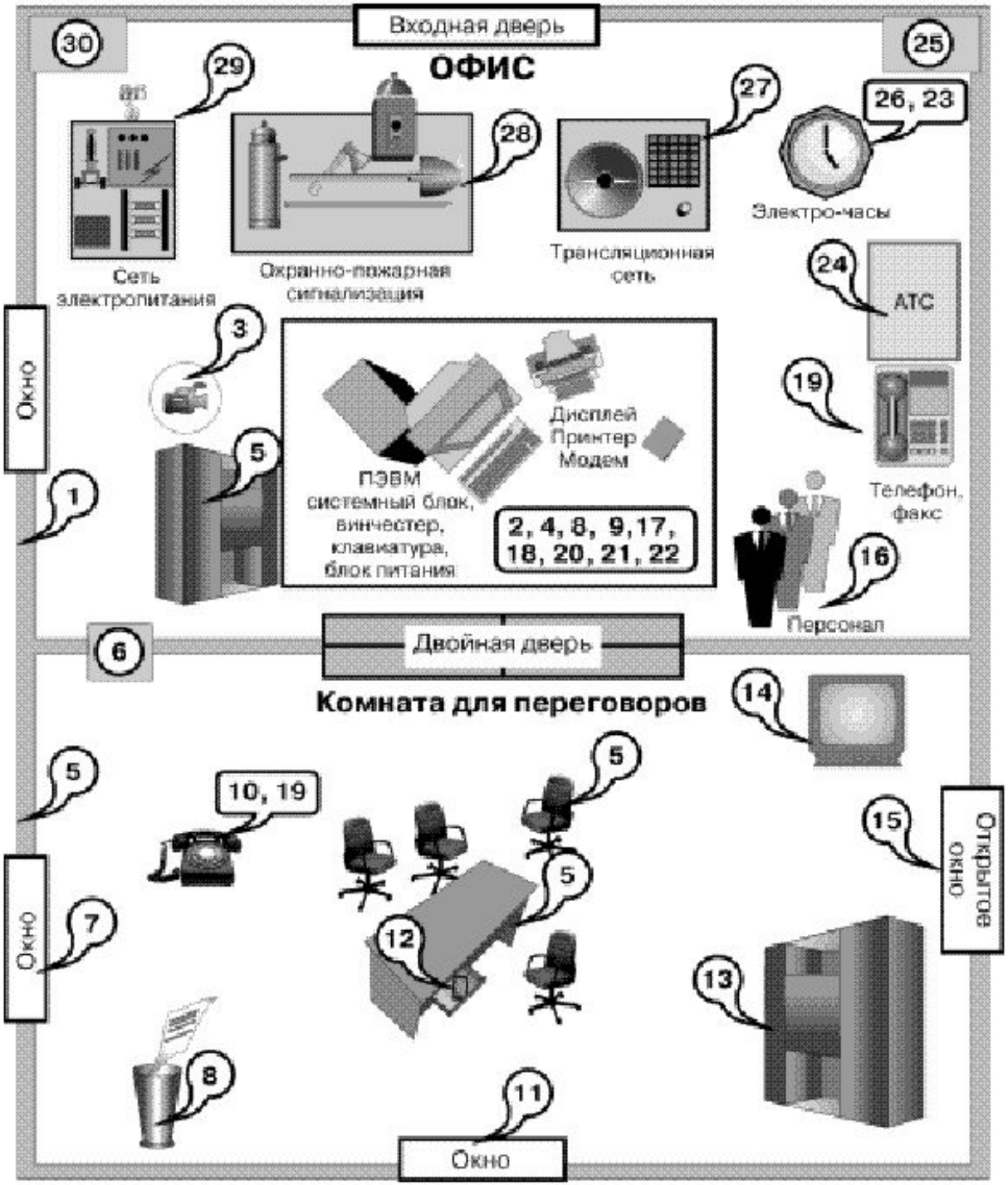
Принцип реализации высокочастотного навязывания в телефонном аппарате

В рассматриваемом случае в телефонную линию подаются от специального высокочастотного генератора высокочастотные колебания с частотой более 100 кГц. Низкочастотные (опасные) сигналы формируются в телефонном аппарате на элементах, обладающих свойствами электроакустических преобразователей (звонок, микрофон и т.д.), которые преобразуют акустические сигналы (разговорную речь в помещении, где расположен телефонный аппарат) в электрические.

Несмотря на то, что цепь микрофона телефонного аппарата разомкнута рычажным переключателем, между цепью микрофона и выходом линии существует паразитная емкость $C_п$ порядка 5-15 пФ. На достаточно высоких частотах емкостное сопротивление этого переключателя будет относительно невысоким, поэтому навязываемые высокочастотные колебания через емкость $C_п$ будут приложены к микрофону.

Если в это время на микрофон действует достаточное звуковое давление опасного сигнала, обусловленное ведением разговоров в помещении, где расположен телефонный аппарат, то на выходе микрофона появится напряжение опасного сигнала. Происходит модуляция высокочастотных колебаний опасным речевым сигналом. Аналогичные явления наблюдаются и в звонковой цепи телефонного аппарата.

Излучение высокочастотных колебаний, промодулированных опасным сигналом, в свободное пространство осуществляется с помощью случайной антенны — телефонного провода. Промодулированный высокочастотный сигнал распространяется также в телефонной абонентской линии за пределы контролируемой территории. Следовательно, прием высокочастотных колебаний можно осуществлять либо путем подключения приемного устройства к телефонной линии, либо по полю.


Входная дверь
ОФИС
30
25
29
28
27
26, 23
Сеть электропитания
Охранно-пожарная сигнализация
Трансляционная сеть
Электро-часы
24
АТС
Окно
3
5
1
Дисплей
Принтер
Модем
ПЭВМ
системный блок, винчестер, клавиатура, блок питания
2, 4, 8, 9,17, 18, 20, 21, 22
19
Телефон, факс
16
Персонал
6
Двойная дверь
Комната для переговоров
14
5
10, 19
5
5
15
Открытое окно
Окно
7
12
13
8
11
Окно

1. Утечка за счет структурного звука в стенах и перекрытиях;
2. Съем информации с ленты принтера, стертых дискет и т.п.;
3. Съем информации с использованием видео-закладок;
4. Программно-аппаратные закладки в ПЭВМ;
5. Радио-закладки в стенах и мебели;
6. Съем информации по системе вентиляции;
7. Лазерный съем акустической информации с окон;
8. Производственные и технологические отходы;
9. Компьютерные вирусы, логические бомбы и т.п.;
0. Съем информации за счет наводок и "навязывания";
1. Дистанционный съем видео информации (оптика);
2. Съем акустической информации с использованием диктофонов;
3. Хищение носителей информации;
4. Высокочастотный канал утечки в бытовой технике;
5. Съем информации направленным микрофоном;

6. Внутренние каналы утечки информации (через обслуживающий персонал);
7. Несанкционированное копирование;
8. Утечка за счет побочного излучения терминала;
9. Съем информации за счет использования "телефонного уха";
0. Съем с клавиатуры и принтера по акустическому каналу;
1. Съем с дисплея по электромагнитному каналу;
2. Визуальный съем с дисплея и принтера;
3. Наводки на линии коммуникаций и сторонние проводники;
4. Утечка через линии связи;
5. Утечка по цепям заземления;
6. Утечка по сети электрочасов;
7. Утечка по трансляционной сети и громкоговорящей связи;
8. Утечка по охранно-пожарной сигнализации;
9. Утечка по сети электропитания;
0. Утечка по сети отопления, газо- и водоснабжения

Радио-микрофоны (закладки)	Электронные "уши"	Средства перехвата телефонной связи	Средства скрытого наблюдения и поиска	Средства контроля компьютеров и сетей	Средства приема, записи, управления и др.
с автономным питанием	микрофоны с проводами	с непосред-ственным подключением	Оптические	пассивные средства кон-троля монитора	приемники для радиозакладок
с питанием от телефонной сети	электронные стетоскопы	с индукционным датчиком	фотографические	активные средства кон-троля монитора	устройства накопления и записи
с питанием от электросети	направленные микрофоны	с датчиками внутри телефон-ного аппарата	тепловизионные и ночного видения	пассивные сред-ства контроля ши-ны (магистрали)	средства переприема (ретрансляторы)
управляемые дистанционно	лазерные микрофоны	телефонной радиотрансляции	телевизионные	активные средства контроля шины (магистрали)	средства ускоренной передачи
с функцией включения по голосу	микрофоны с передачей по электросети	перехвата сотовой теле-фонной связи	определения местоположения	аппаратные закладки	устройства дистанционного управления
полуактивные	с исполь-зованием микро-фона аппарата	перехвата пейджинговых сообщений	маркирования и целеуказания	программные закладки	источники питания
с накоплением и быстрой передачей	гидроакусти-ческие микрофоны	многоканальног о перехвата	видеозакла-дочные	компьютерные вирусы	вспомогательные и другие средства

Табл. 1. Основные технические средства коммерческой разведки.

N п/п	Действие человека (типовая ситуация)	Каналы утечки информации	Методы и средства получения информации	Методы и средства защиты информации
1	Разговор в помещении или на улице	акустика	подслушивание, диктофон, микрофон, направленный микрофон, полуактивная система	шумовые генераторы, поиск закладок, защитные фильтры, ограничение доступа
		виброакустика	стетоскоп, вибродатчик	
		гидроакустика	гидроакустический датчик	
		акустоэлектроника	радиотехнические спецприемники	
2	Разговор по проводному телефону	акустика	аналогично п. 1	аналогично п.1
		электросигнал в линии	параллельный телефон, прямое подключение, электромагнитный датчик, диктофон, телефонная закладка	маскирование, скремблирование, шифрование
		наводки	радиотехнические спецустройства	спецтехника
3	Разговор по радиотелефону	акустика	аналогично п. 1	аналогично п.1
		электромагнитные волны	радиоприемные устройства	аналогично п.2
4	Документ на бумажном носителе	Наличие	кража, визуально, копирование, фотографирование	ограничение доступа, спецтехника
5	Изготовление документа на бумажном носителе	наличие	аналогично п.4	аналогично п.4
		паразитные сигналы, наводки	специальные радио-технические устройства	экранирование
6	Почтовое отправление	Наличие	кража, прочтение	специальные методы защиты
7	Документ на небумажном носителе	Носитель	хищение, копирование, считывание	контроль доступа, физическая защита, криптозащита
8	Изготовление документа на небумажном носителе	изображение на дисплее	визуально, копирование фотографирование	контроль доступа, криптозащита
		паразитные сигналы, наводки	специальные радиотехнические устройства	
9	Передача документа по каналу связи	электрические и оптические сигналы	несанкционированное подключение, имитация зарегистрированного пользователя	криптозащита