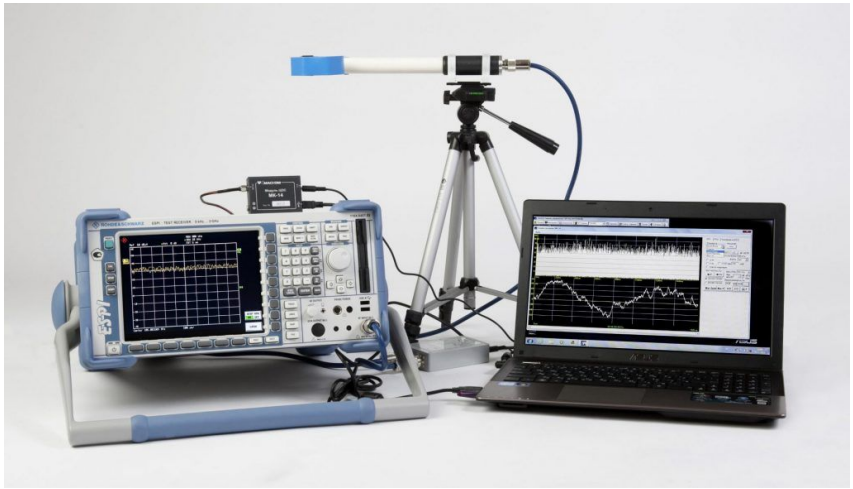
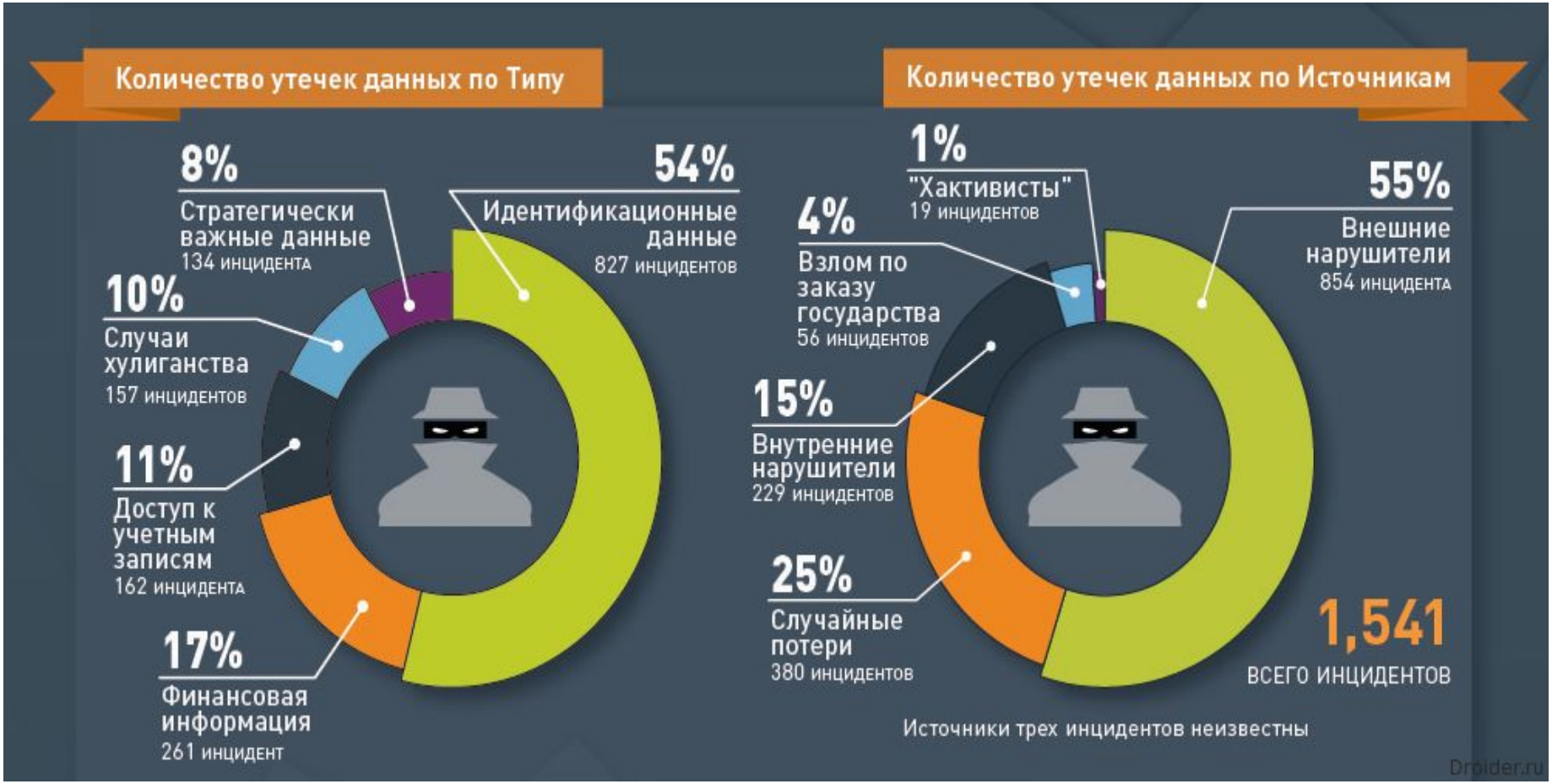
Побочные каналы утечки информации

1. Возможность образования технических каналов утечки информации в системах , средствах информатизации и связи
2. Модель технического канала утечки
3. Определение размеров контролируемой зоны
4. Побочные излучения технических средств обработки информации
5. ПКУИ по цепям заземления
6. Канал утечки по цепям электропитания
7. Виброакустический канал утечки информации
8. Высокочастотное облучение
9. Высокочастотное навязывание
10. Меры защиты от ПКУИ



Литература: Соколов А. В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. – М.: Изд-во «АСТ»; СПб.: Изд-во «Полигон», 2000. – 272 с.



Как утекала информация в 2016 году

Число утечек информации и объем персональных данных, скомпрометированных в результате утечек

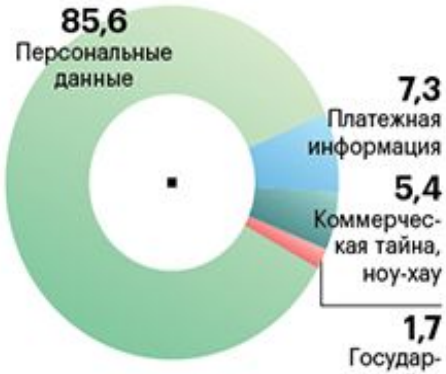
Утечки по вектору воздействия, %

Внутренние утечки по источнику (виновнику), %

Утечки и объем скомпрометированных персональных данных по отраслям

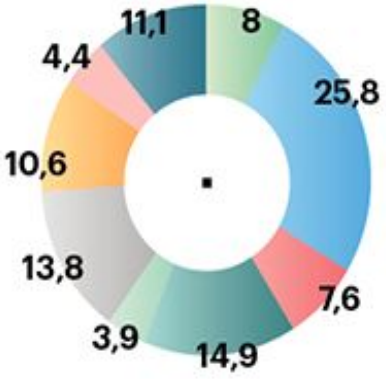
Банки и финансы | Медицина | Торговля, HoReCa | Высокие технологии | Промышленность и транспорт | Госорганы и силовые структуры | Образование | Муниципальные учреждения | Другое/не определено

Утечки по типам данных, %

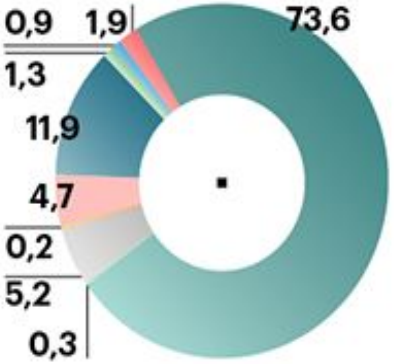


Утечки по каналам, %

Число утечек, %

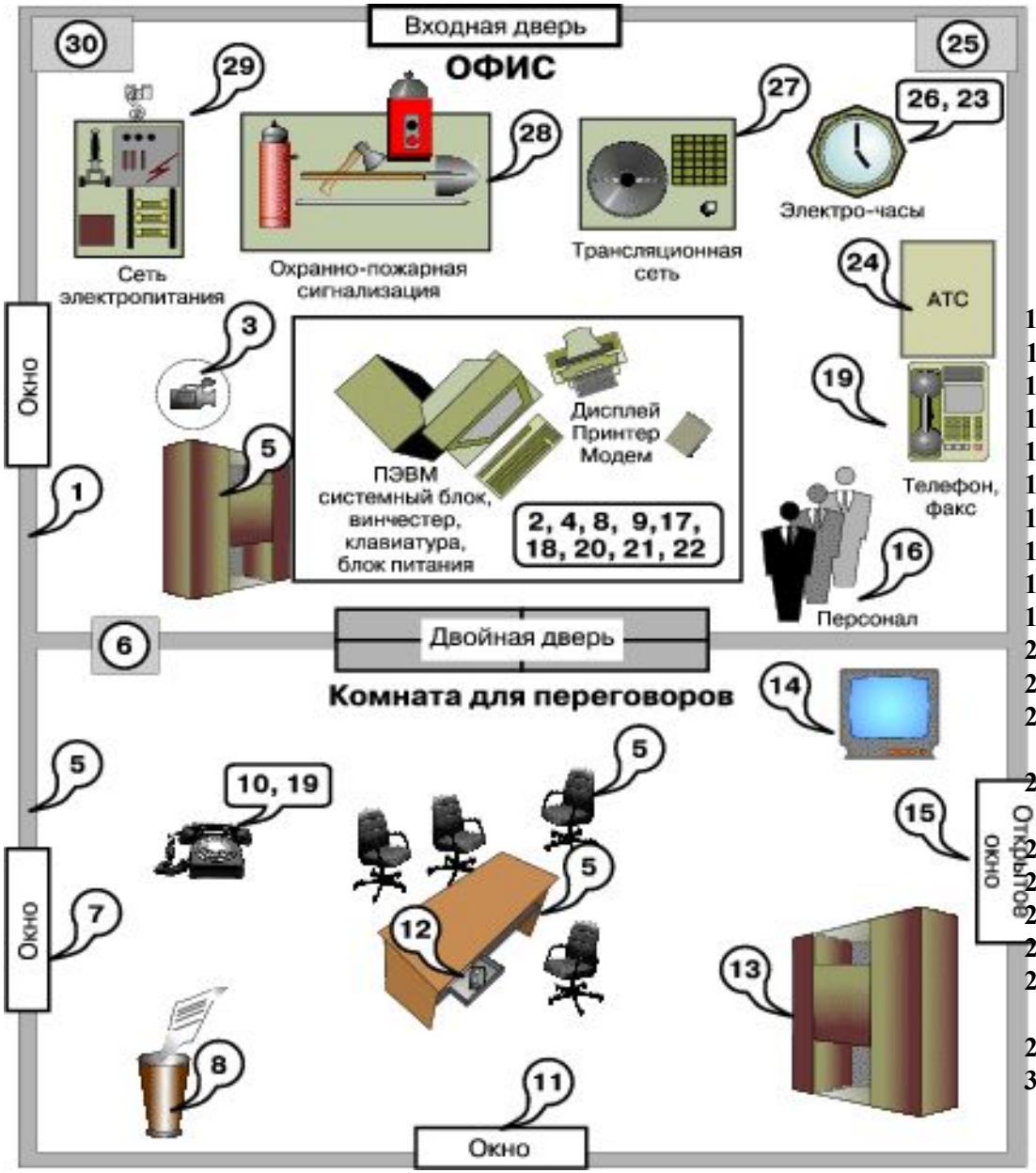


Количество записей, %



Источник: InfoWatch

Возможные каналы утечки информации в офисе

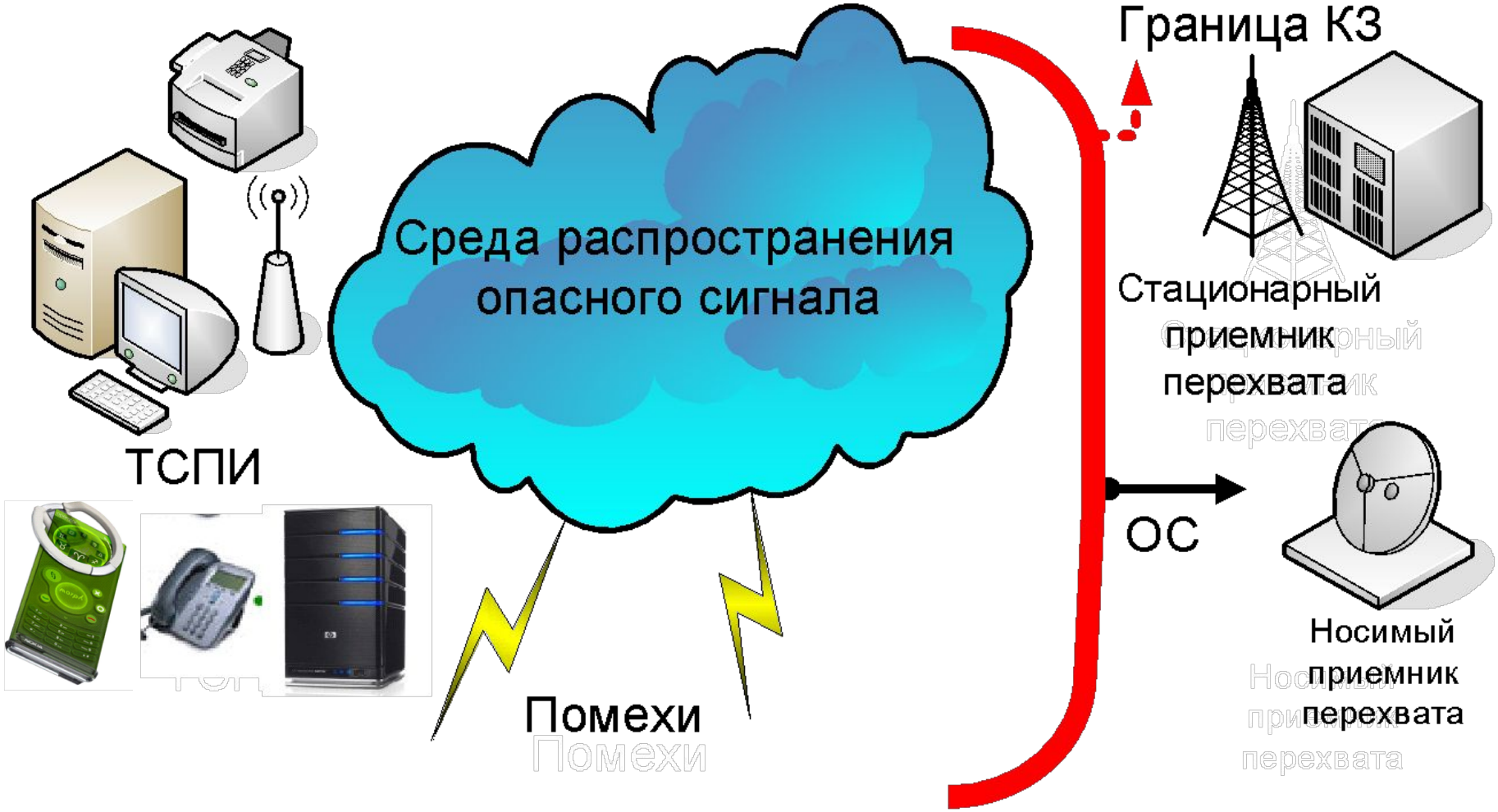


1. Утечка за счет акустических сигналов в стенах и перекрытиях.
2. Съем информации с принтера и носителей.
3. Съем информации с помощью видеозакладок.
4. Программно-аппаратные закладки в ЭВМ.
5. Радиозакладки в стенах и мебели.
6. Съем информации в системе вентиляции.
7. Съем информации с окон.
8. Производственные и технологические отходы.
9. Компьютерные вирусы.
10. Съем информации ПЭМИН и «ВЧ-навязывания»
11. Оптический канал утечки.
12. Запись разговора на диктофон.
13. Хищение носителей информации.
14. Утечка за счет бытовой техники.
15. Утечка за счет направленного микрофона.
16. Утечка при помощи персонала.
17. Несанкционированное копирование.
18. ПЭМИН терминала.
19. Съем информации за счет «телефонного уха».
20. Съем информации с клавиатуры и принтера.
21. Съем информации с монитора.
22. Визуальный съем информации с монитора и принтера.
23. Наводки на линии коммуникаций и сторонние проводники.
24. Утечка через линии связи.
25. Утечка по цепям заземления.
26. Утечка по сети электрочасов.
27. Утечка по трансляционной сети и ГГС.
28. Утечка по цепям охранно-пожарной сигнализации.
29. Утечка по цепям электропитания.
30. Утечка по сетям отопления, газо-и водоснабжения.

Возможность образования технических каналов утечки информации в системах , средствах информатизации и связи обусловлена следующими причинами:

1. **Наличием информационных** радио-, оптических и электрических **сигналов** в различных технических средствах передачи и обработки информации.
2. Наличием **побочных электромагнитных излучений** систем и средств информатизации и связи.
3. Образованием **наводок** электромагнитных излучений **на** различные **токоведущие цепи и конструкции.**.
4. Применением **специальных воздействий** на элементы технических средств.
5. Применением различных **закладных устройств.**.
6. Возникновением и распространением в окружающей среде **акустических колебаний при обсуждении вопросов**, содержащих секретные сведения.
7. Наличием **случайных электроакустических преобразователей** в отдельных элементах технических средств.

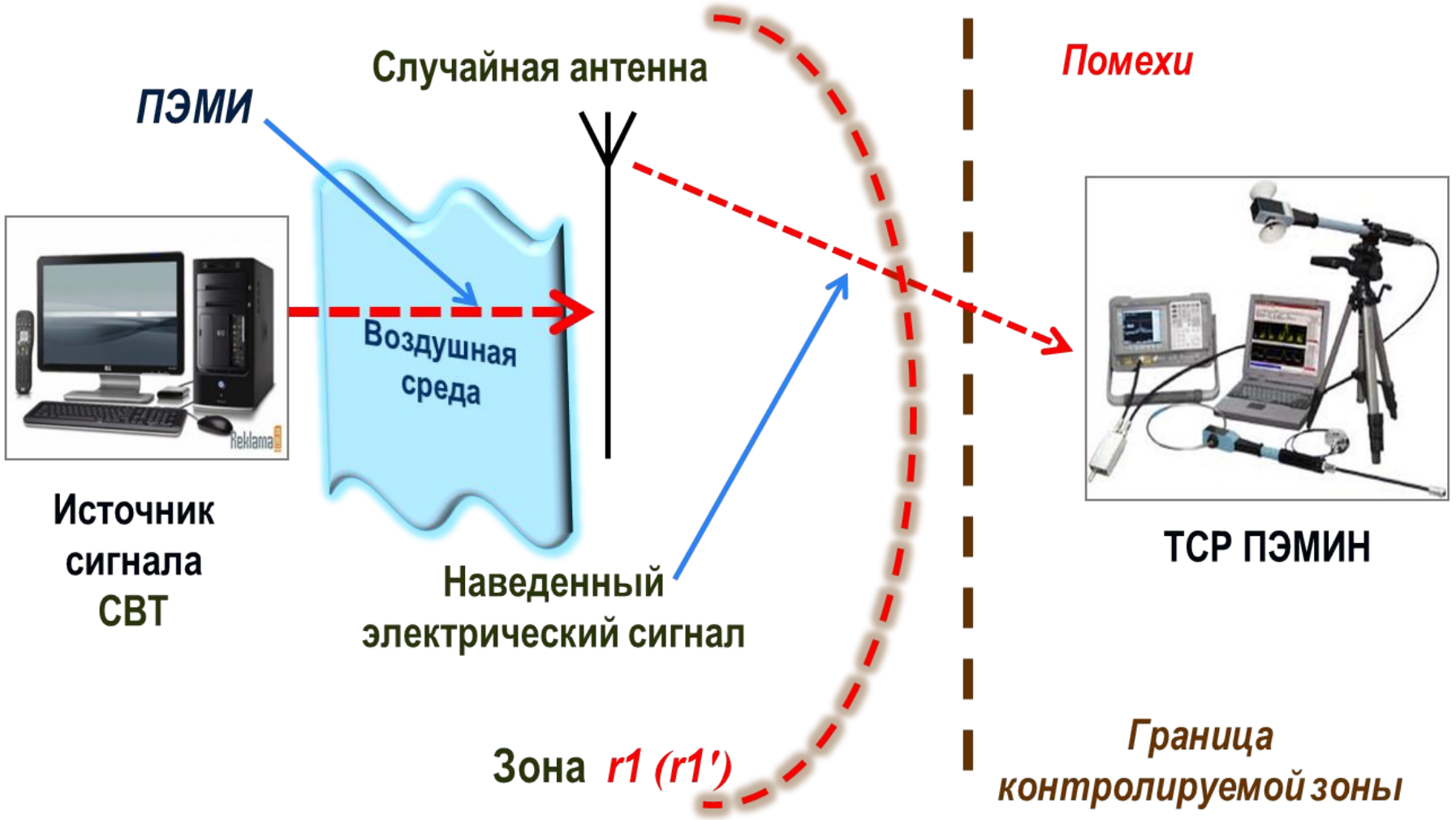
Модель технического канала утечки



$$\rho_{ОС}^{вх.ПП} = \rho_{ОС}^{вых.ТСПИ} - W_{помехи} - W_{ОС}^{КЗ} - W_{ОС}^{вх.ПП}$$

$$\rho_{ОС}^{выхПП} = \rho_{ОС}^{вх.ПП} - W_{внутр}^{Шума}$$

Модель технического канала утечки



ТЕХНИЧЕСКИМ КАНАЛОМ УТЕЧКИ ИНФОРМАЦИИ принято называть электропроводную **цепь или среду, по которой возможна утечка сведений**, обрабатываемых ТСПИ или обсуждаемых в выделенных помещениях.

ОПАСНЫМ СИГНАЛОМ (ОС) принято называть **сигнал** любой физической природы, **несущий информацию, подлежащую защите**.

Физически носителями опасного сигнала могут быть: акустические колебания; протекающие по любым проводящим коммуникациям токи; наводимая на посторонние цепи электродвижущая сила (ЭДС); распространяющиеся в окружающем пространстве электромагнитные поля различных диапазонов

СРЕДА РАСПРОСТРАНЕНИЯ ОС – это **некоторая материальная субстанция между ТСПИ**, **как источником опасного сигнала и местом возможной установки аппаратуры перехвата информации.** В качестве среды распространения ОС могут выступать: кабели связи, сигнализации и электропитания; шины и провода системы заземления; трубы систем вентиляции, тепло- и водоснабжения; окружающее пространство.

ПРИЕМНИК ПЕРЕХВАТА ИНФОРМАЦИИ (ППИ) представлен одиночными или комплексированными **средствами разведки ПЭМИН,** обеспечивающими прием и регистрацию звуковых сигналов, электромагнитных излучений и наводок ТСПИ. Конструктивно ППИ является портативной, исполняемой в возимом, носимом и автоматическом автономном вариантах, аппаратурой.

КОНТРОЛИРУЕМОЙ ЗОНОЙ (КЗ) называют территорию, на которой исключено несанкционированное и неконтролируемое пребывание лиц и транспортных средств – потенциальных носителей АПИ.

На практике используют два подхода к определению размеров КЗ.

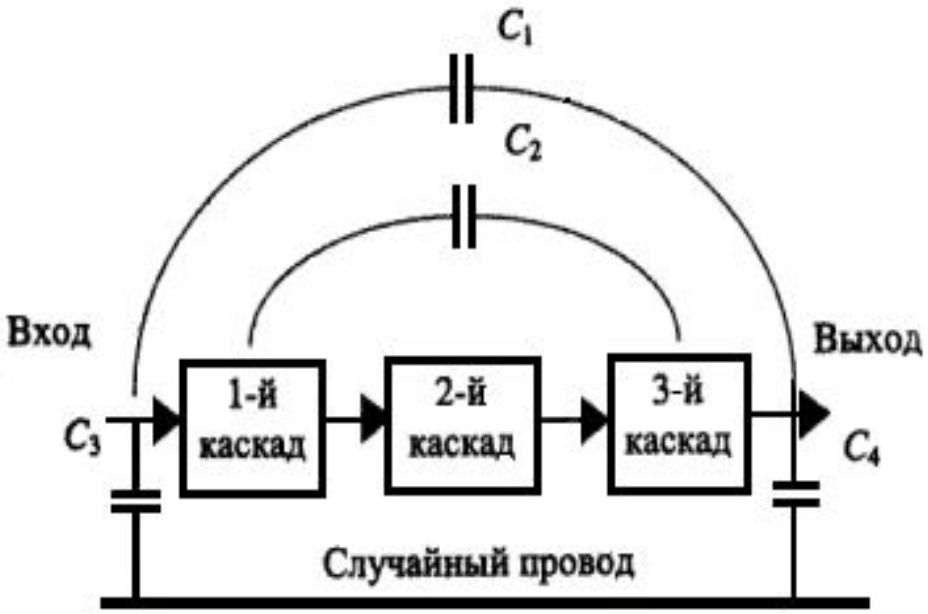
Первый из них предполагает нормативное установление, *в зависимости от категории защищаемого объекта, таких размеров КЗ,* при которых гарантированно исключается возможность ведения разведки ПЭМИН.

Второй подход основан на учете состава ТСПИ защищаемого объекта и расчете для каждого из них радиуса *R2*, так называемой *"Зоны 2", т.е. расстояния, на котором соотношение сигнал/помеха исключает возможность* приема и регистрации средствами разведки ПЭМИН опасных сигналов различной физической природы.

Побочные излучения технических средств обработки информации

Наряду с основным излучением **любое** радиопередающее устройство осуществляет формирование в окружающем пространстве **электромагнитных полей, соответствующих побочным радиоизлучениям** и связи могут содержать передаваемую в радиолинии информацию **вследствие их модуляции информационными сигналами.**

Электромагнитные излучения, возникающие при работе ПЭВМ (излучения дисплея, усилителей записи и считывания, кабельных соединений), являются **потенциальными носителями опасного сигнала.**



Технические средства различного назначения могут иметь в своем составе **устройства,** которые для выполнения своих основных функций **генерируют электромагнитные колебания** (эталонные и измерительные генераторы, генераторы тактовых частот, генераторы развертки электронно-лучевых трубок, гетеродины радиоприемных устройств).

ПЭМИ компьютера

ПЭМИ дисплея компьютера

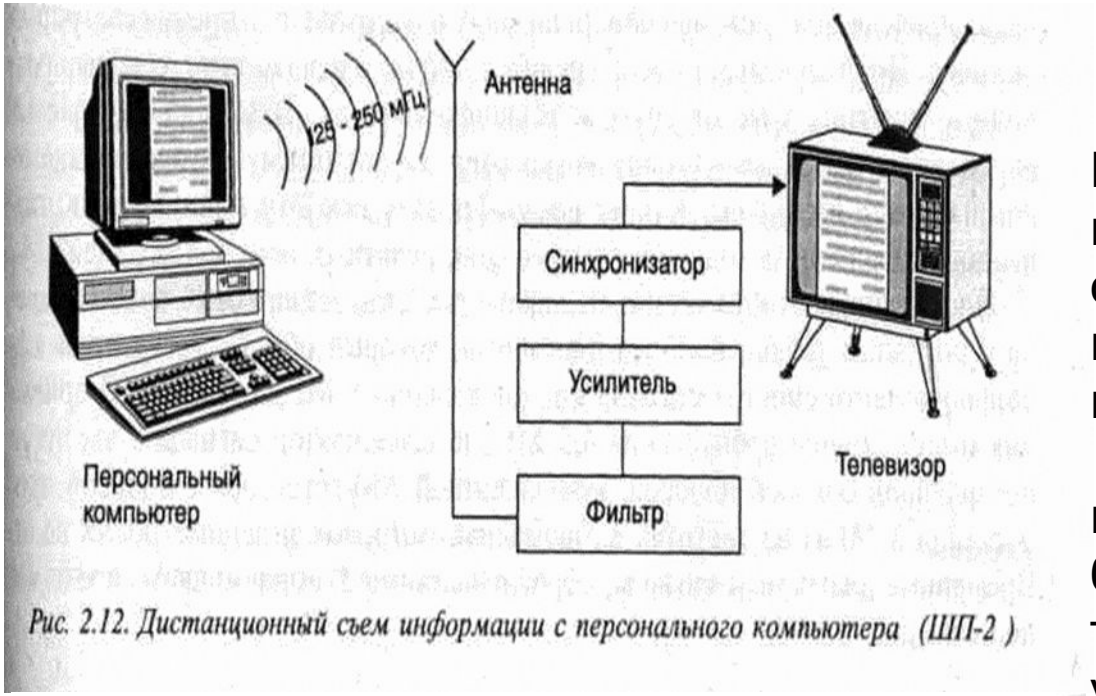


Рис. 2.12. Дистанционный съем информации с персонального компьютера (ШП-2)

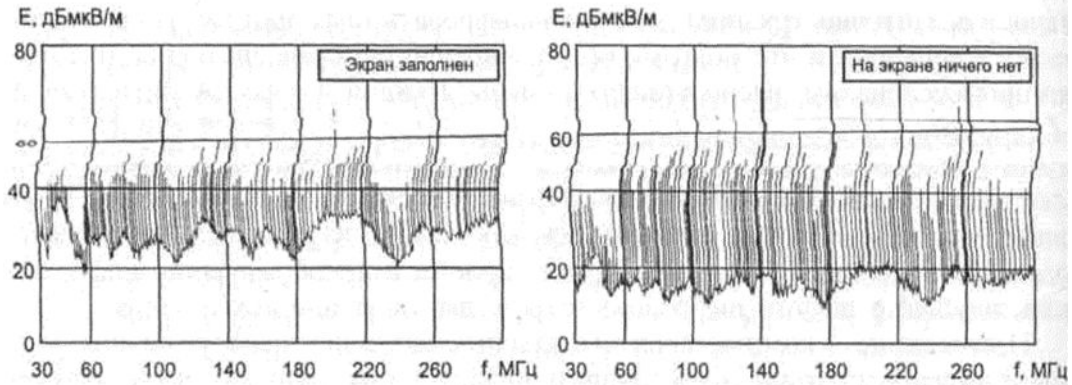


Рис. 2.13. Напряженность электрического поля E на расстоянии 1 м от дисплея

Опыт голландского инженера Вим ван Эка (Wim van Eck). На выставке Securecom-85 в Каннах он продемонстрировал возможность перехвата излучения монитора компьютера.

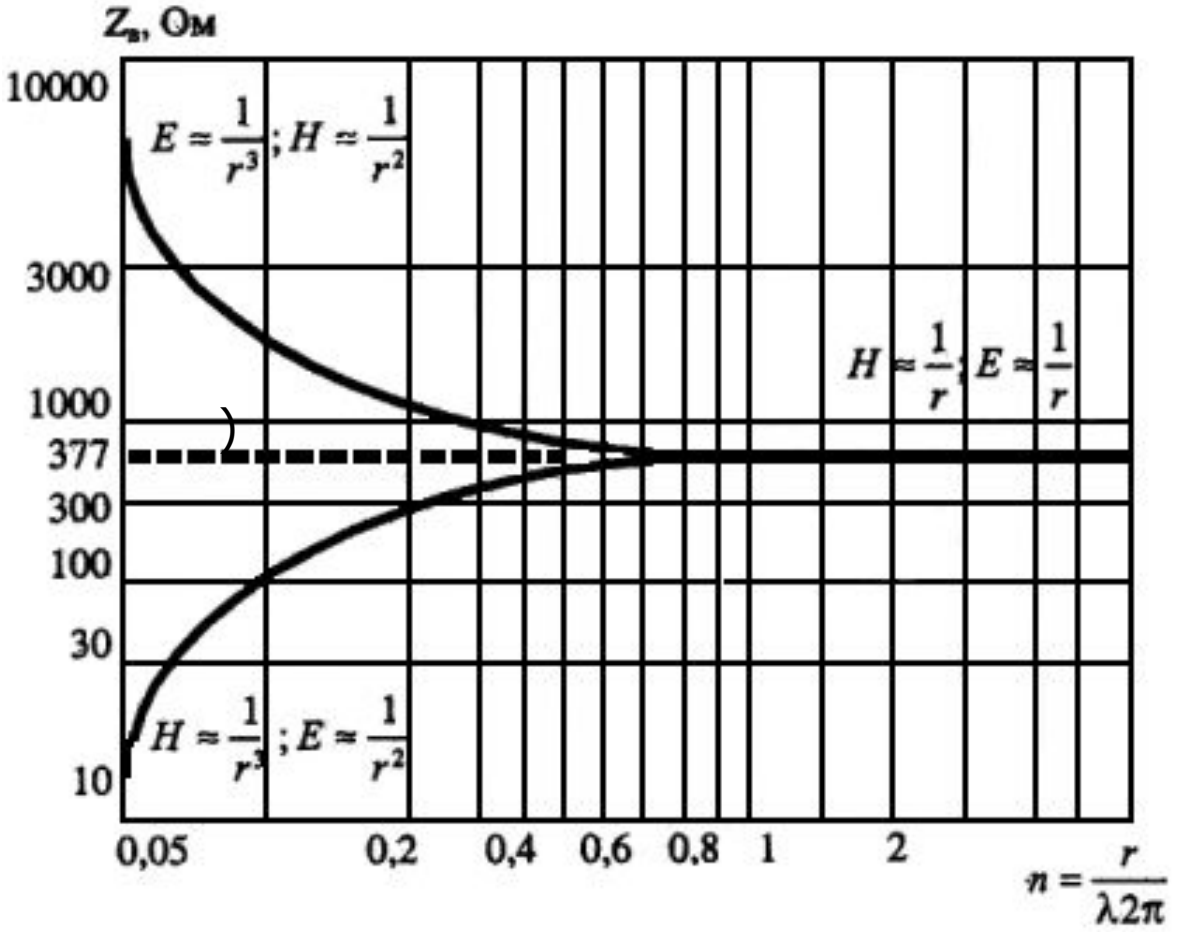
Опыт был достаточно прост: в автомобиле, стоящем на улице, был установлен обычный телевизионный приемник с усовершенствованной антенной, на экране которого можно было наблюдать ту же самую картину, которую воспроизводил монитор компьютера в здании рядом с автомобилем.

Распространение опасного сигнала за счет электромагнитного поля ближней и дальней зоны

Волновое сопротивление в ближней зоне при $r >> \frac{\lambda}{2\pi}$ зависит от типа излучателя (электрический или магнитный) и от расстояния до него.

Для оценки интенсивности электромагнитного поля в этой зоне достаточно определить одну из составляющих поля.

Обычно осуществляют измерение напряженности электрического поля или плотности потока мощности.



Типы излучателей и структура электромагнитного поля ТСПИ

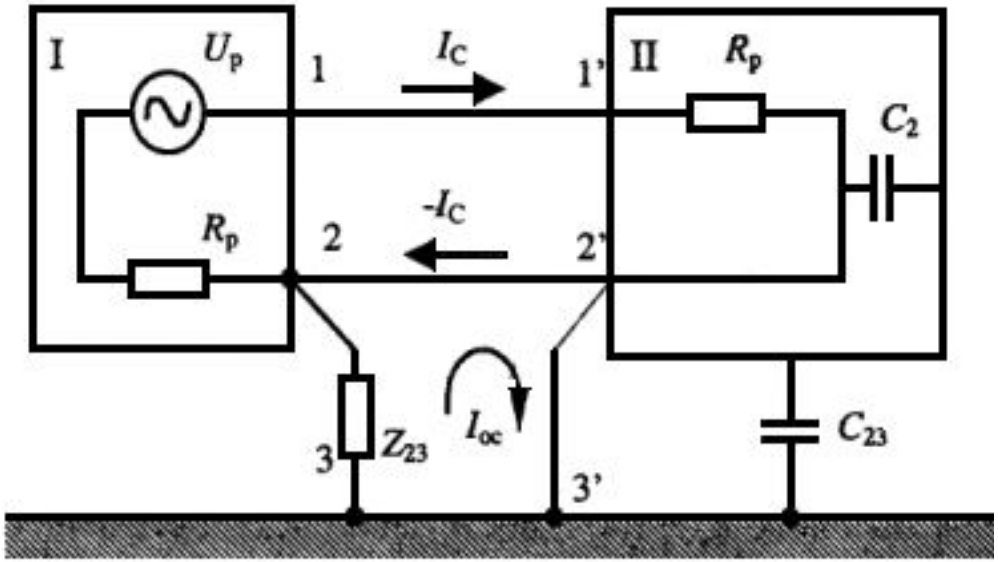
1. **Электрические цепи, технические средства или их элементы** обладают значительным сопротивлением и для них характерны большие амплитуды напряжений и малые амплитуды токов, то по своим свойствам они **подобны электрическим излучателям.** К таким элементам можно отнести, например, телевизионные кинескопы.
2. **Низкоомные электрические цепи и средства с большими амплитудами токов и малыми амплитудами напряжений** - например, мощные транзисторные усилители - **близки** по своим свойствам **к магнитным излучателям.**
3. В большинстве практических случаев **результирующее электромагнитное поле создается группой разнотипных источников излучения.** Поэтому характер изменения компонент этого поля существенно отличается от того, который свойственен одиночному излучателю, и обычно определяется экспериментально.

Причины попадания ОС в цепи заземления

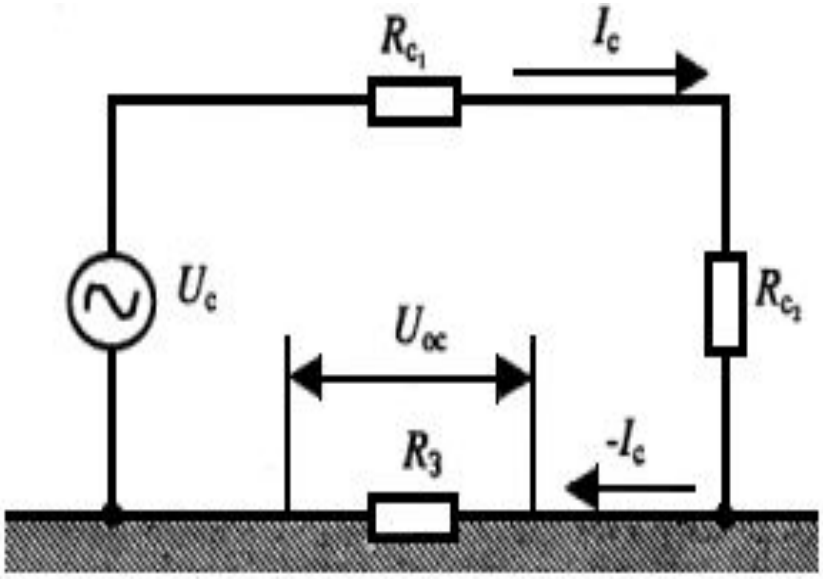
Одной из причин попадания опасного сигнала в систему заземления является **наличие электромагнитного поля** - носителя опасного сигнала в местах расположения элементов системы заземления.

Это **электромагнитное поле будет наводить** в расположенной поблизости системе заземления **ток опасного сигнала.** Аналогичным образом опасные сигналы могут наводиться на цепь, образуемую нулевым проводом, через который ток опасного сигнала будет попадать в систему заземления и далее в грунт.

Величина тока опасного сигнала в этом случае будет определяться интенсивностью воздействующего электромагнитного поля, сопротивлением цепей заземления и проводимостью почвы.



Образование контуров заземления



Протекание обратных токов

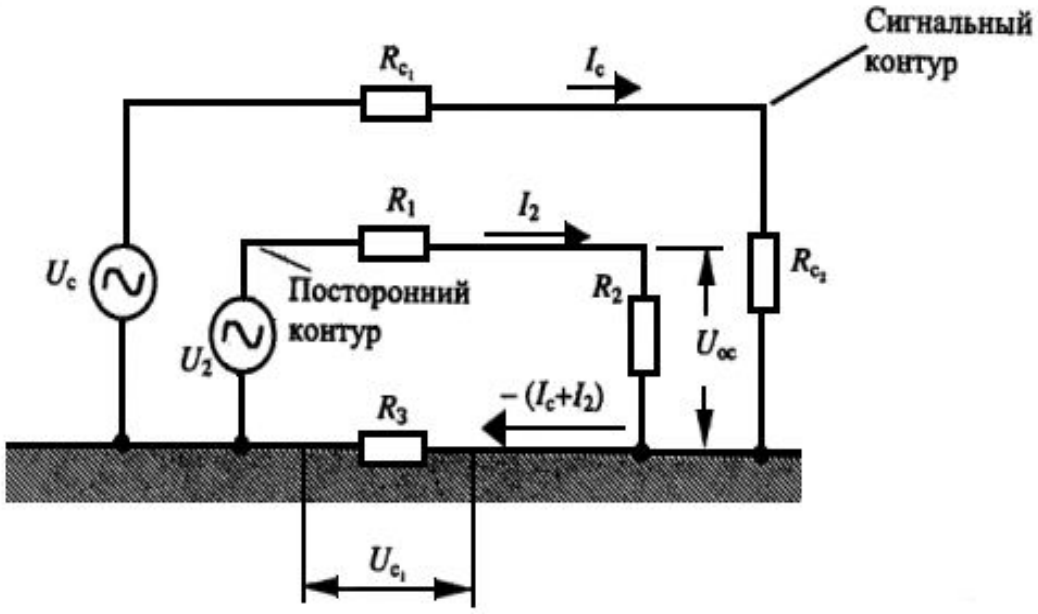
Проникновение опасного сигнала в цепи заземления может быть связано с образованием так называемых **контуров заземления.**

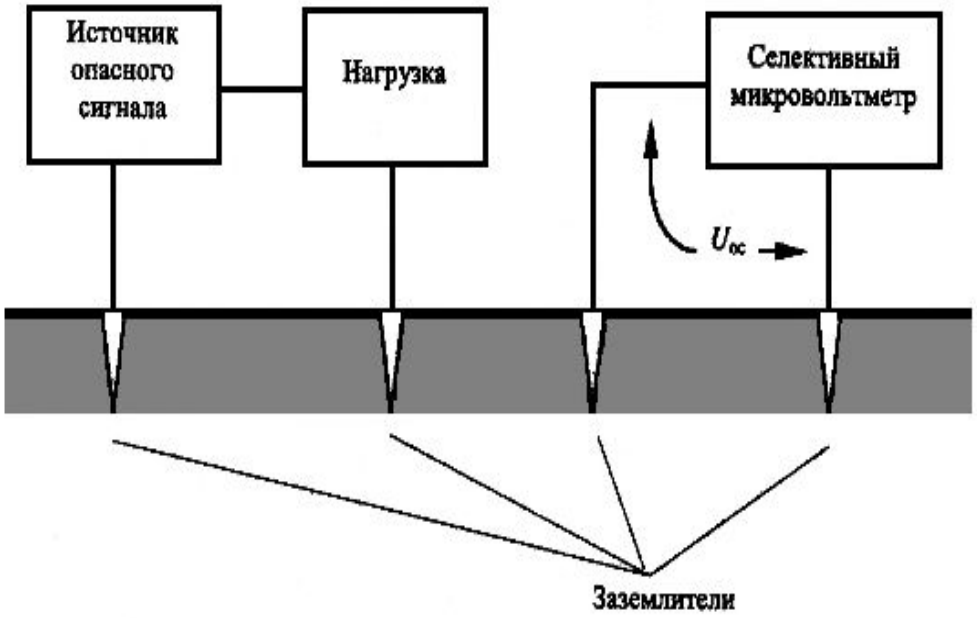
Пусть возвратный проводник соединен с корпусом первого (I) устройства, а корпус — с землей. Если этот проводник соединен с корпусом второго (II) устройства, также имеющего электрический контакт с землей (соединение 2' - 3') , то образуется **замкнутый проводящий контур** 2-2'-3`-3-2.

Внешнее электромагнитное поле источника опасного сигнала наводит в этом контуре **ЭДС**, вызывая протекание тока *Ioc*.

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

ПКУИ по цепям заземления





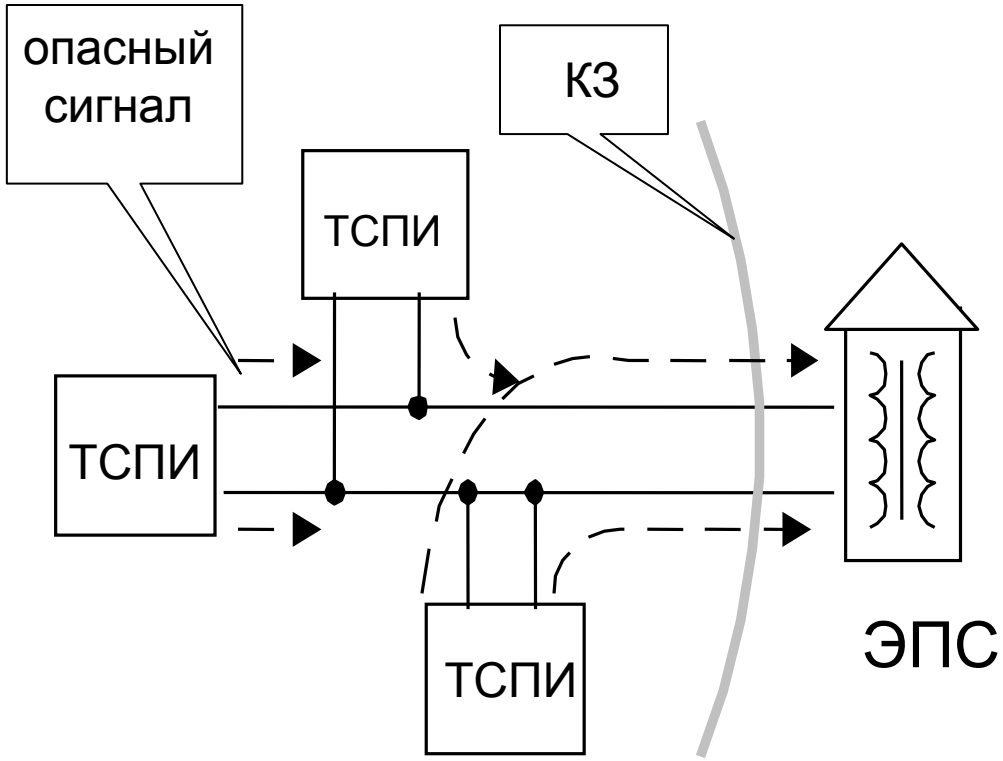
В случае для двух различных контуров - **сигнального и постороннего - общая земля является обратным проводом с эквивалентным сопротивлением.**

На эквивалентном сопротивлении земли возникает падение напряжения за счет протекания обратного тока опасного сигнала.

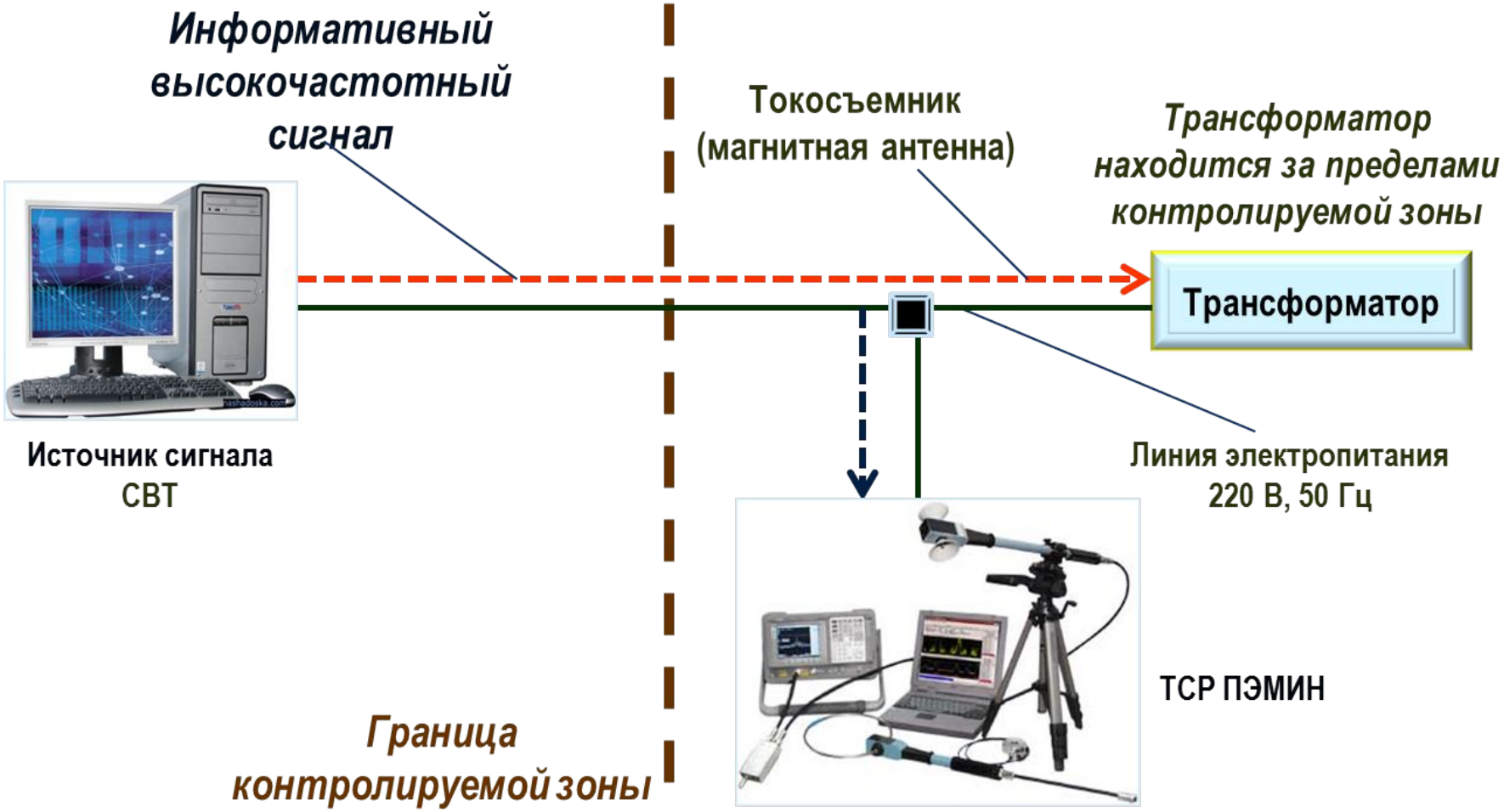
Утечка информации может быть обусловлена также **наличием электромагнитного поля опасного сигнала в грунте вокруг заземлителя.** Из-за большого затухания, вносимого грунтом, магнитное поле в землю практически не проникает.

Электрическое поле в земле определяется величиной потенциала заземлителя и параметрами грунта, где происходит растекание тока опасного сигнала. С помощью дополнительных специально установленных заземлителей можно осуществить перехват опасного сигнала.

Канал утечки по цепям электропитания



1. Как правило, **провода** общей сети питания **распределяются по различным помещениям**, где расположены технические системы, и **соединены с различными устройствами**.
2. Образуется нежелательная связь между отдельными техническими средствами.
3. Кроме того, провода сети питания являются **линейными антеннами,** способными излучать или воспринимать электромагнитные поля.
4. На практике **значительная часть нежелательных наводок** между удаленными друг от друга устройствами происходит с участием сети питания


Информативный высокочастотный сигнал
Токосъемник (магнитная антенна)
Трансформатор находится за пределами контролируемой зоны
Трансформатор
Источник сигнала СВТ
Линия электропитания 220 В, 50 Гц
ТСР ПЭМИН
Граница контролируемой зоны

АКТИВНЫЕ УСТРОЙСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ЦЕПЯМ ПИТАНИЯ И СИСТЕМАМ ЗАЗЕМЛЕНИЯ

SEL SP-41/C

БАРЬЕР-4

СКИТ-М-С

ИМПУЛЬС

МП-3

СОНАТА-С1

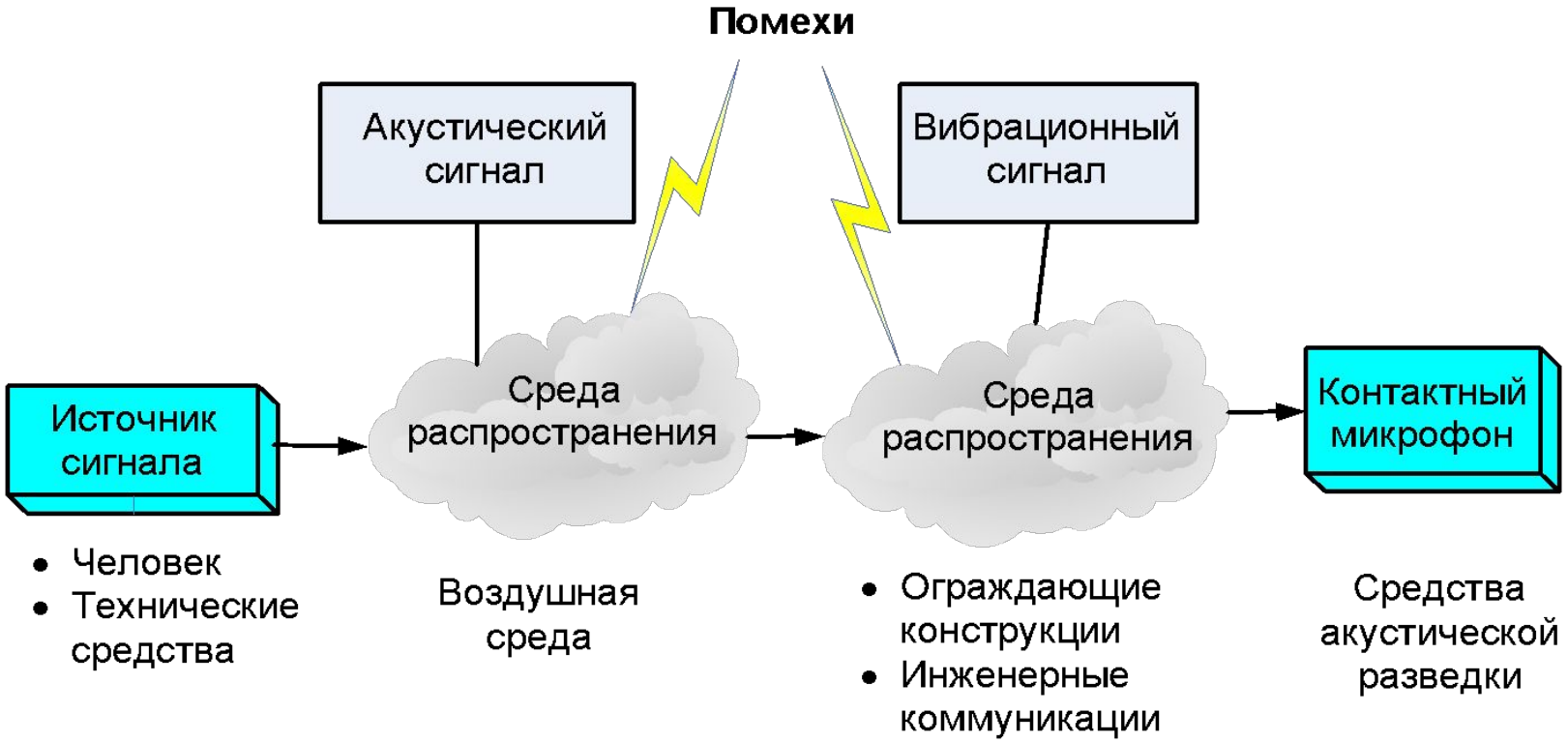
SEL SP-41/D

SI-8001

СОПЕРНИК

ЦИКАДА-М1

Виброакустический канал утечки информации



Виброакустический канал утечки информации. Воздействие акустических волн на поверхность твердого тела приводит к **возникновению в нем вибрационных колебаний в результате виброакустического преобразования.**

Эти колебания, распространяющиеся в твердой среде, могут быть **перехвачены специальными средствами разведки,** а речевая информация, содержащаяся в акустическом поле, при определенных условиях может быть восстановлена. **Вибродатчики** преобразуют вибрационные колебания в электрические сигналы, соответствующие звуковым частотам.

СИСТЕМЫ, КОМПЛЕКСЫ И ПРИБОРЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ И ВИБРОАКУСТИЧЕСКИМ КАНАЛАМ

ANG-2000

SI-3001

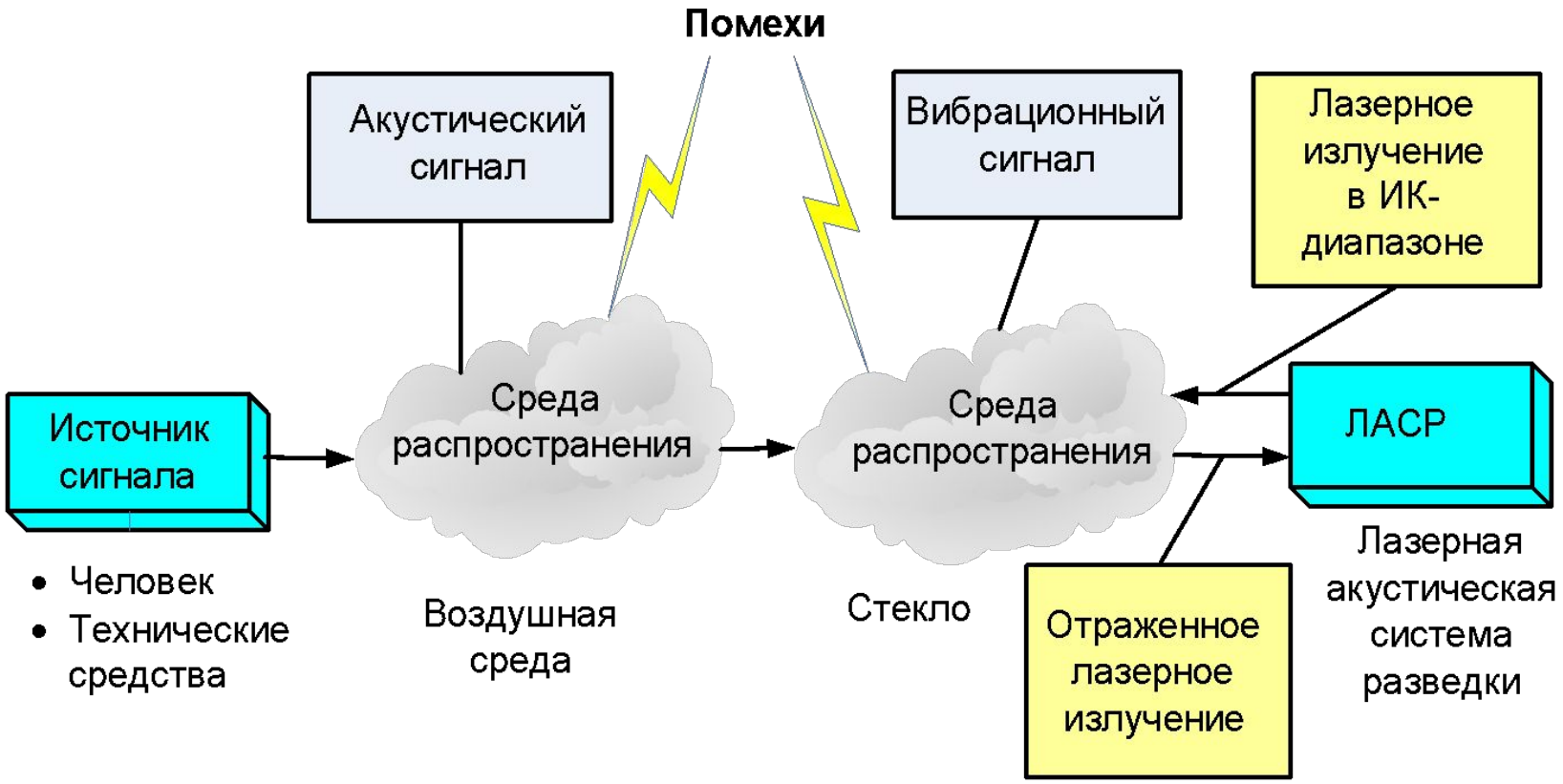
VAG-6/6

БАРОН DIGITAL

СОНАТА-АВ 1М

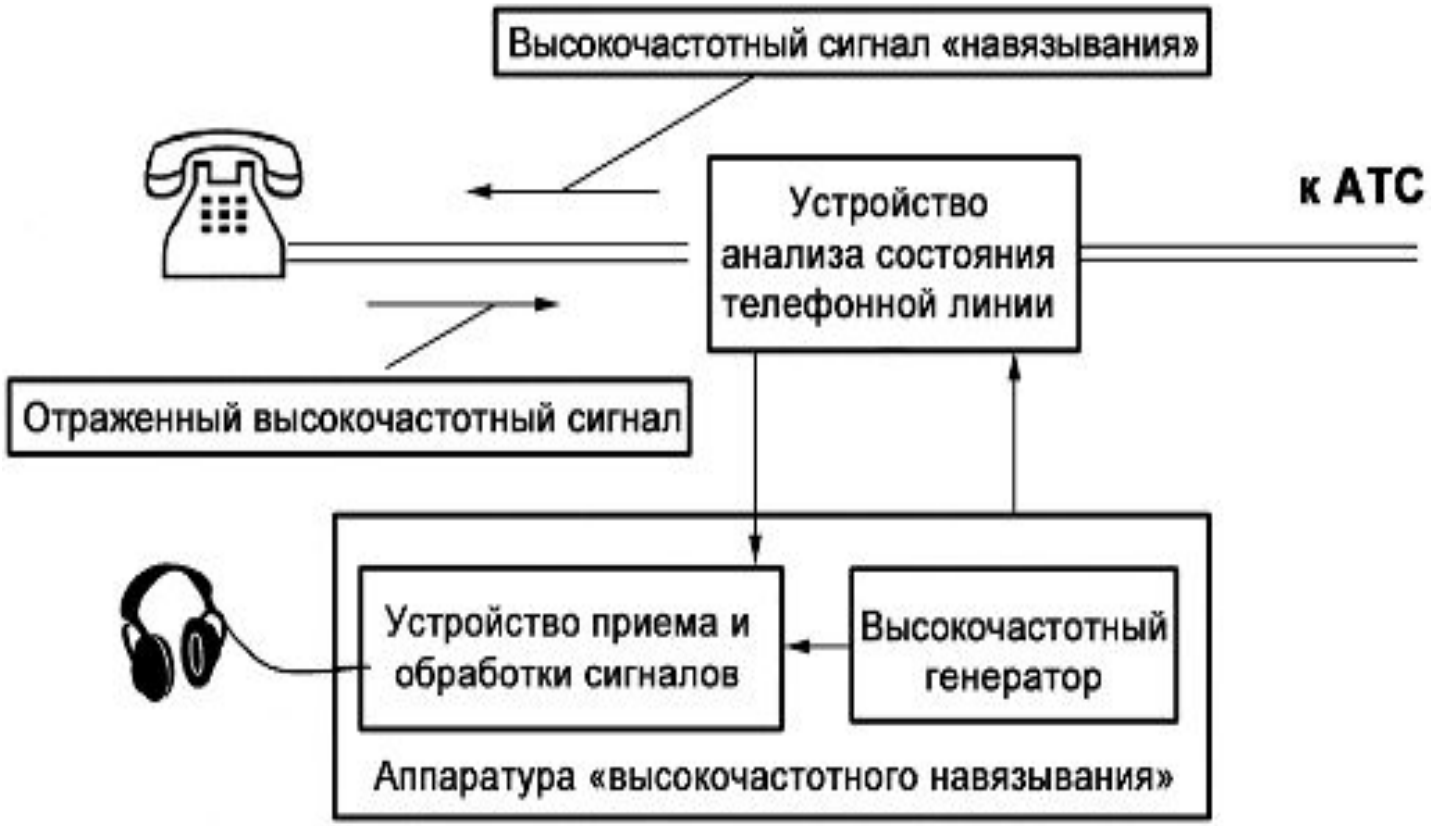
СКИТ-М-ВА

Высокочастотное облучение



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.**

Высокочастотное навязывание



ВЧ-навязывание осуществляется посредством контактного введения высокочастотного сигнала в электрические цепи, **имеющие функциональные или паразитные связи** с техническим средством.

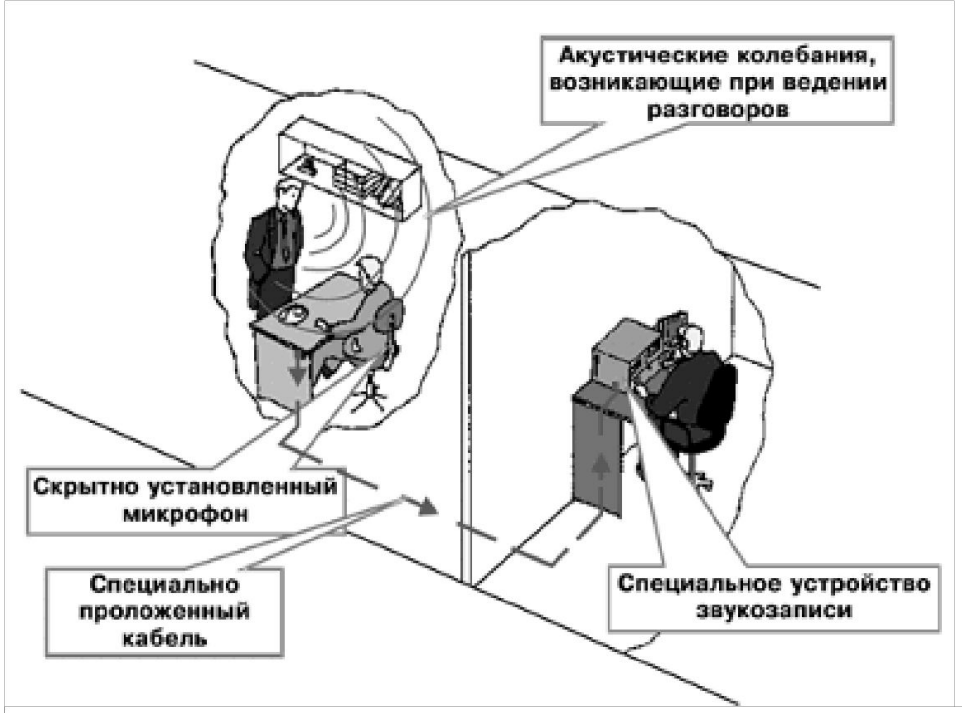
Меры защиты от ПКУИ

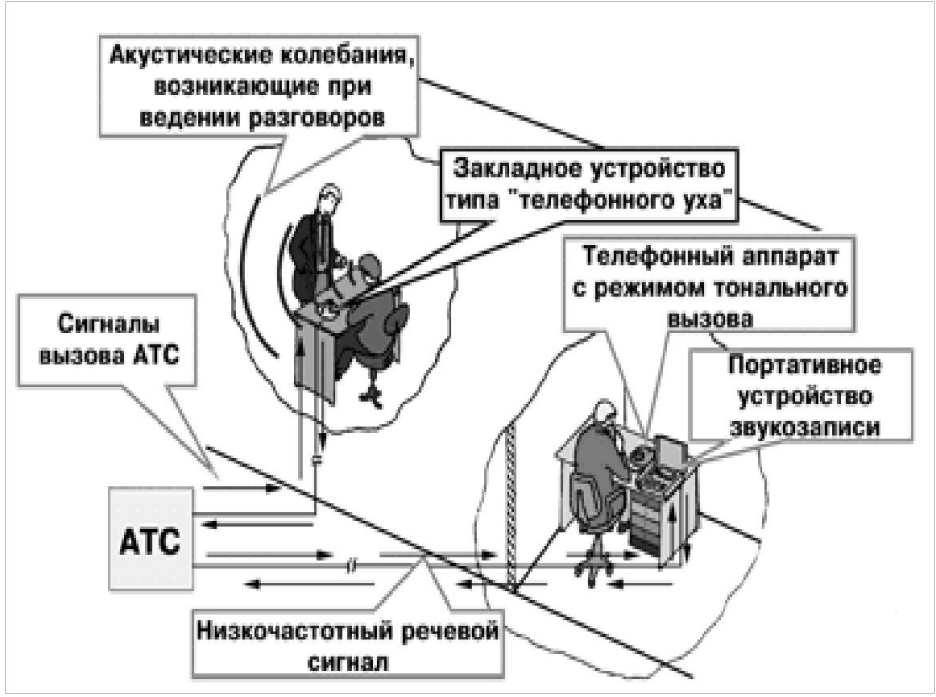
1. Правильное **размещение и монтаж** ТСПИ в помещениях и на объектах с учетом их особенностей и реальных размеров КЗ;
2. Применение **ТСПИ, прошедших специальные исследования** и имеющих сертификаты (предписания на эксплуатацию);
3. **Локализацию ПЭМИН** технических средств в пределах КЗ защищаемых объектов.

В локализации ПЭМИН должны сочетаться меры пассивного и активного характера. К пассивным относят:

- экранирование ТСПИ и помещений;
- фильтрацию опасных токов и напряжений.

Активные меры состоят в зашумлении линий, помещений и применяются в тех случаях, когда реализацией мер пассивного характера не удается снизить нормируемые параметры ПЭМИН на границе КЗ до уровня установленных требований.





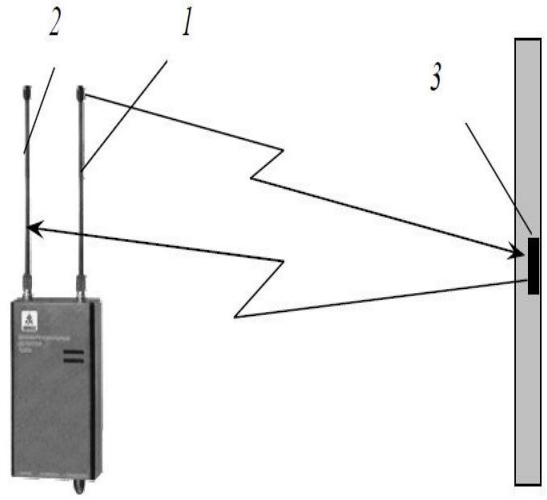


Рис. 1.48. Схема аудио-транспондера: *1* – антенна облучающего передатчика; *2* – антенна приемника; *3* – полуактивная радиозакладка в стене

Фото 1. Направленный микрофон «Супер Ухо – 100»

Фото 2. Внешний вид параболических направленных микрофонов

Параболический отражатель выполнен из пластика. В фокусе отражателя помещен электретный микрофон, подключенный к входу малошумящего усилителя низкой частоты. Встроенный 8-кратный бинокль позволяет точно навести микрофон на цель.

Микрофон имеет размеры 290´150´90 мм и массу 1,2 кг. Питание микрофона осуществляется от батарейки типа «крона». Время работы от внутренней батарейки – до 60 ч.

Параболические микрофоны чаще всего маскируются под антенны спутникового телевидения и устанавливаются на балконах домов.

Фото 3. Внешний вид параболических направленных микрофонов

УСТРОЙСТВО БЛОКИРОВАНИЯ РАБОТЫ СИСТЕМ МОБИЛЬНОЙ СВЯЗИ

DLW 4003
DLW 4012

Скат

Москит GSM 3

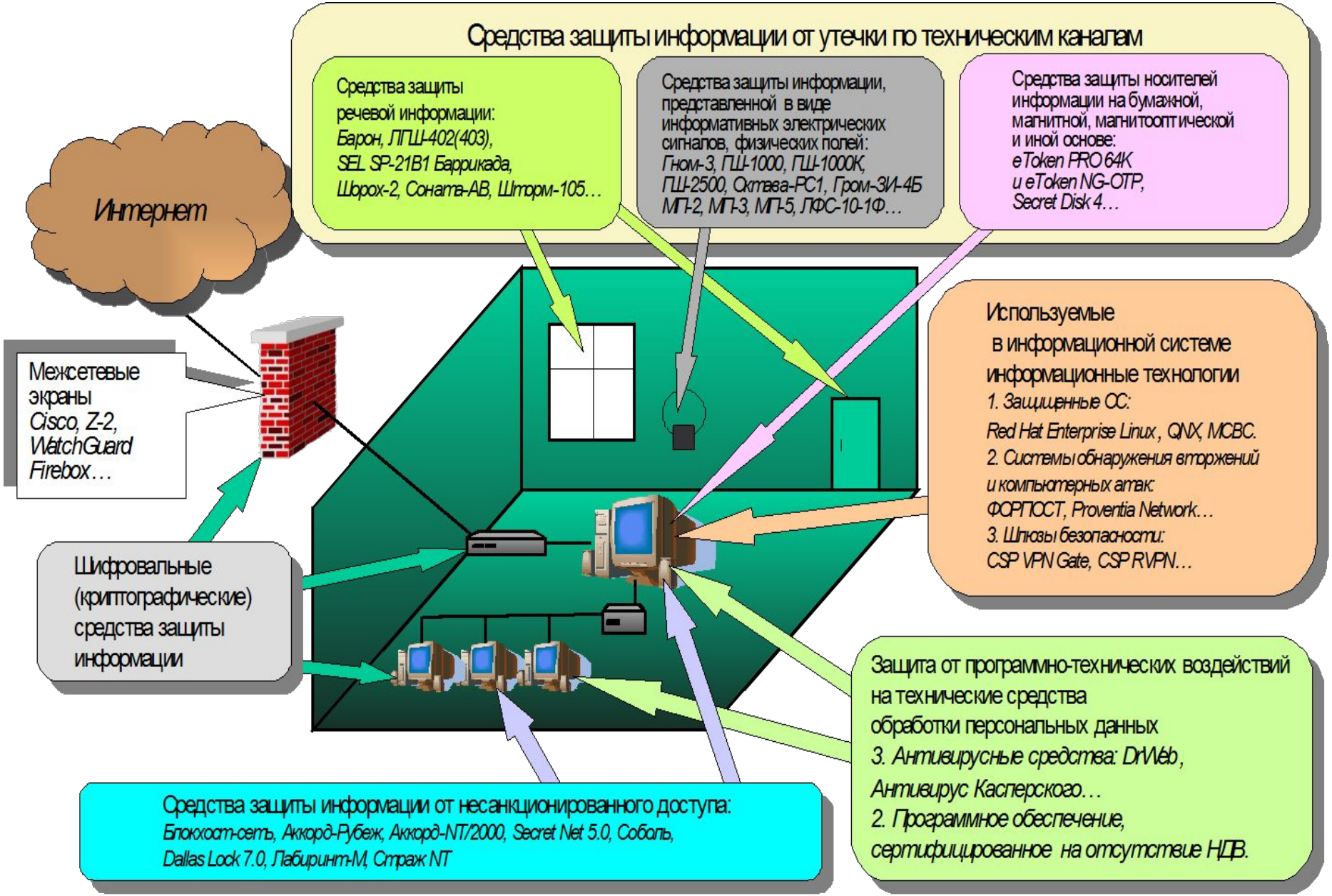
Мозаика

Сапфир

DLW 2000

Гамма

C-CUARD-300YK


Средства защиты информации от утечки по техническим каналам
Средства защиты речевой информации: Барон, ЛПШ-402(403), SEL SP-21B1 Баррикада, Шорох-2, Соната-АВ, Шторм-105…
Средства защиты информации, представленной в виде информативных электрических сигналов, физических полей: Гном-3, ГШ-1000, ГШ-1000К, ГШ-2500, Октава-РС1, Гром-ЗИ-4Б МП-2, МП-3, МП-5, ЛФС-10-1Ф…
Средства защиты носителей информации на бумажной, магнитной, магнитооптической и иной основе: eToken PRO 64K и eToken NG-OTP, Secret Disk 4…
Интернет
Межсетевые экраны Cisco, Z-2, WatchGuard Firebox…
Используемые в информационной системе информационные технологии
1. Защищенные ОС: Red Hat Enterprise Linux, QNX, МСВС.
2. Системы обнаружения вторжений и компьютерных атак: ФСРПОСТ, Proventia Network…
3. Шлюзы безопасности: CSP VPN Gate, CSP RVPN…
Шифровальные (криптографические) средства защиты информации
Защита от программно-технических воздействий на технические средства обработки персональных данных
3. Антивирусные средства: DrWeb, Антивирус Касперского…
2. Программное обеспечение, сертифицированное на отсутствие НДВ.
Средства защиты информации от несанкционированного доступа: Блокхост-сеть, Аккорд-Рубеж, Аккорд-NT/2000, Secret Net 5.0, Соболь, Dallas Lock 7.0, Лабиринт-М, Страж NT

Dr.WEB®
www.drweb.com

Средства защиты информации

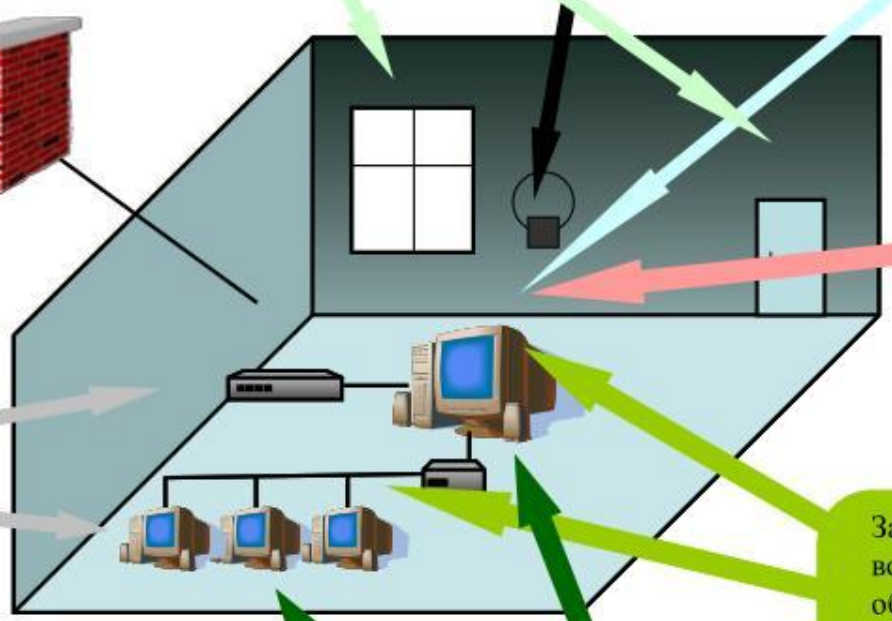
Средства защиты речевой информации:
Барон, ЛГШ-402(403), SEL SP-21B1 Баррикада, Шорох-2, Соната-АВ, Шторм-105…

Средства защиты информации, представленной в виде информативных электрических сигналов, физических полей:
Гном-3, ГШ-1000, ГШ-1000К, ГШ-2500, Октава-РС1, Гром-ЗИ-4Б
МП-2, МП-3, МП-5, ЛФС-10-1Ф…

Средства защиты носителей информации на бумажной, магнитной, магнитоопрической и иной основе:
eToken PRO 64K и eToken NG-OTP, Secret Disk 4…

Интернет

Межсетевые экраны
Cisco, Z-2, WatchGuard Firebox…



Используемые в информационной системе информационные технологии
1. Защищенные ОС:
Red Hat Enterprise Linux, QNX, МСВС 3.0...
2. Системы обнаружения вторжений и компьютерных атак:
ФОРПОСТ, Proventia Network…
3. Шлюзы безопасности:
CSP VPN Gate, CSP RVPN…

Шифровальные (криптографические) средства защиты информации

Защита от программно-технических воздействий на технические средства обработки персональных данных
1. Антивирусные средства:
Dr.Web
2. Программное обеспечение, сертифицированное на отсутствие НДВ.

Средства защиты информации от несанкционированного доступа:
Блокхост-сеть, Аккорд-Рубеж, Аккорд-NT/2000, Secret Net 5.0, Соболь, Dallas Lock 7.0, Лабиринт-М, Страж NT

СЗИ от утечки по ТКУИ

Комплекс для проведения акустических и виброакустических измерений СПРУТ-7А

Система «Барон»

Соната

"Копейка" вибрационный излучатель на стекло

"Молот" вибрационный излучатель на стену

Вибропреобразователь на оконное стекло КВП-7

Вибропреобразователь на стену КВП-2

Акустический преобразователь на дверной проём

Система «Шорох-2М»

"Серп" вибрационный излучатель на раму окна

СЗИ от утечки

Кейс «ТЕНЬ» для транспортировки ноутбуков с возможностью автоматического уничтожения информации при попытке НСД

Защиты от НСД «SecretNet»

Устройство для быстрого уничтожения информации на HDD «СТЕК-Н»

USB-ключи и пр.

КРИПТО ПРО

MAXPATROL

Электронный замок для защиты от НСД «Соболь»