# ФИЗИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОННЫХ СПОСОБОВ ВОЗДЕЙСТВИЯ УГРОЗ НА ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

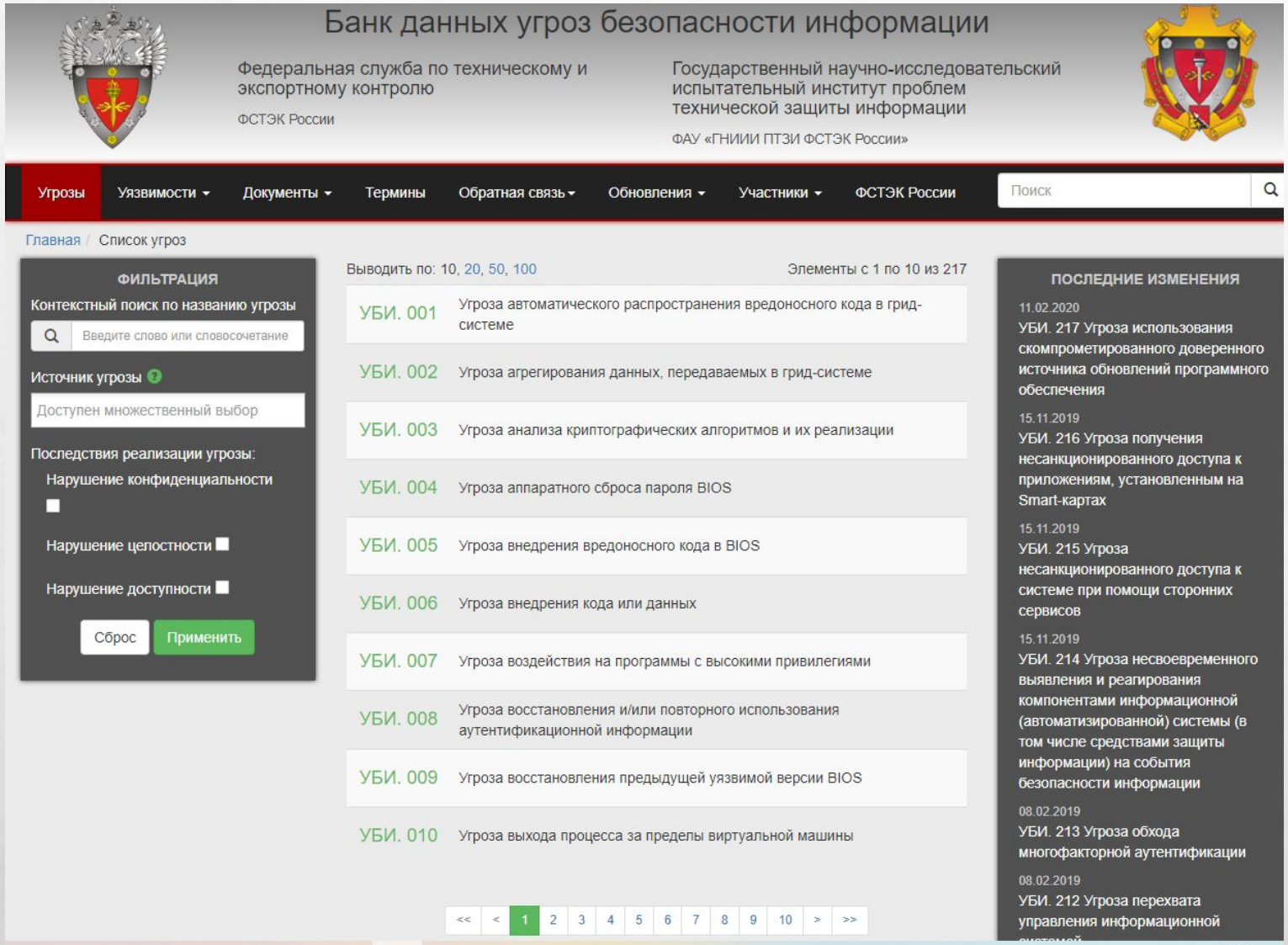
ФИЛИМОНОВ Д. Н., СТУДЕНТ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ», ЕГУ ИМ. И. А. БУНИНА

Информация (Information) – сведения сообщения, данные независимо от формы их представления

- Безопасность информации [данных] (Information (Data) security) состояние защищённости информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность. *Безопасность информации означает, что информация находится в таком защищенном виде, который способен противостоять любым дестабилизирующим воздействиям.*
- Угроза (Threat) – возможная причина нежелательного инцидента, которая может нанести ущерб [информационной] системе или всей организации. Угроза – это фактор, стремящийся нарушить работу системы.
- Угроза безопасности информации (Information security threat) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. *Угроза информации обусловлена вполне определенными факторами, совокупностью явлений и условий, которые могут сложиться в конкретной ситуации.*
- Источник угрозы безопасности информации (Information security threat source) - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации
- Модель угроз безопасности информации (Information security threats model ) - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации
- Защита информации от преднамеренного воздействия (Intentional exposure protection of information) - защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и/или воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

# РЕЗУЛЬТАТЫ РЕАЛИЗАЦИИ УГРОЗ ИБ

- нарушение секретности (конфиденциальности) информации (разглашение, утрата, хищение, утечка и перехват и т.д.)
- нарушение целостности информации (уничтожение, искажение, подделка и т.д.)
- нарушение доступности информации и работоспособности информационных систем (блокирование данных и информационных систем, разрушение элементов информационных систем, компрометация системы защиты информации и т.д.)




Насчитываются сотни угроз информационной безопасности. Полное множество угроз описать невозможно из-за множества влияющих на нее факторов, обусловленных сложностью архитектуры современных АС обработки информации.

Угрозы, непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение и т. п.).
создание помех в радиоэфире с помощью дополнительного звукового или шумового фона, изменения (наложения) частот передачи информации;
подключение подавляющих подавляющих фильтров в информационные цепи, цепи питания и заземления;

# ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

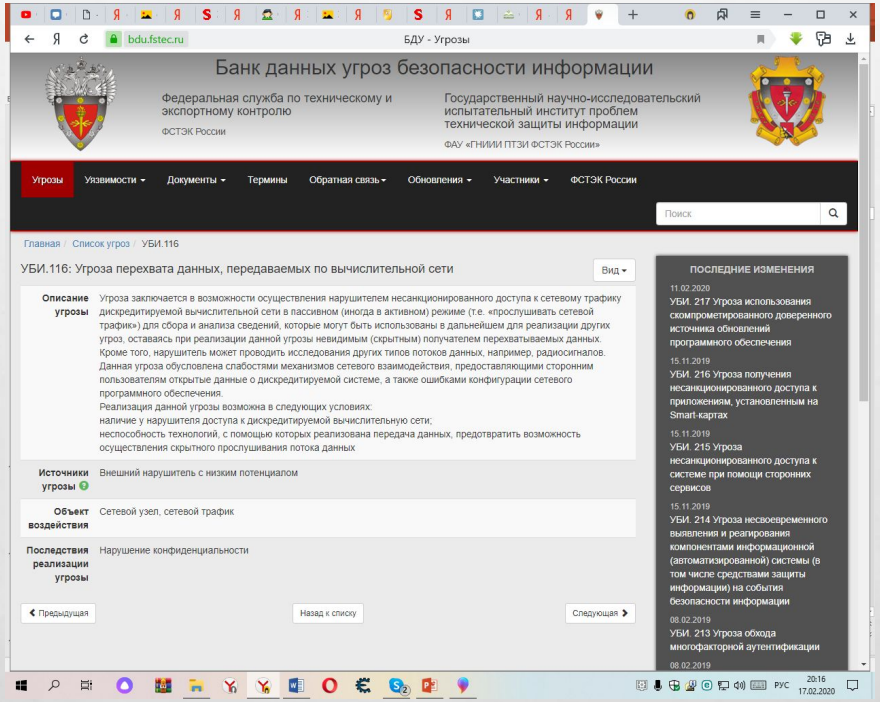
- Информационные ресурсы, содержащие конфиденциальную информацию (секретную, ограниченного доступа или же коммерческую тайну), а также общедоступную открытую информацию и научные знания;
- Информационная инфраструктура общества (сети связи и информационных коммуникаций, центры анализа и обработки данных, системы и средства защиты информации);
- Система формирования, распространения и использования информационных ресурсов в стране;
- Система формирования общественного сознания, базирующаяся на средствах массовой информации;
- Права граждан, юридических лиц и государства на получение, распространение и использование информации, а так же защиту конфиденциальной информации и интеллектуальной собственности.

- Информация, выраженная в определенной форме, предназначенная для передачи, называется сообщением.
- Чаще информация представляется в двоичной форме, т.е. только двумя условными символами, например 1 и 0. Соответственно сообщением служит последовательность конечного числа двоичных символов.
- Природа сообщений может быть как электрической, так и неэлектрической.
- Для передачи сообщений от источника к получателю используют физические процессы, например звуковые и электромагнитные волны, ток.
- Физический процесс, отображающий сообщение, называется сигналом.
- По своей природе сигналы могут быть электрическими, световыми, звуковыми и т.п.
- В РСПИ используются электрические сигналы. Поэтому при передаче сообщения неэлектрической природы предварительно преобразуются в электрические колебания с помощью преобразователей: микрофонов, передающих телевизионных трубок, датчиков температуры, давления и т.п.

# РАДИОЭЛЕКТРОННЫЕ СПОСОБЫ ВОЗДЕЙСТВИЯ УГРОЗ:

- перехват информации в технических каналах её утечки;
- перехват информации в сетях передачи данных и линиях связи;
- внедрение электронных устройств перехвата информации в технические средства и помещения;
- навязывание ложной информации по сетям передачи данных и линиям связи;
- радиоэлектронное подавление линий связи и систем управления с использованием одноразовых и многоразовых генераторов различных видов электромагнитной энергии.

# РАДИОЭЛЕКТРОННОЕ ПОДАВЛЕНИЕ ЛИНИЙ СВЯЗИ И СИСТЕМ УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ОДНОРАЗОВЫХ И МНОГОРАЗОВЫХ ГЕНЕРАТОРОВ РАЗЛИЧНЫХ ВИДОВ ЭЛЕКТРОМАГНИТНОЙ ЭНЕРГИИ.

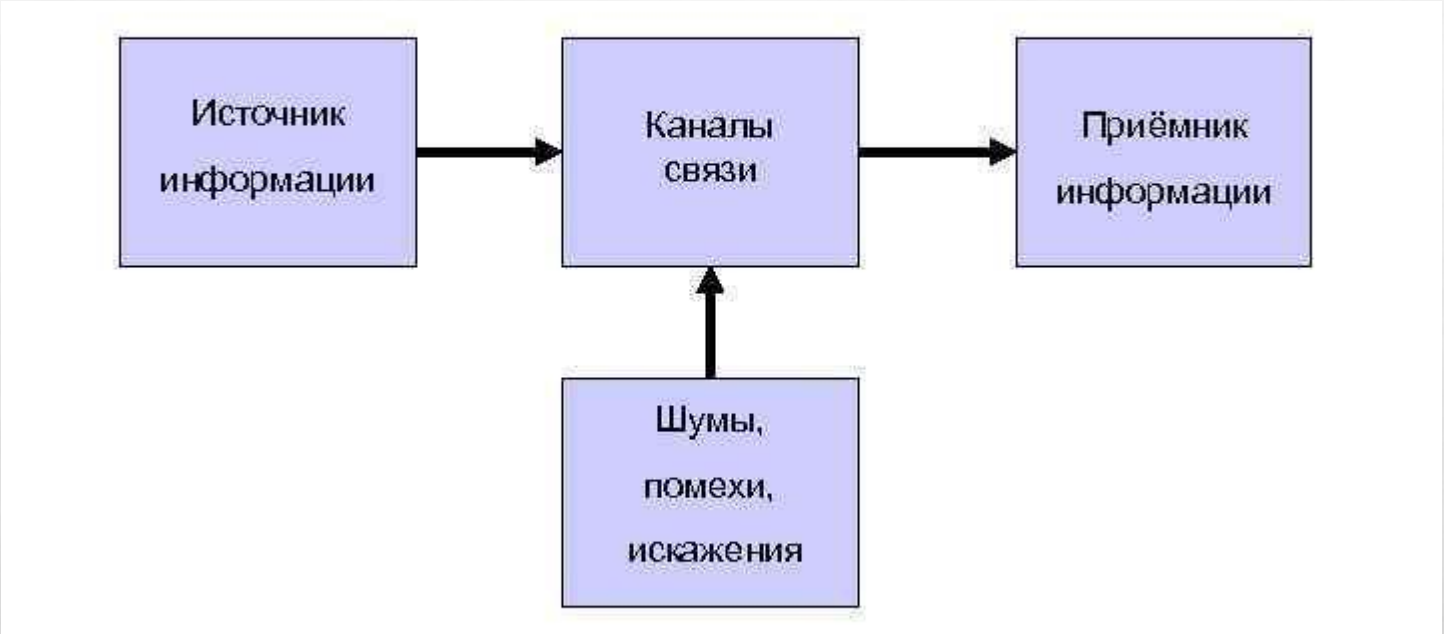


bdu.fstec.ru
БДУ - Угрозы
Банк данных угроз безопасности информации
Федеральная служба по техническому и экспортному контролю
ФСТЭК России
Государственный научно-исследовательский испытательный институт проблем технической защиты информации
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
Угрозы
Уязвимости
Документы
Термины
Обратная связь
Обновления
Участники
ФСТЭК России
Поиск
Главная / Список угроз / УБИ.116
УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети
Вид
Описание угрозы
Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном (иногда в активном) режиме (т.е. «прослушивать сетевой трафик») для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым (скрытным) получателем перехватываемых данных. Кроме того, нарушитель может проводить исследования других типов потоков данных, например, радиосигналов. Данная угроза обусловлена слабостями механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибками конфигурации сетевого программного обеспечения.
Реализация данной угрозы возможна в следующих условиях:
наличие у нарушителя доступа к дискредитируемой вычислительной сети;
неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных
Источники угрозы
Внешний нарушитель с низким потенциалом
Объект воздействия
Сетевой узел, сетевой трафик
Последствия реализации угрозы
Нарушение конфиденциальности
Предыдущая
Назад к списку
Следующая
ПОСЛЕДНИЕ ИЗМЕНЕНИЯ
11.02.2020
УБИ. 217 Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения
15.11.2019
УБИ. 216 Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах
15.11.2019
УБИ. 215 Угроза несанкционированного доступа к системе при помощи сторонних сервисов
15.11.2019
УБИ. 214 Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
08.02.2019
УБИ. 213 Угроза обхода многофакторной аутентификации
08.02.2019
РУС
20:16
17.02.2020

# РАДИОЭЛЕКТРОННЫЕ СПОСОБЫ ВОЗДЕЙСТВИЯ УГРОЗ:

- перехват информации в технических каналах её утечки (за счет побочных электромагнитных излучений, создаваемых техническими средствами обработки и передачи информации за счет наводок в коммуникациях, сети питания, заземления, радиотрансляции, пожарной и охранной сигнализаций и т.д.) и в линиях связи путём прослушивания конфиденциальных разговоров с помощью акустических, виброакустических и лазерных технических средств разведки, прослушивания конфиденциальных телефонных переговоров, путём визуального наблюдения за работой средств отображения информации;
- перехват информации в сетях передачи данных и линиях связи;
- внедрение электронных устройств перехвата информации в технические средства и помещения;
- навязывание ложной информации по сетям передачи данных и линиям связи.
- радиоэлектронное подавление линий связи и систем управления с использованием одноразовых и многоразовых генераторов различных видов электромагнитной энергии

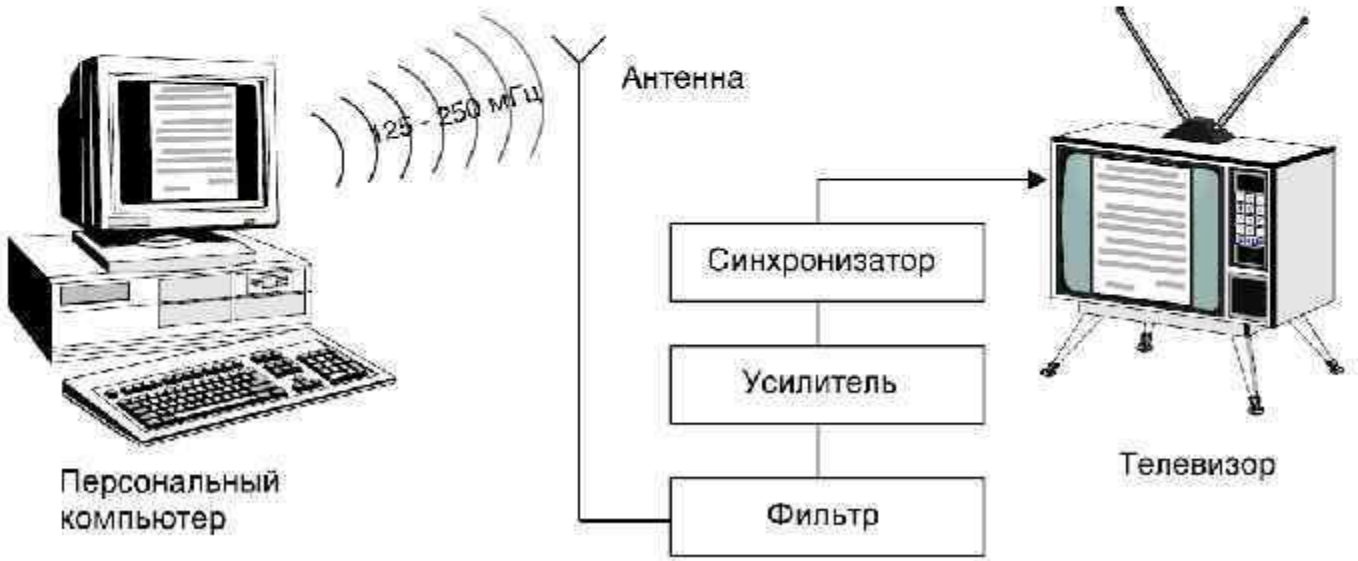
Специальная защита технических средств передачи и обработки информации включает организационные мероприятия и технические меры по закрытию возможных технических каналов утечки информации за счет побочных электромагнитных излучений, наводок, высокочастотного навязывания и электроакустических преобразований и осуществляется в сочетании с аппаратурными, программными, криптографическими методами защиты.

# СТРУКТУРА СЕТИ ПЕРЕДАЧИ ДАННЫХ

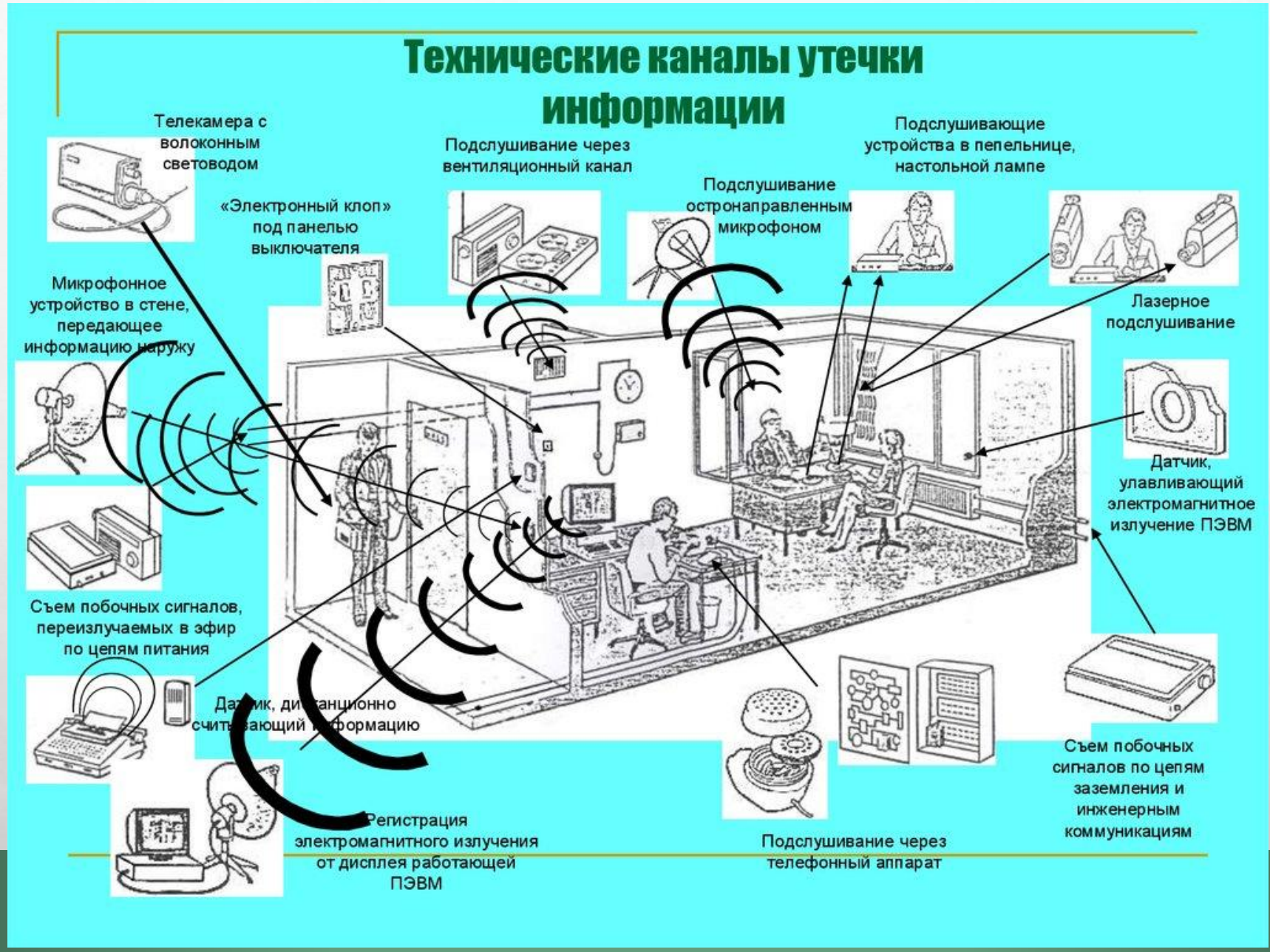


# Технические каналы утечки информации

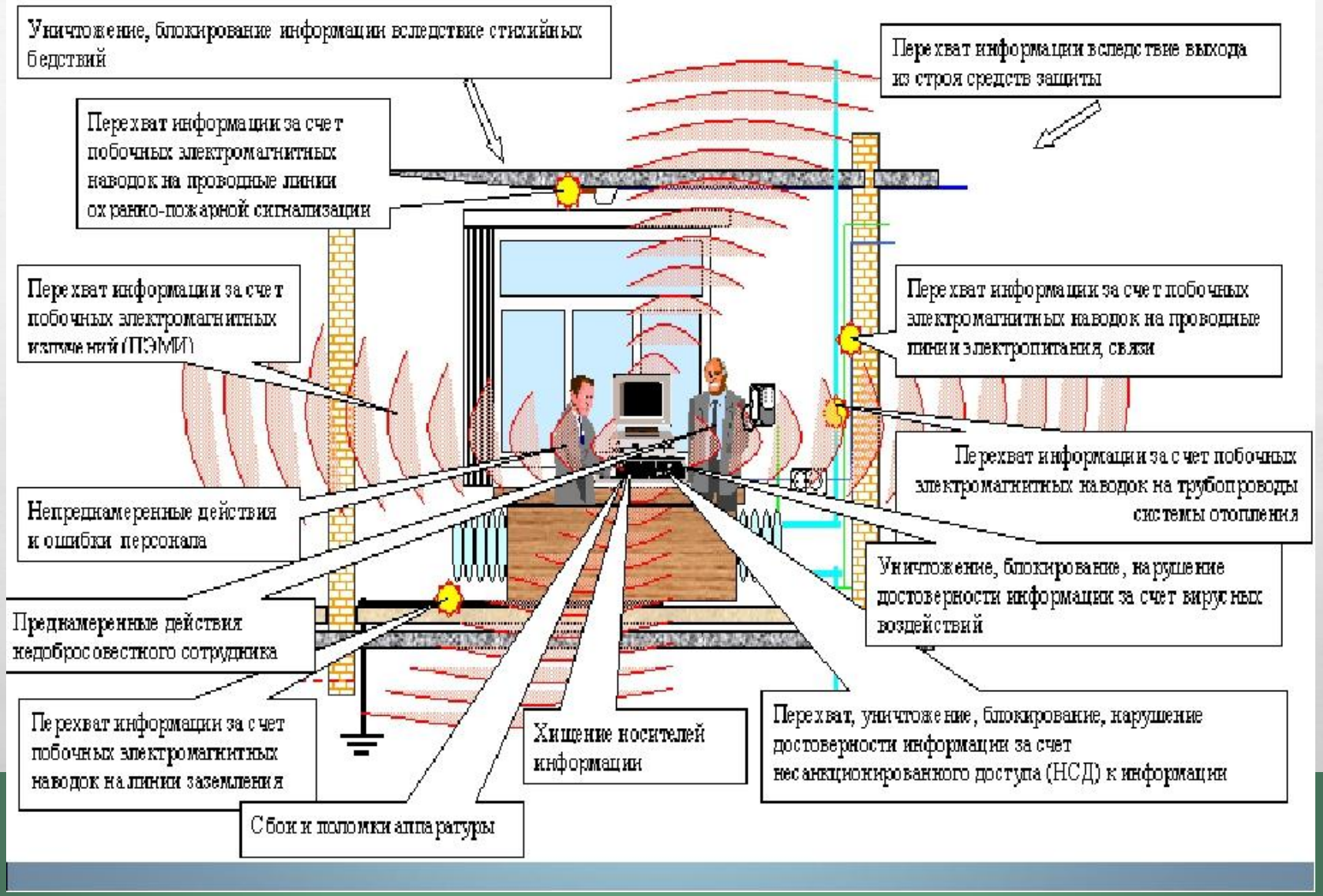
Существующие методы радиоперехвата позволяют фиксировать циркулирующую в работающих компьютерах информацию на расстоянии до нескольких сотен метров



# Технические каналы утечки информации



**Технические каналы утечки и воздействия на информацию при обработке ее техническими средствами**



# Радиоэлектронный канал утечки информации

В качестве носителей информации 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).

- Преобразователем является прибор, который преобразует изменения одной физической величины в изменения другой.
- Акустическая энергия, возникающая при разговоре, может вызвать механические колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению или изменению электромагнитного излучения.

- Наиболее чувствительными к акустическим воздействиям элементами радиоэлектронной аппаратуры являются катушки индуктивности и конденсаторы переменной емкости.

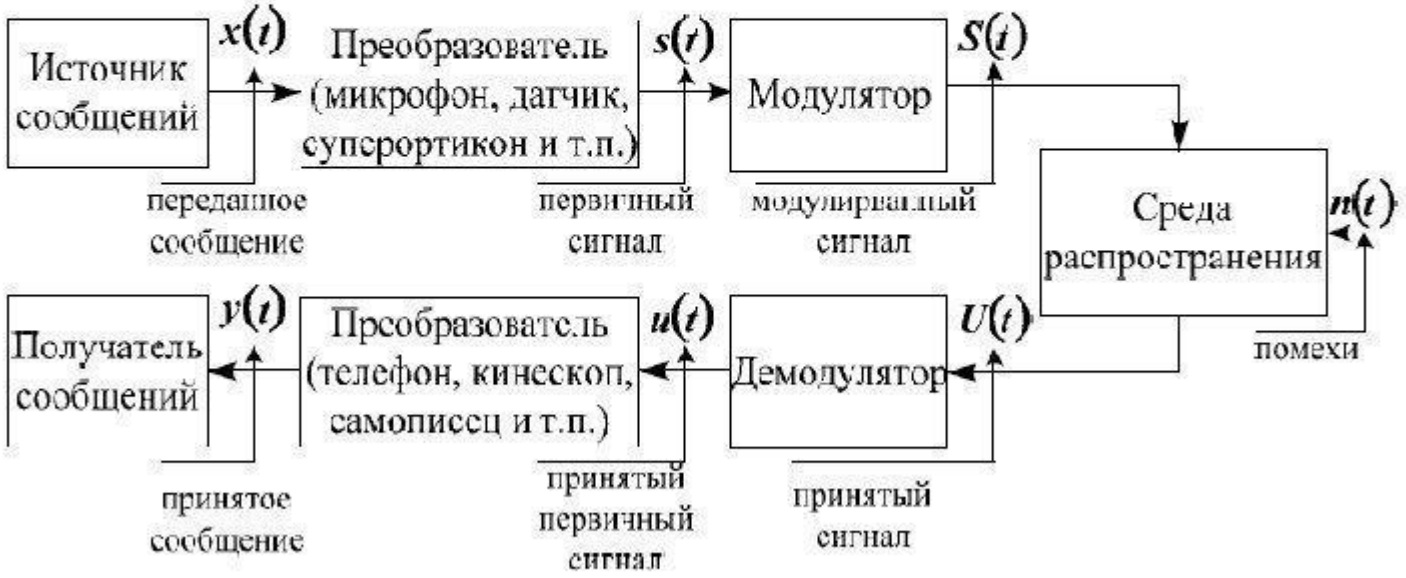
Способами непосредственного воздействия на носители защищаемой информации могут быть:
создание искусственных магнитных полей для размагничивания носителей;

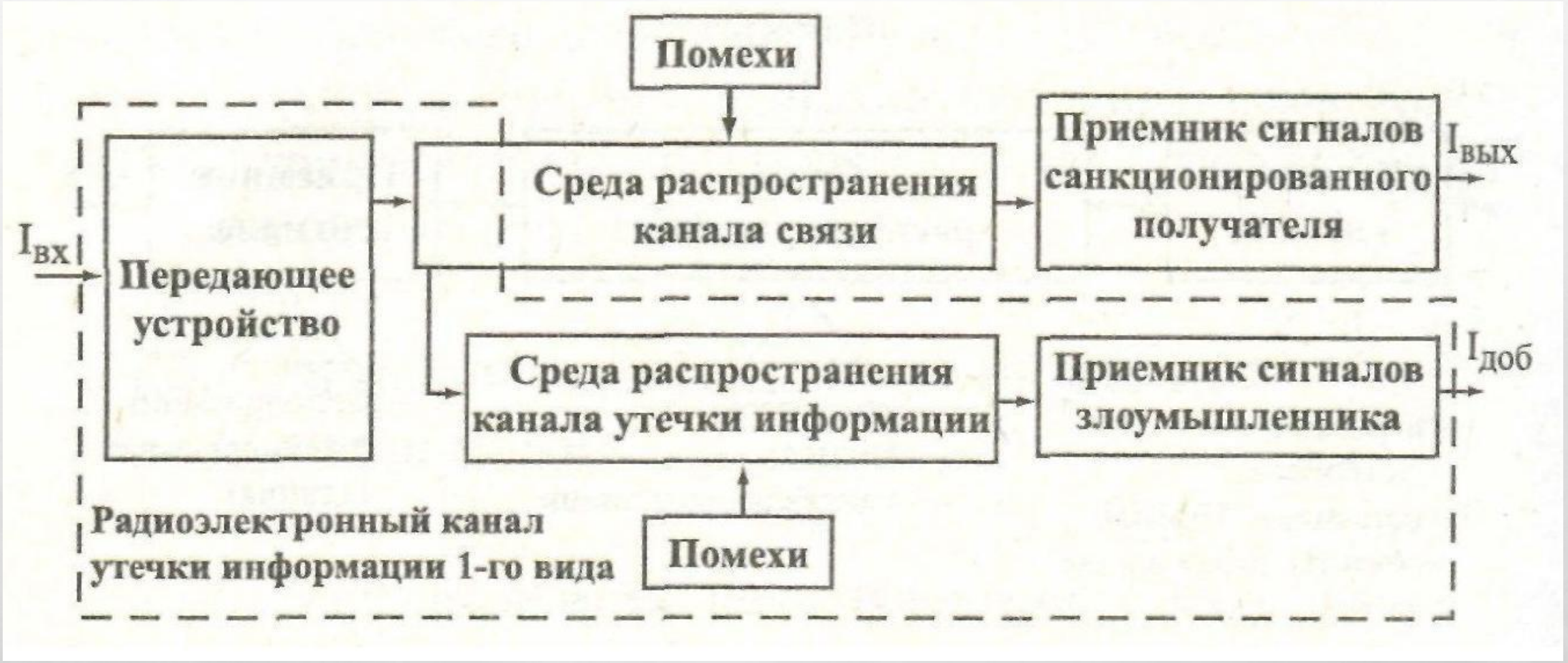
К способам вывода из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи можно отнести:
вмонтирование в ЭВМ разрушающих радио- закладок.

создание помех в радиоэфире с помощью дополнительного звукового или шумового фона, изменения (наложения) частот передачи информации;
— передача ложных сигналов;
— подключение подавляющих подавляющих фильтров в информационные цепи, цепи питания и заземления;

Эти виды дестабилизирующего воздействия приводит к реализации трех форм проявления уязвимости информации: уничтожению, искажению и блокированию.

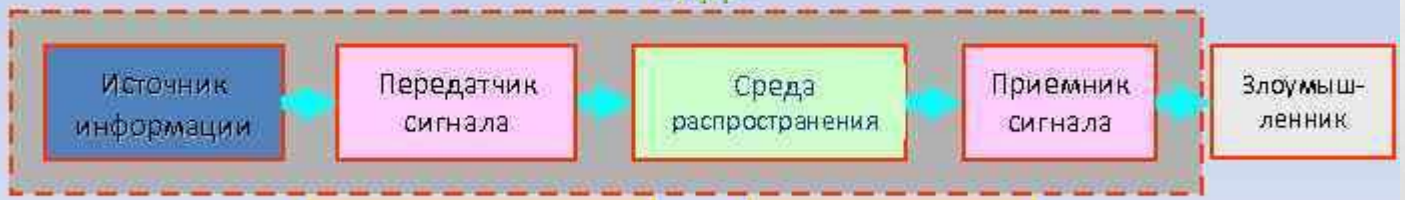
# Обобщённая структурная схема системы электросвязи – последовательность преобразования сигналов




Помехи
Среда распространения канала связи
Приемник сигналов санкционированного получателя
$I_{вых}$
$I_{вх}$
Передающее устройство
Среда распространения канала утечки информации
Приемник сигналов злоумышленника
$I_{доб}$
Радиоэлектронный канал утечки информации 1-го вида
Помехи

## Структура радиоэлектронного канала утечки информации 1-го вида


## Структура радиоэлектронного канала утечки информации 2-го вида



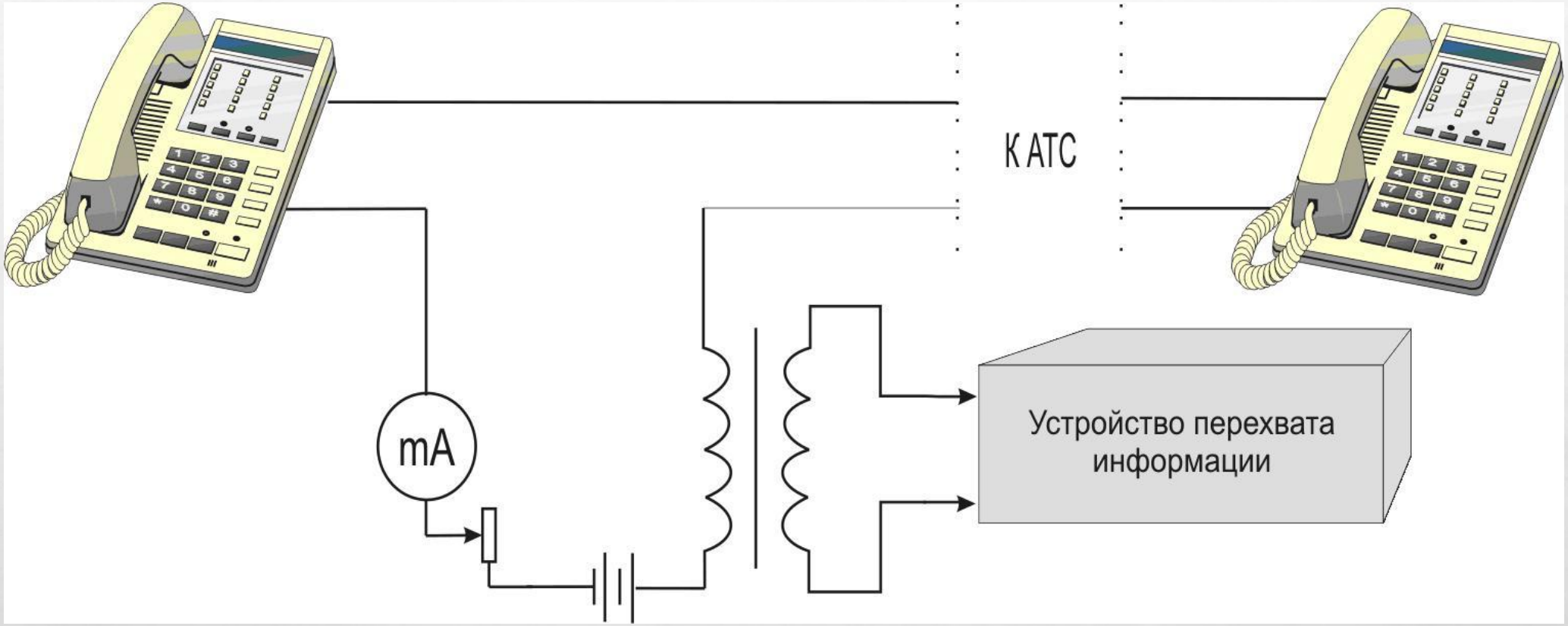

$U_{mC} = 0{,}01...0{,}1 мВ$ $P_C = 1...10 мВт$

**Передатчик такого канала утечки информации образуется случайно (безучастия источника и получателя информации) или специально создается (внедряется) – с помощью закладного устройства злоумышленником**

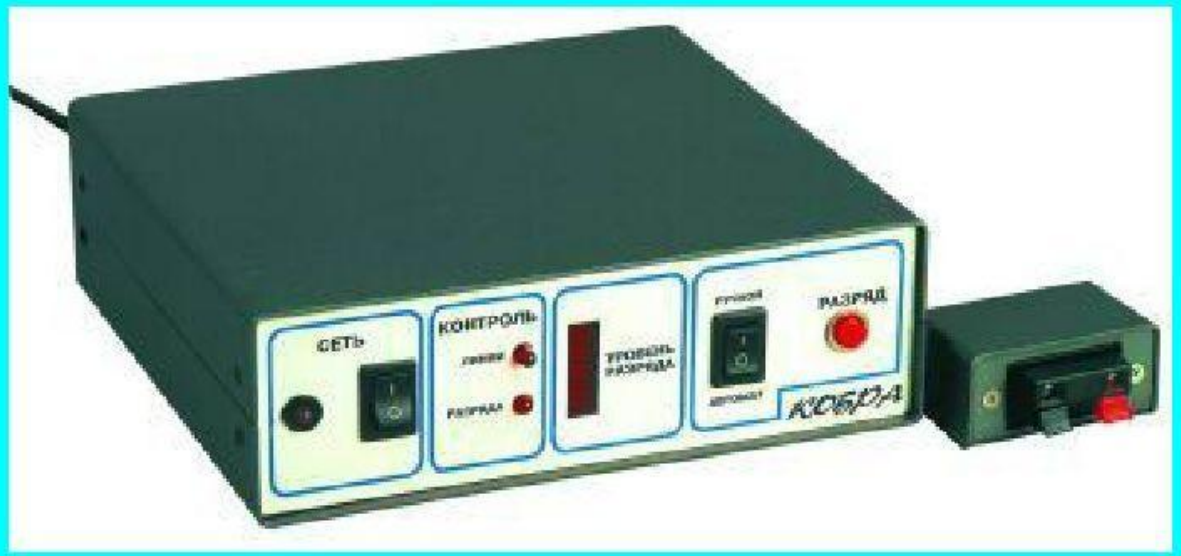
## Введение

В радиоэлектронных каналах утечки информации источники сигналов могут быть:

- передающие устройства функциональных каналов связи;
- источники побочных электромагнитных излучений и наводок (ПЭМИН);
- объекты, отражающие электромагнитные волны в радиодиапазоне;
- объекты, излучающие собственные (тепловые) электромагнитные волны в радиодиапазоне.


К АТС
mA
Устройство перехвата информации

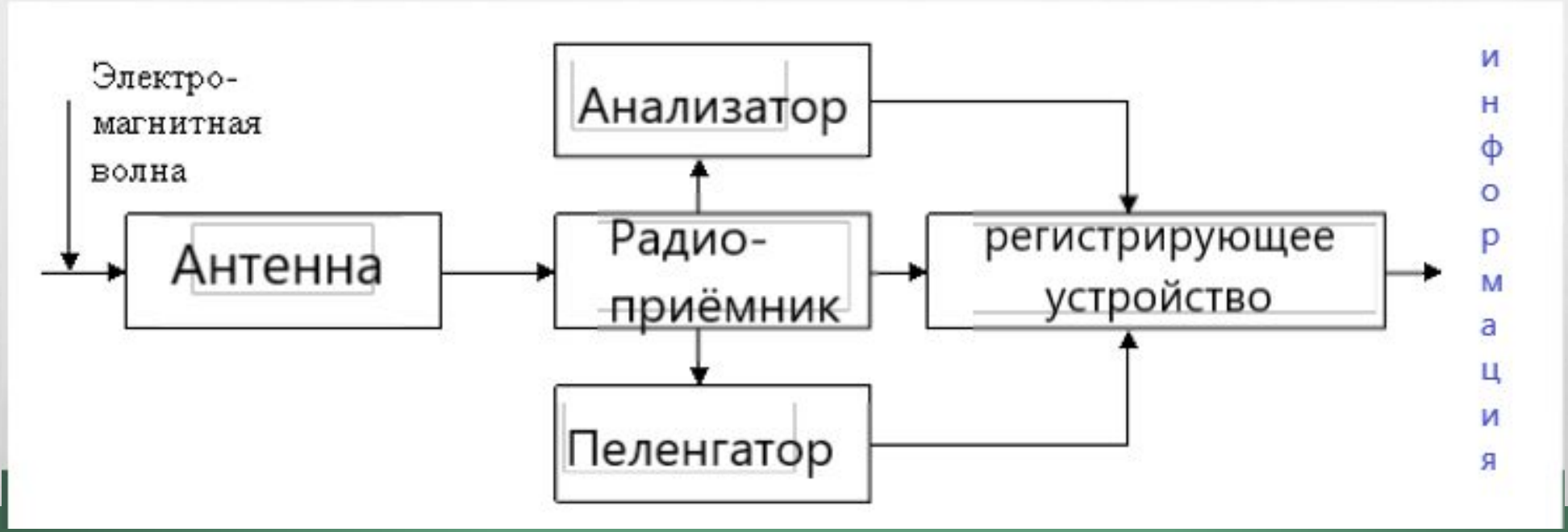

Внешний вид уничтожения электронных устройств перехвата информации: «ГИ – 1500» («Молния») (а) и «Кобра» (б)



Перехват электромагнитного, магнитного, электрического полей, а также электрических сигналов с информацией называется радио- и радиотехнической разведкой. К основным этапам перехвата можно отнести следующее:

- обнаружение сигналов в пространстве, представляющих ценность для злоумышленника;
- усиление сигналов;
- анализ *технических характеристик* принимаемых сигналов и съем информации;
- определение расположения источников сигналов.

Упрощенная схема типового комплекса для перехвата радиосигналов:



Типовой комплекс для перехвата радиосигналов включает:

- приемную антенну; * радиоприемник;
- анализатор *технических характеристик* сигнала; * радиопеленгатор;
- регистрирующее устройство.

Антенна предназначена для пространственной *селекции* и преобразования ЭМ-волны в эквивалентные электрические сигналы.
В радиоприемнике происходят поиск и отбор сигналов по частоте, усиление и демодуляция выделенных сигналов, усиление и обработка демодулированных сигналов.
Для анализа радиосигналов после *частотной селекции* и усиления они подаются на входы измерительной аппаратуры анализатора, определяющие параметры сигналов: частота, вид *модуляции*, структура кода и т.п.
Радиопеленгатор предназначен для определения направления на источник излучения и определения его координат.
Анализатор и пеленгатор могут иметь собственные радиоприемники (или их элементы) и антенны.
Регистрирующее устройство обеспечивает запись сигналов для документирования и последующей обработки.

**Электромагнитый ТКУИ** - перехват электромагнитных излучений на частотах работы передатчиков систем и средств связи. Используется для перехвата информации, передаваемой *по* каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) будет прямо пропорциональна величине мощности передатчика, высоте приемной и передающей антенн и обратно пропорциональна расстоянию ( рис. 6.3).


**Рис. 6.3.** Перехват информации по каналам радиосвязи

**Индукционный ТКУИ** – бесконтактный съем информации с кабельных линий связи. Возможность такого съема информации возникает за счет эффекта возникновения вокруг кабеля связи электромагнитного поля, модулированного информационным сигналом. Это *поле* перехватывается специальным индукционным датчиком, далее усиливается и демодулируется на аппаратуре злоумышленника. Следует отметить, что бесконтактные закладные устройства обнаружить труднее всего, так как они не изменяют характеристик канала связи.

# Индукционный канал

Используется эффект возникновения вокруг электрических цепей электромагнитного поля при прохождении по ним информационных электрических сигналов, которые перехватываются специальными индукционными датчиками.

Индукционные датчики применяются в основном для съема информации с симметричных высокочастотных кабелей.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные высокочувствительные низкочастотные усилители, снабженные магнитными антеннами.

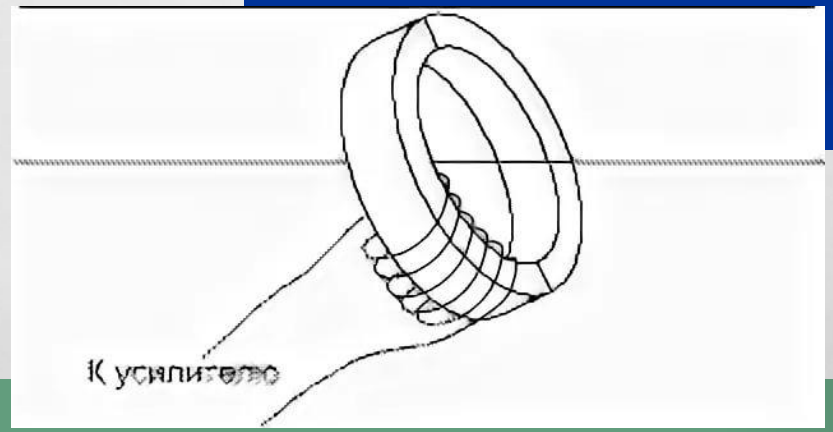



Рис. 1.21. Классификация технических каналов перехвата информации, передаваемой по каналам связи

**Электрический ТКУИ** - съем информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Для подключения аппаратуры *злоумышленник* может использовать параллельное или последовательное подключение к линии связи.

## Помехи

По характеру возникновения электромагнитные помехи разделяются на:

- Пассивные помехи создаются отражениями радиолокационных сигналов от объектов, находящихся в зоне обзора антенны прибора.
- Активные помехи представляют собой электромагнитные колебания, которые создаются каким-либо источником в диапазоне частот прибора.

В зависимости от причины возникновения на:

- Естественные (неорганизованные)
  - Пассивные помехи - это отражения от земной и морской поверхностей; местных предметов
  - Активные помехи - это воздействия на антенны и приемники электромагнитных сигналов других радиосистем, работающих в том же диапазоне радиоволн.
- Умышленные (организованные).

Кроме того существуют и комбинированные помехи.

# Радиопомехи

### Радиоэлектронные помехи

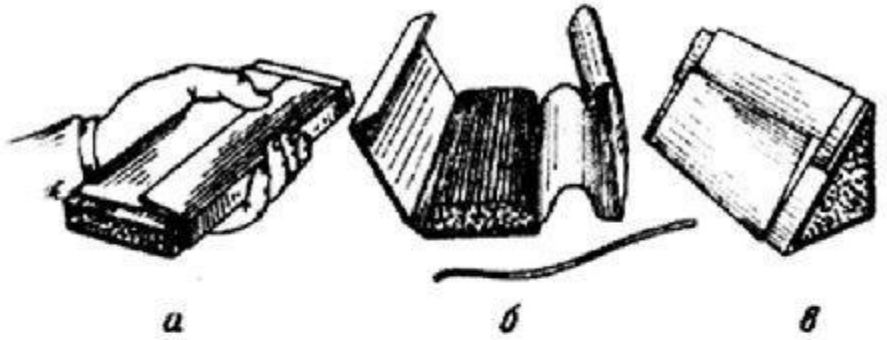
- Радиопомехи - электромагнитные излучения, затрудняющие или исключающие прием радиосигналов и выделение из них полезной информации радиоэлектронными средствами.

- Радиопомехи различаются:
  - по происхождению;
  - по способу формирования;
  - по эффекту воздействия;
  - по соотношению ширины спектра помех и сигналов;
  - по интенсивности и направленности излучения.

Являются одним из средств радиоэлектронной борьбы (РЭБ)

# Пассивные помехи в виде металлизированных лент

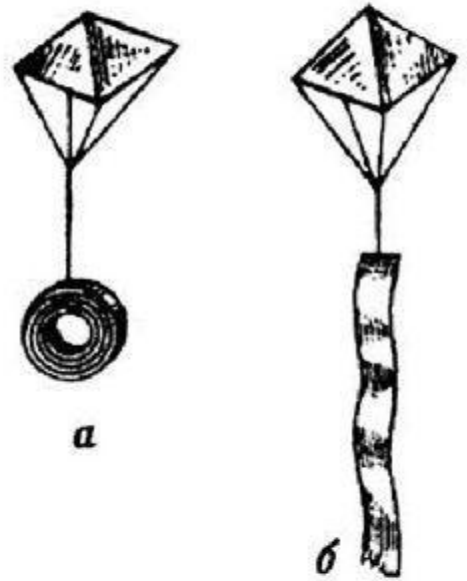
Если длина ленты равна половине длины волны электромагнитного колебания, то вследствие резонансных явлений в ленте возбуждаются интенсивные колебания, и она становится вторичным излучателем электромагнитной энергии.



*а* *б* *в*

Так как эффективность воздействия одиночного отражателя весьма невелика, то ленты укладываются в пачки и сбрасываются с самолета пачками. На рисунке показано, как выглядели эти пачки.

Длинные (до 50 – 100 м) металлизированные ленты, сбрасываемые на небольших парашютиках для увеличения времени их опускания.



*а* *б*

Такие ленты были удобны тем, что они оказывали влияние сразу на все радиолокационные станции независимо от их диапазона.

**Аппаратура для борьбы с пассивными помехами основана на априорном знании отличий свойств помех от свойств полезных сигналов.**

**Основные различия сигналов целей и пассивных маскирующих помех**

***1. Распределенный характер мешающих отражателей и близкий к сосредоточенному — блестящих элементов цели.***

***2. Отличия в поляризации отраженных сигналов***

***3. Различия в скорости перемещения мешающих отражателей и цели.***

**Основное различие сигналов заложено в частотах отраженных сигналов и обусловлено разными радиальными составляющими скоростей движения цели и источников пассивных помех. Различия в радиальных скоростях целей и отражателей имеются и могут быть использованы для селекции по скорости.**

**Селекцию по скорости (иначе по эффекту движения цели) называют *селекцией движущихся целей* (СДЦ).**

Основным признаком, по которому отличаются движущиеся и неподвижные объекты, является различная **величина доплеровского сдвига частоты высокочастотного заполнения отраженного сигнала**.

**Активные помехи.**

Активные помехи создаются передатчиком помех, которые настраиваются на частоты подавляемой РЭС противника. Эффект подавления достигается за счет превышения мощности помехи над мощностью сигнала на входе приемного устройства, подавляемой РЭС, либо за счет выбора параметров помеховых сигналов (соответствующей модуляции помехового сигнала).

На рис. 1 представлен типичный случай создания активных помех. Самолет-поставщик помех (ПП) прикрывает помехами самолет цель (Ц) от ПВО. В зависимости от вида помех эффект прикрытия может быть различным. Сигнал нельзя полностью прикрыть, его можно или замаскировать помехой, или подделать. Отсюда имеются два вида помех:

- маскирующие помехи, с помощью которых отметка цели маскируется так, что её невозможно выделить на фоне помех;
- имитирующие помехи, создающие на экранах РЛС отметки, аналогичные отметкам цели.

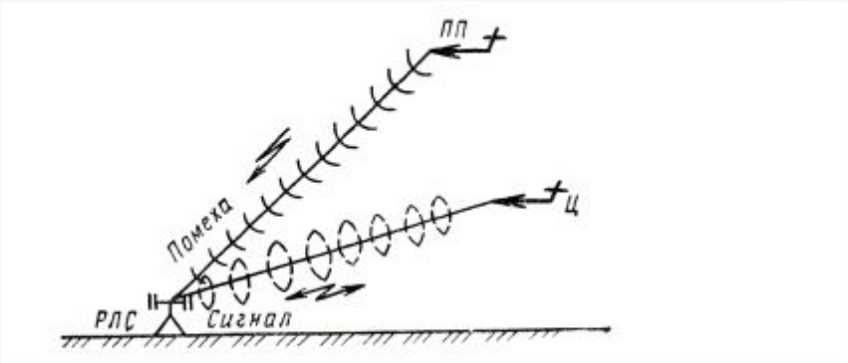



Рис. 1. Принцип создания помех наземным РЛС (Ц – цель, ПП – поставщик помех)


Ю.М. Перунов, К.И. Фомичев, Л.М. Юдин
РАДИОЭЛЕКТРОННОЕ ПОДАВЛЕНИЕ ИНФОРМАЦИОННЫХ КАНАЛОВ СИСТЕМ УПРАВЛЕНИЯ ОРУЖИЕМ


БЛА
Радиоподавление канала управления БЛА
30 км
Радиоразведка канала передачи данных
50 км
Канал передачи данных разведки/телеметрии
Канал управления
Радиоподавление и дезинформация бортовых приемников GPS/GLONASS
40 км
10 км
Радиоподавление канала передачи данных разведки/ телеметрии от БЛА
10 км
Радиоразведка канала управления БЛА
Гроза-С
Наземный пункт управления БЛА

**РАДИОЭЛЕКТРОННЫЕ ПОМЕХИ**

Определение понятия « радиоэлектронные помехи»

Радиоэлектронные помехи — это непоражающие электромагнитные или акустические излучения, которые ухудшают качество функционирования РЭС, управляемого оружия и военной техники или систем обработки информации. Воздействуя на приемные устройства, помехи имитируют или искажают наблюдаемые и регистрируемые оконечной аппаратурой сигналы или изображения, затрудняют или исключают выделение полезной информации, ведение радиопереговоров и обнаружение целей с помощью РЭС, снижают их дальность действия и точность работы автоматических систем управления. Под действием помех РЭС и системы могут перестать быть источниками информации, несмотря на их полную исправность и работоспособность.

Так как подавить разнообразные РЭС помехами одного вида невозможно, то применяют специальные их виды, предназначенные для подавления радиолокации, радионавигации, радиосвязи, лазерной, инфракрасной техники и т. д. Более того, для подавления средств одного и того же класса, но использующих различные виды сигналов и способы их обработки, применяются отличающиеся друг от друга виды помех.

По эффекту воздействия на РЭС различают маскирующие и имитирующие помехи. Маскирующие помехи ухудшают характеристики приемного устройства РЭС, что увеличивает количество принятых символов, снижающих информативность сообщения, создают фон, на котором затрудняется или полностью исключается обнаружение, распознавание, выделение полезных сигналов или отметок целей. С увеличением мощности помех их маскирующее действие возрастает.

Имитирующие (дезинформирующие) помехи — это сигналы, излучаемые станцией помех для внесения ложной информации в подавляемые средства. По структуре они близки к полезным сигналам и поэтому создают в оконечном устройстве РЭС сигналы или отметки ложных целей, подобные реальным, снижают пропускную способность системы, вводят в заблуждение операторов, приводят к потере части полезной информации, увеличивают вероятность ложной тревоги. Воздействуя на средства управления оружием, они срывают автоматическое сопровождение целей по направлению, дальности, скорости и перенацеливают их на цели, имитируемые помехой, а также вызывают ошибки сопровождения цели. При воздействии имитирующих помех характеристики приемного устройства не ухудшаются.

Эффект воздействия помех сказывается в ухудшении качества обрабатываемой информации в результате ее разрушения либо старения, что увеличивает степень неопределенности при принятии решений.


КАМАЗ