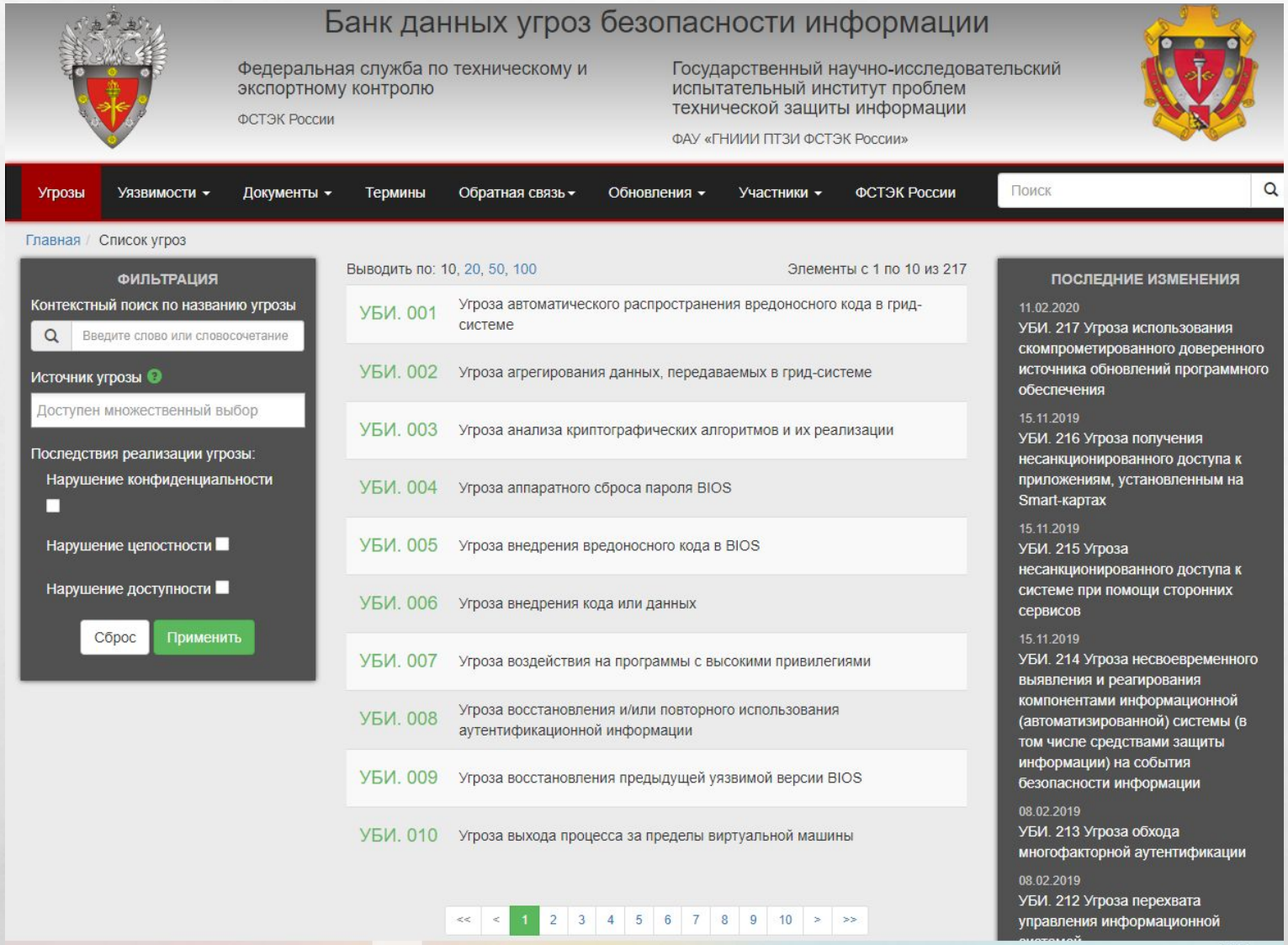
ФИЗИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОННЫХ СПОСОБОВ ВОЗДЕЙСТВИЯ УГРОЗ НА ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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
- 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
- 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.).

ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 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.

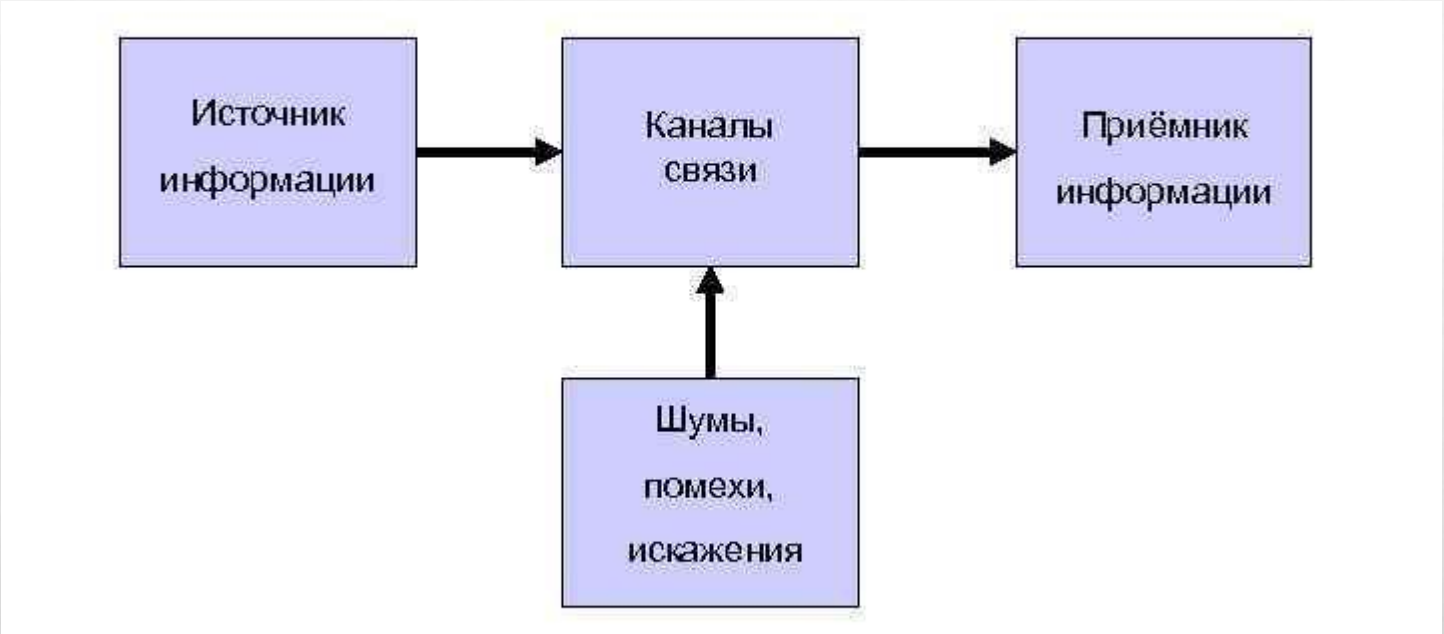
РАДИОЭЛЕКТРОННЫЕ СПОСОБЫ ВОЗДЕЙСТВИЯ УГРОЗ:

- 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.

РАДИОЭЛЕКТРОННЫЕ СПОСОБЫ ВОЗДЕЙСТВИЯ УГРОЗ:

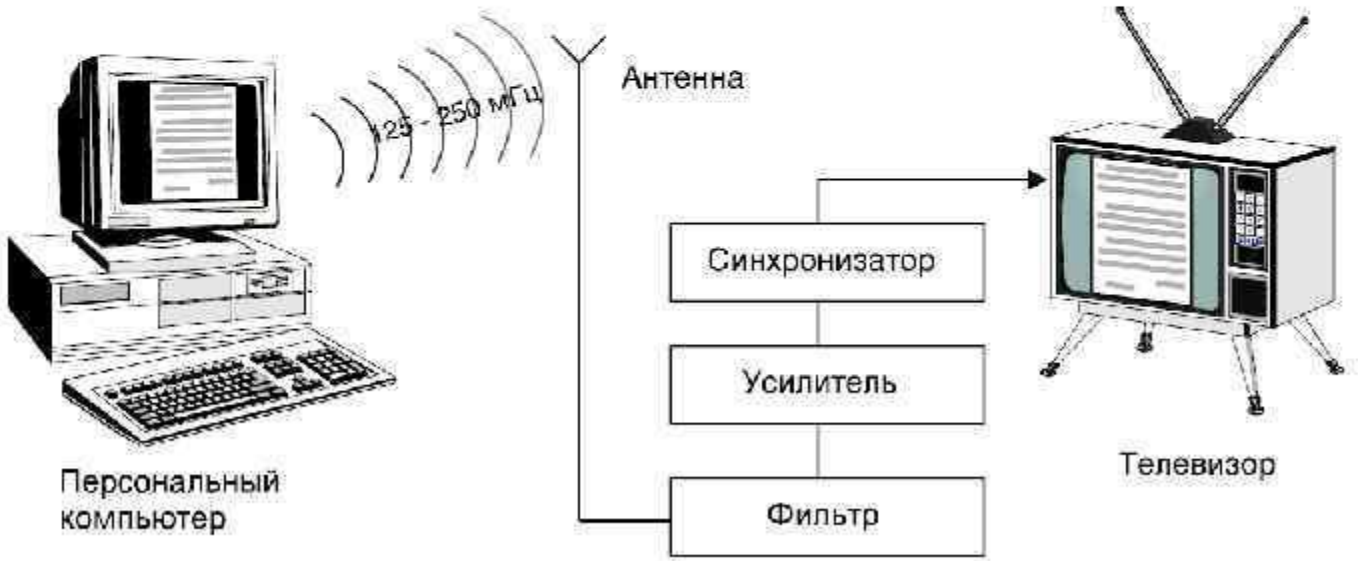
- перехват информации в технических каналах её утечки (за счет побочных электромагнитных излучений, создаваемых техническими средствами обработки и передачи информации за счет наводок в коммуникациях, сети питания, заземления, радиотрансляции, пожарной и охранной сигнализаций и т.д.) и в линиях связи 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

СТРУКТУРА СЕТИ ПЕРЕДАЧИ ДАННЫХ

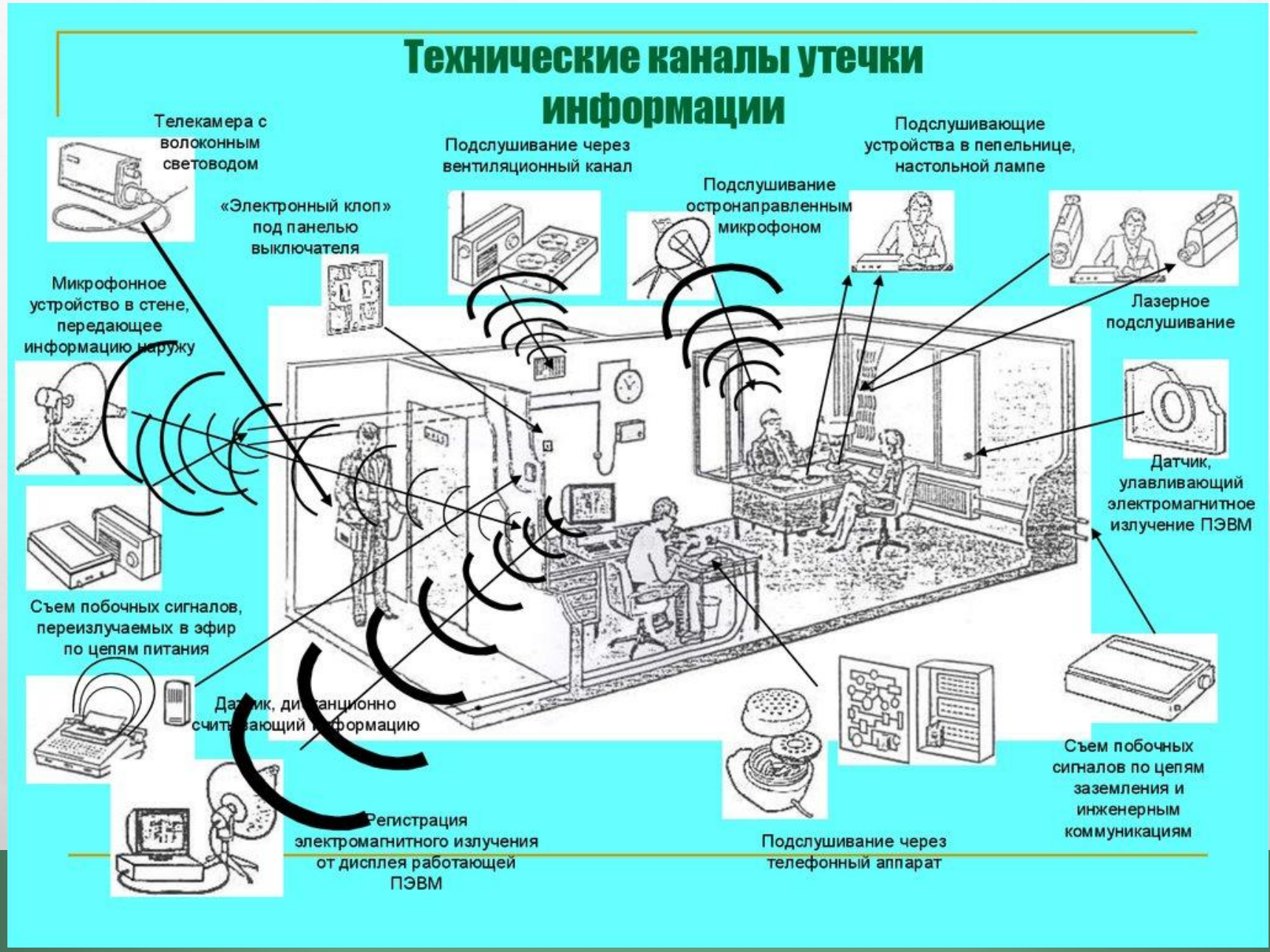


Технические каналы утечки информации

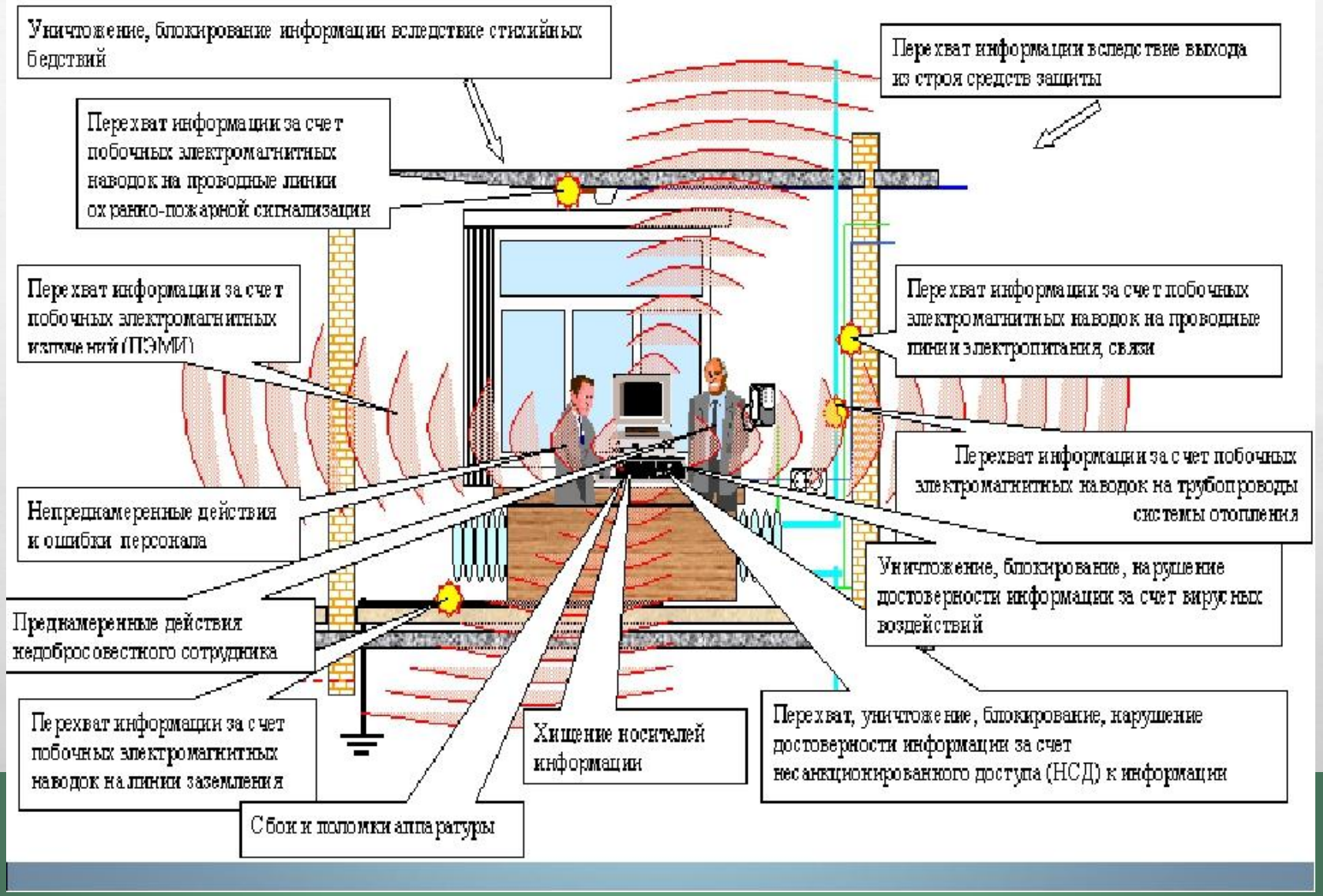
Существующие методы радиоперехвата позволяют фиксировать циркулирующую в работающих компьютерах информацию на расстоянии до нескольких сотен метров



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.