
Курс: **эксплуатация подсистем безопасности АС**

# Тема: **Средства защиты информации**

Преподаватель: Пятков Антон Геннадьевич

Красноярск

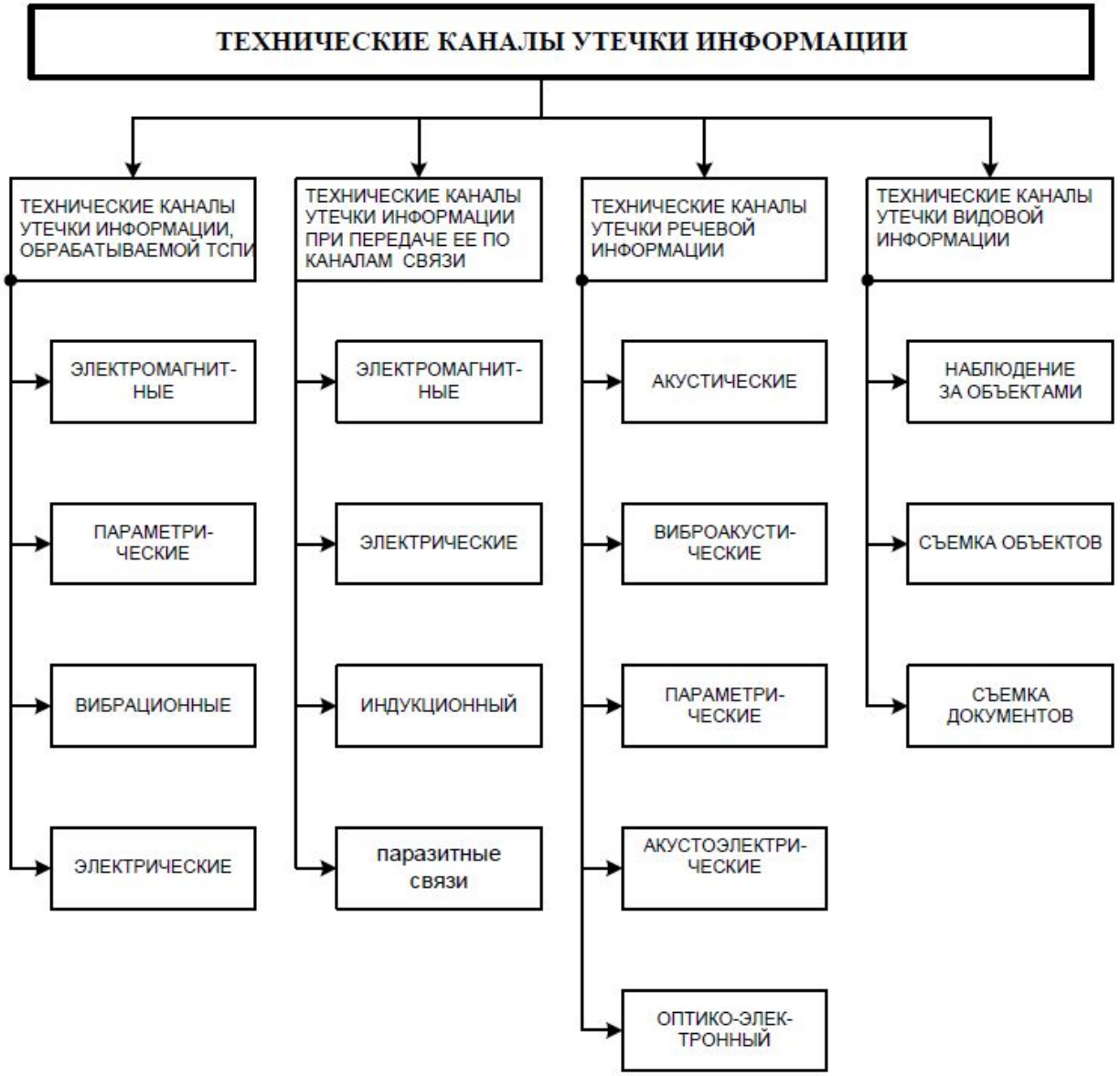
# ТКУИ

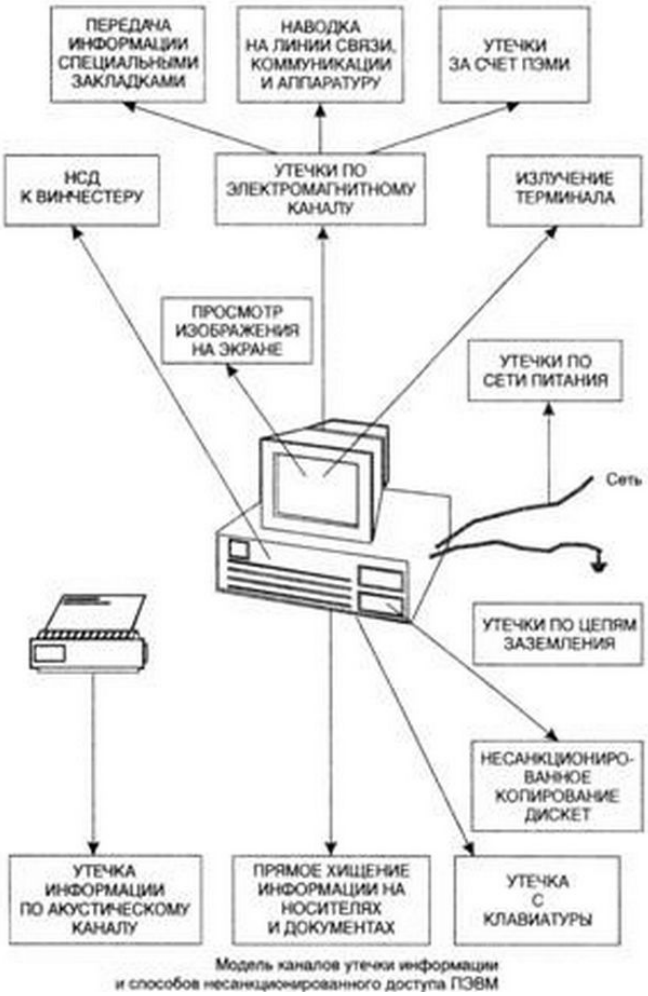
Технические каналы утечки информации (ТКУИ) – совокупность объекта разведки, технического средства разведки и физической среды, в которой распространяется информационный сигнал.

В сущности, под ТКУИ понимают способ получения с помощью технических средств разведки разведывательной информации об объекте.

Особенности ТКУИ определяются физической природой информационных сигналов и характеристиками среды распространения сигналов утекаемой информации.

# ТКУИ



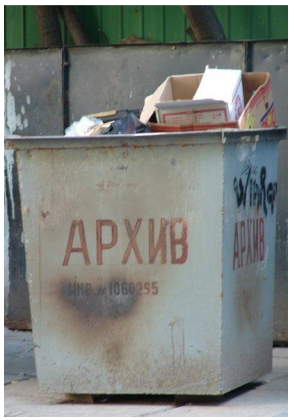
Модель каналов утечки информации и способов несанкционированного доступа ПЭВМ

# Шпионаж

Материально-вещественный канал

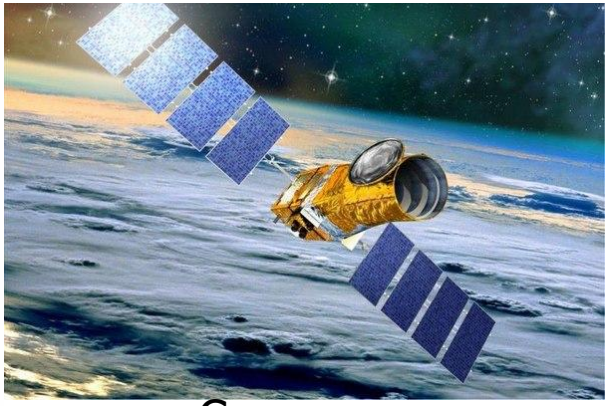
По уголовному законодательству РФ различаются шпионаж:

- ✔ как самостоятельное преступление (ст. 276 УК РФ);
- ✔ как форма государственной измены (ст. 275 УК РФ).




Шпионаж по назначению делим на:

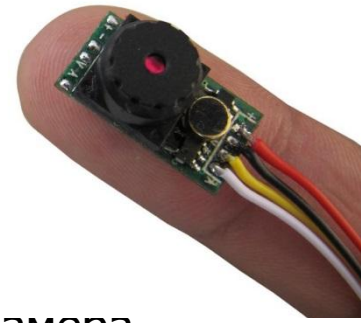
- ✔ политический (военная разведка: стратегическая, тактическая);
- ✔ промышленный шпионаж (экономическая, бизнес-разведка);
- ✔ добывание сведений об организованной преступности, международных террористических организациях и подготавливаемых за рубежом государственных переворотах.

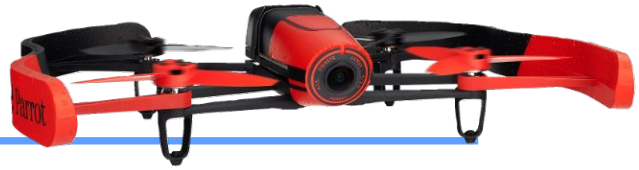
Спутники

ПЭМИ

Видеокамера

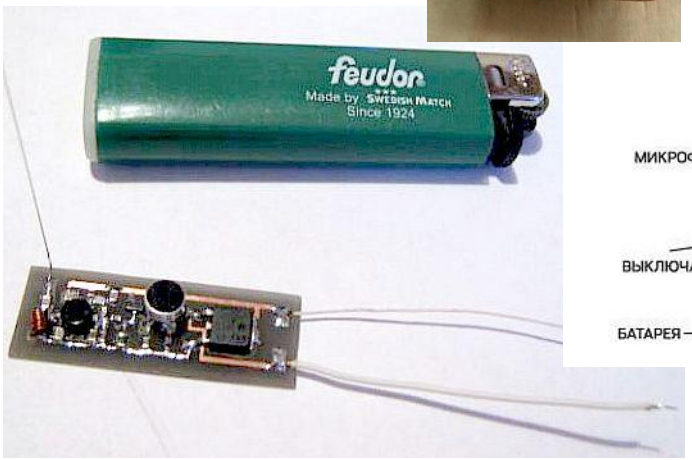


# Шпионаж



К методам шпионажа и диверсий относятся:

- ✔ подслушивание;
- ✔ визуальное наблюдение;
- ✔ хищение документов и МНИ;
- ✔ хищение программ и атрибутов системы защиты;
- ✔ сбор и анализ отходов (бумаги, МНИ, отходы);
- ✔ подкуп и шантаж сотрудников;
- ✔ поджоги;
- ✔ взрывы.


Закладные устройства


# Защита от шпионажа

Для защиты от традиционного шпионажа и диверсий должны быть решены задачи:

- ✔ создание системы охраны объектов;
- ✔ организация работ с конфиденциальными ресурсами на объекте КС;
- ✔ противодействие наблюдению;
- ✔ противодействие подслушиванию;
- ✔ защита от злоумышленных действий персонала.

Состав системы охраны зависит от охраняемого объекта. В общем случае:

- ✔ инженерные конструкции (установка оконных решеток; применение стекол, устойчивых к механическому воздействию; закаливание стекол; изготовление многослойных стекол; применение защитных пленок);
- ✔ охранная сигнализация (охват всей КЗ; чувствительность; надежная работа в любых погодных/временных условиях; устойчивость к естественным помехам; быстрота и точность определения места нарушения; контроль);
- ✔ средства наблюдения (автоматизированное видеонаблюдение; контроль за действиями персонала; видеозапись действий нарушителей; видеоохрана);
- ✔ подсистема доступа на объект (КПП, идентификаторы доступа);
- ✔ дежурная смена охраны (её состав, экипировка, место размещения).

# Защита от шпионажа

Для противодействия хищениям документов, МНИ, атрибутов систем защиты, изучению отходов, документов и МНИ, противодействия созданию неучтенных копий документов необходимо определять порядок учета, хранения, выдачи, работы и уничтожения носителей информации.

Для этого в каждой организации должны быть:

- ✔ разграничены полномочия дежурных лиц по допуску их к ресурсам;
- ✔ определены и оборудованы места хранения/работы конф. ресурсов;
- ✔ установлен порядок учета/выдачи/работы/сдачи на хранение конф.ресурсов;
- ✔ назначены ответственные лица, определены их полномочия и обязанности;
- ✔ организован сбор и уничтожение ненужных документов и списанных МНИ;
- ✔ контроль выполнения установленного порядка работы с конф. ресурсами.

Для противодействия наблюдению в оптическом диапазоне используются:

- ✔ оконные стекла с односторонней проводимостью света;
- ✔ шторы и защитные окрашивания стекол;
- ✔ корректное размещение рабочих столов, мониторов, табло и плакатов;
- ✔ двери, шторы и пр. закрывается при обработке данных.

# Защита от шпионажа

Методы борьбы с подслушиванием делят на 2 группы:

1) методы защиты речевой информации при передаче её по каналам связи (защищается с использованием методов аналогового скремблирования и дискретизации речи с последующим шифрованием).

Скремблирование – изменение характеристик речевого сигнала таким образом, что полученный модулированный сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает такую же полосу частот спектра, как и исходный открытый.

Применяются способы частотного преобразования сигналов: частотная инверсия спектра сигнала; частотная инверсия спектра сигнала со смещением несущей частоты; разделение полосы частот речевого сигнала на поддиапазоны с последующей перестановкой и инверсией;

2) методы защиты информации от прослушивания акустических сигналов в помещениях:

- ✔ звукоизоляция и звукопоглощение акустического сигнала;
- ✔ зашумление помещений или твердой среды для маскировки акустических сигналов;
- ✔ защита от несанкционированной записи речевой информации на диктофон;
- ✔ обнаружение и изъятие закладных устройств.

# 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 по ТКУИ


Акустический сейф "Ладья"

Нелинейный локатор

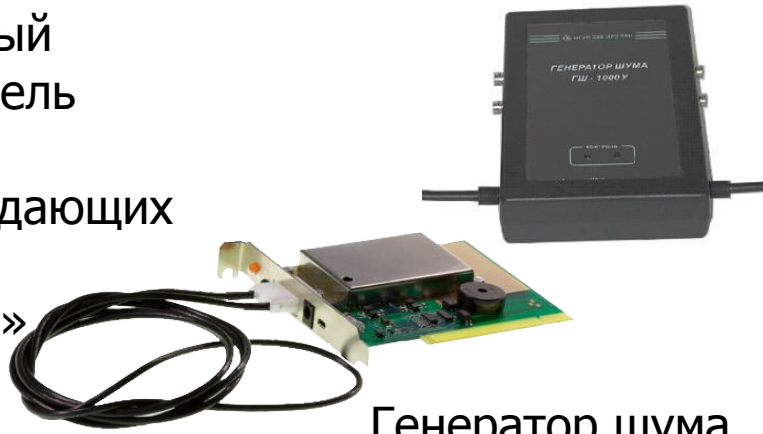

**«МОРФЕЙ-МК»** предназначен для блокирования возможности организации связи между базовыми станциями (дальность подавления до 50 метров)


Эндоскоп, зеркала

# СЗИ от утечки по ТКУИ

Сетевые генераторы шума СОПЕРНИК


Селективный обнаружитель цифровых радиопередающих устройств «Скорпион»




Генератор шума ГШ-К-1000


Стационарные шумогенераторы ГНОМ-3М

Компьютеризированный металлодетектор «КОРНЕТ»

Селективный обнаружитель оружия в ручной клади «РУБЕЖ»

Портативная рентгенотелевизионная установка «НОРКА»

# 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»

# Средства ЗИ в АС по РД ГТК

1. Подсистема управления доступом:

1.1. Идентификация, проверка подлинности и контроль доступа субъектов:

- к системе (к АС);
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам;
- к программам;
- к томам, каталогам, файлам, записям, полям записей;

1.2. Управление потоками информации;

2. Подсистема регистрации и учета:

2.1. Регистрация и учет:

- входа (выхода) субъектов доступа в (из) систему (узел сети);
- выдачи печатных (графических) выходных документов;
- запуска (завершения) программ и процессов (заданий, задач);
- доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;
- доступа программ, субъектов доступа к терминалам/ЭВМ/узлам сети ЭВМ/ каналам связи/внешним устройствам ЭВМ/программам/томам/каталогам/ файлам/записям/полям записей;
- изменения полномочий субъектов доступа;
- создаваемых защищаемых объектов доступа;

# Средства ЗИ в АС по РД ГТК

2.2. Учет носителей информации:

2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей;

2.4. Сигнализация попыток нарушения защиты;

3. Криптографическая подсистема:

3.1. Шифрование конфиденциальной информации;

3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах;

3.3. Использование аттестованных (сертифицированных) СКЗИ;

4. Подсистема обеспечения целостности:

4.1. Обеспечение целостности программных средств и обрабатываемой в АС информации;

4.2. Физическая охрана средств вычислительной техники и носителей информации;

4.3. Наличие администратора (службы) защиты информации в АС;

4.4. Периодическое тестирование СЗИ НСД;

4.5. Наличие средств восстановления СЗИ НСД;

4.6. Использование сертифицированных средств защиты.