Государственное бюджетное профессиональное образовательное учреждение
г. Москвы
Колледж связи № 54
им. П.М. Вострухина

ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МДК 02.02 «Инженерно-техническая защита информации"

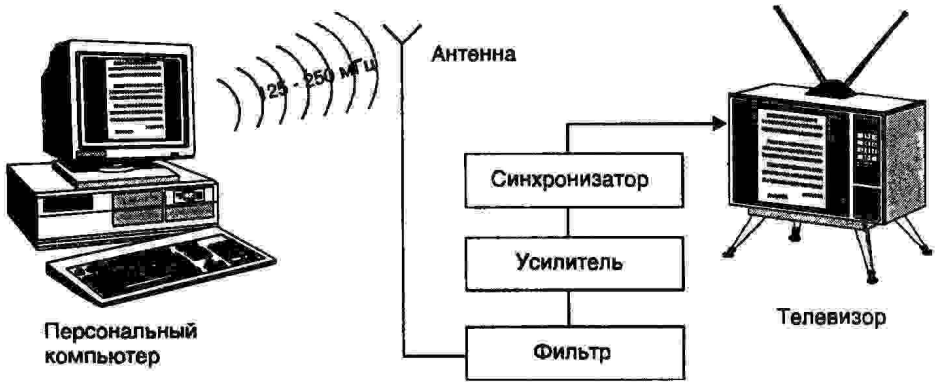
РАЗДЕЛ 3. Средства защиты информации Тема 1. Типы электронных устройств и алгоритмы обнаружения специальных технических средств

МОСКВА 2015

ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель занятия:

Изучить классификацию всех известных специальных технических средств негласного получения информации, принципы и особенности их работы, рассмотреть основные алгоритмы обнаружения таких средств, а также уяснить порядок проведения поисковых мероприятий



Лаборатория Информационной Безопасности

Учебные вопросы:

1. Специальные средства негласного получения информации и их классификация.

2. Методы обнаружения специальных технических средств.

3. Организация проведения поисковых мероприятий

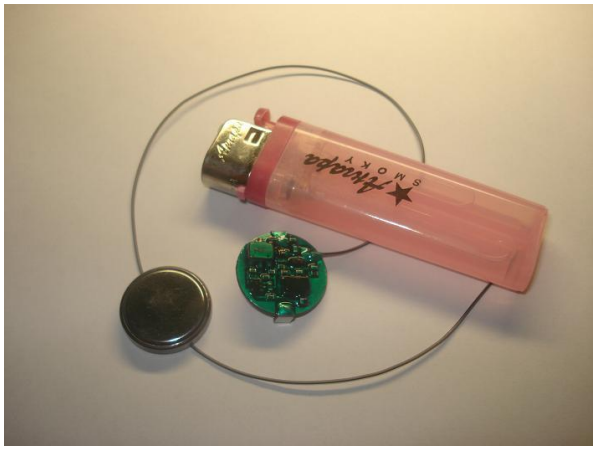
Лаборатория Информационной Безопасности

Специальные средства негласного получения информации и их классификация

Лаборатория Информационной Безопасности

Специальные технические средства негласного получения информации

У злоумышленников есть достаточно большой выбор средств для несанкционированного получения конфиденциальной информации.



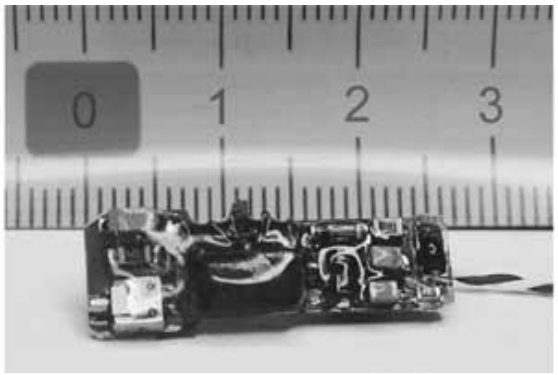
Одни удобны благодаря простоте установки, но, соответственно, также легко могут быть обнаружены. Другие очень сложно разыскать, но их непросто и установить.

Лаборатория Информационной Безопасности

1. По способу передачи информационного сигнала:

- радиоканалы

а) **радиозакладки** - электронные устройства перехвата акустической (речевой) информации, использующие для передачи информации радиоканал. Они являются одними из доступных и распространенных средств акустической разведки.



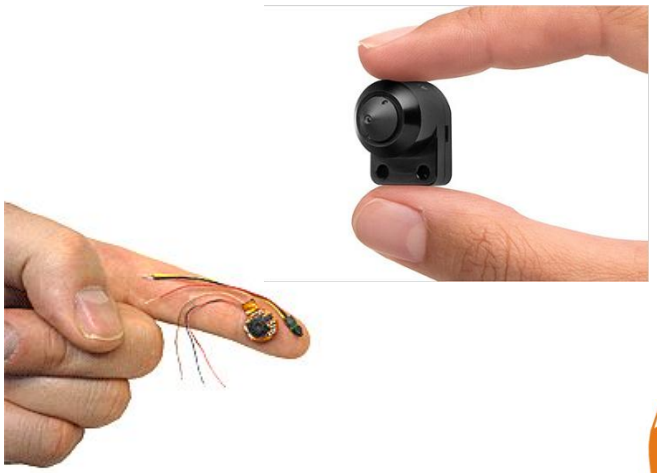
б) **беспроводные видеокамеры**

СТС являются видеокамеры, обладающие по крайней мере одним из следующих признаков:

закамуфлированные под бытовые предметы;

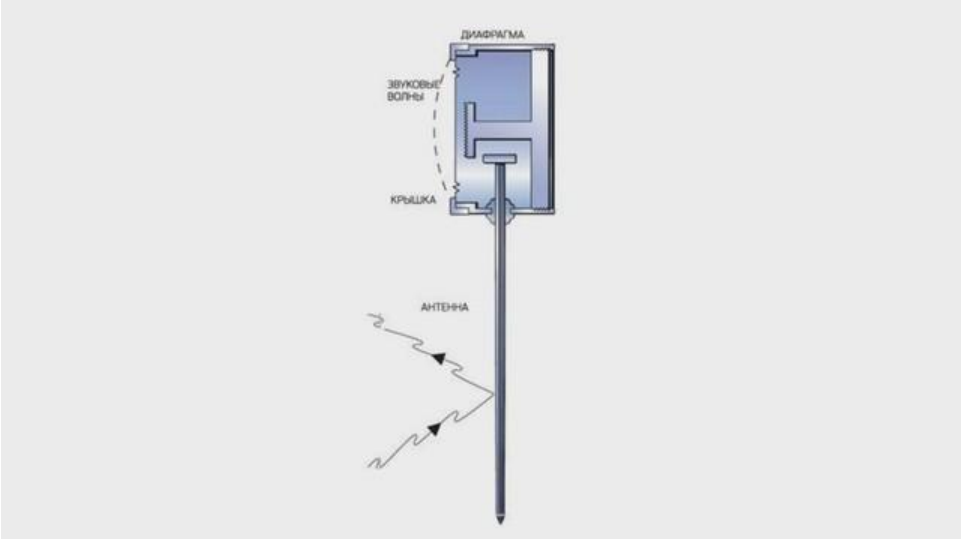
имеющие вынесенный зрачок входа (PIN-HOLE);

работающие при низкой освещенности объекта или при низкой освещенности на приемном элементе.



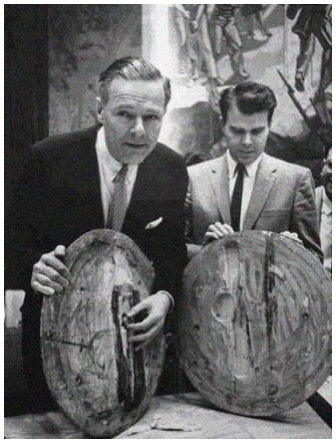
Классификация технических средств негласного получения информации

в) **эндовибратор** - это миниатюрное электронное устройство, у которого отсутствует источник питания, передатчик и микрофон. Основой его является цилиндрический объемный резонатор, настроенный на внешнее излучение определенной частоты, чаще всего в диапазоне 300 Мега Герц.



Лаборатория Информационной Безопасности

Дополнительная информация



В конце 1943 года Сталину сообщили, что советский электротехник Лев Термен (находясь в то время в заключении) изобрел уникальное подслушивающее устройство – эндовибратор. Под влиянием человеческого голоса в помещении меняется характер колебаний, которые и мог фиксировать эндовибратор. Устройство записывало колебания на пленку, после чего их восстанавливали специальным образом и записи превращались в первоначальную речь.

Жучок «Златоуст» отработал в кабинете посольства **8 лет !!!**, пережив 4-х разных послов США. Примечательно, что каждый вновь назначенный посол в Москве стремился изменить интерьер комнаты, чтобы он максимально гармонировал с советским презентом, настолько изящным и качественным он был.

Лаборатория Информационной Безопасности

Классификация технических средств негласного получения информации

- проводные линии

а) **сеть переменного тока,** 220 В

б) **слаботочные линии,** (U= до 70В).

Сетевые микрофоны

- инфракрасный диапазон

Инфракрасные **прослушивающие устройства** - это устройства, которые передают информацию по оптическому каналу в инфракрасном, то есть невидимом глазу спектре. Инфракрасный передатчик может преобразовать акустические колебания в световые, а затем передать информацию на специальное принимающее устройство - приемник оптического излучения.

Лаборатория Информационной Безопасности

2. По наличию системы голосовой активации:

- с системой VOX

VOX — активация голосом. В этом режиме работающая на прием станция автоматически переходит в режим передачи PTT при начале вашей речи. При окончании речи рация опять переходит в режим приема. Уровень срабатывания «громкость голоса» регулируется.

- без системы VOX

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОСТАНОВЛЕНИЕ
от 10 марта 2000 г. N 214

ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О ВВОЗЕ В РОССИЙСКУЮ ФЕДЕРАЦИЮ И ВЫВОЗЕ ИЗ РОССИЙСКОЙ ФЕДЕРАЦИИ СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ, И СПИСКА ВИДОВ СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ, ВВОЗ И ВЫВОЗ КОТОРЫХ ПОДЛЕЖАТ ЛИЦЕНЗИРОВАНИЮ

2. Специальные технические средства для негласного визуального наблюдения и документирования:

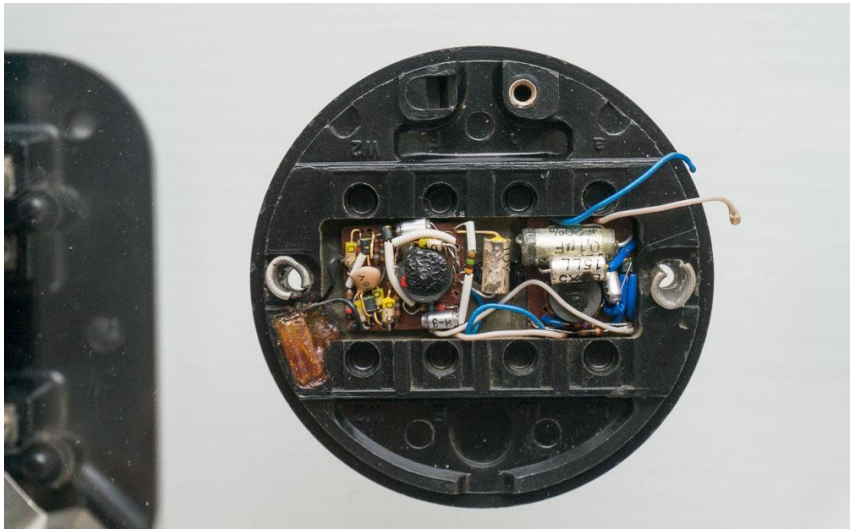
……б) телевизионные и видеокамеры, закамуфлированные под бытовые предметы……

Лаборатория Информационной Безопасности

3. По наличию автономных источников питания:

- с АИП

- без АИП



Классификация технических средств негласного получения информации

4. По наличию камуфляжа:

- с ним

- без камуфляжа

Статья 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации

Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для негласного получения информации, наказываются:

штрафом в размере до **200 000** рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев,

либо ограничением свободы на срок **до четырех лет**, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового,

либо лишением свободы на срок **до четырех лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Не покупайте камеры-ручки, камеры-автомобильне брелоки, камеры-зажигалки, камеры-часы и прочие СТС. На рынке предлагается много изделий, на которые распространяется действие статьи 138 УК РФ.

Лаборатория Информационной Безопасности

Дополнительная информация

Так, приговором Советского районного суда г. Челябинска осужден к штрафу в размере **30 000** рублей житель города за совершение двух преступлений, предусмотренных ст. 138-1 УК РФ.

Органами предварительного расследования и судом установлено, что он, не имея лицензии на осуществление деятельности по приобретению в целях продажи и реализации специальных технических средств, предназначенных для негласного получения информации, умышленно, действуя в нарушение пункта 2 части первой статьи 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», по месту своего жительства по объявлению, размещенному на интернет-сайте, незаконно **приобрел с целью последующего сбыта предмет в виде брелка от автомобильной сигнализации со встроенной видеокамерой, микрофоном и накопителем информации,** позволяющий производить негласную аудио и видео запись.

После этого **разместил объявление о продаже указанного аппарата в сети «Интернет», и продал его**, т.е. осуществил незаконный сбыт. Таким же способом приобрел у неустановленного лица с целью последующего сбыта **предмет в виде электромеханических наручных часов со встроенной миниатюрной видеокамерой, микрофоном и накопителем информации,** позволяющий производить негласную аудио и видеозапись, и продал его. При назначении наказания судом учтено, что подсудимый полностью признал вину, положительно характеризуется, активно способствовал раскрытию преступления, раскаялся в содеянном.

Лаборатория Информационной Безопасности

5. По видам модуляции:

- **Аналоговые** (узкополосная частотная модуляция, широкополосная частотная модуляция)

Положительные стороны:

а) дешевизна;

б) трудноразличимы на фоне легальных сигналов.

Отрицательные стороны:

а) канал передачи не закодирован, поэтому услышать записываемую речь может любой желающий;

б) низкая помехозащищенность.

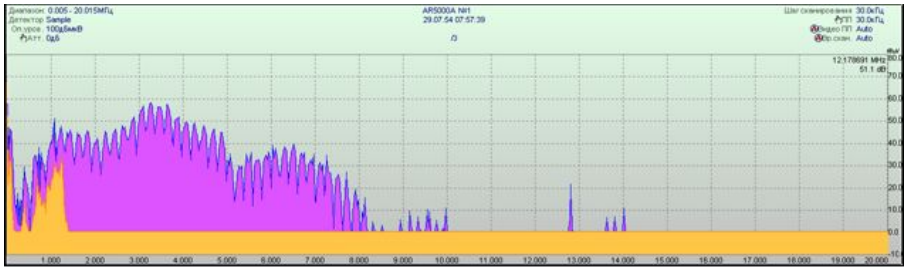
- Цифровые

а) цифровая модуляция (дельта-модуляция, амплитудная манипуляция, частотная манипуляция и т.д.).

Положительные стороны:

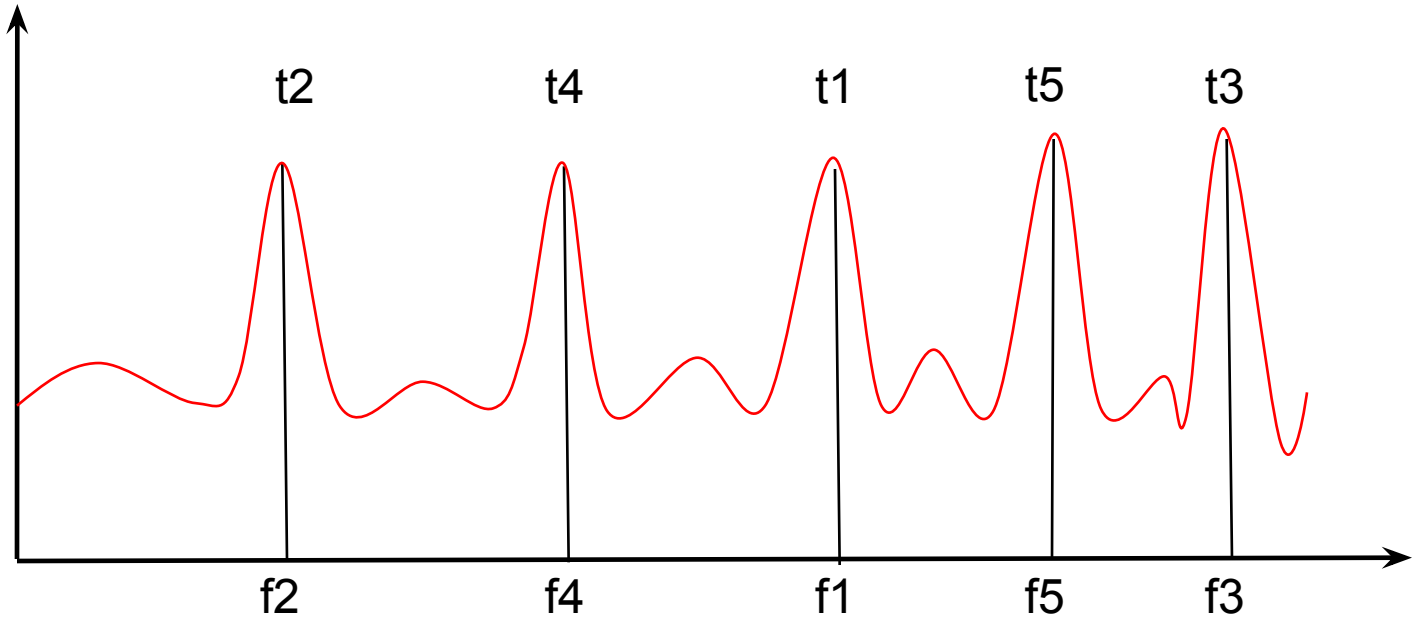
- для приема сигнала нужны демодуляторы, т.е. не все могут услышать в приемнике запись. Достигается скрытность;
- высокая помехозащищенность.

б) шумоподобный сигнал



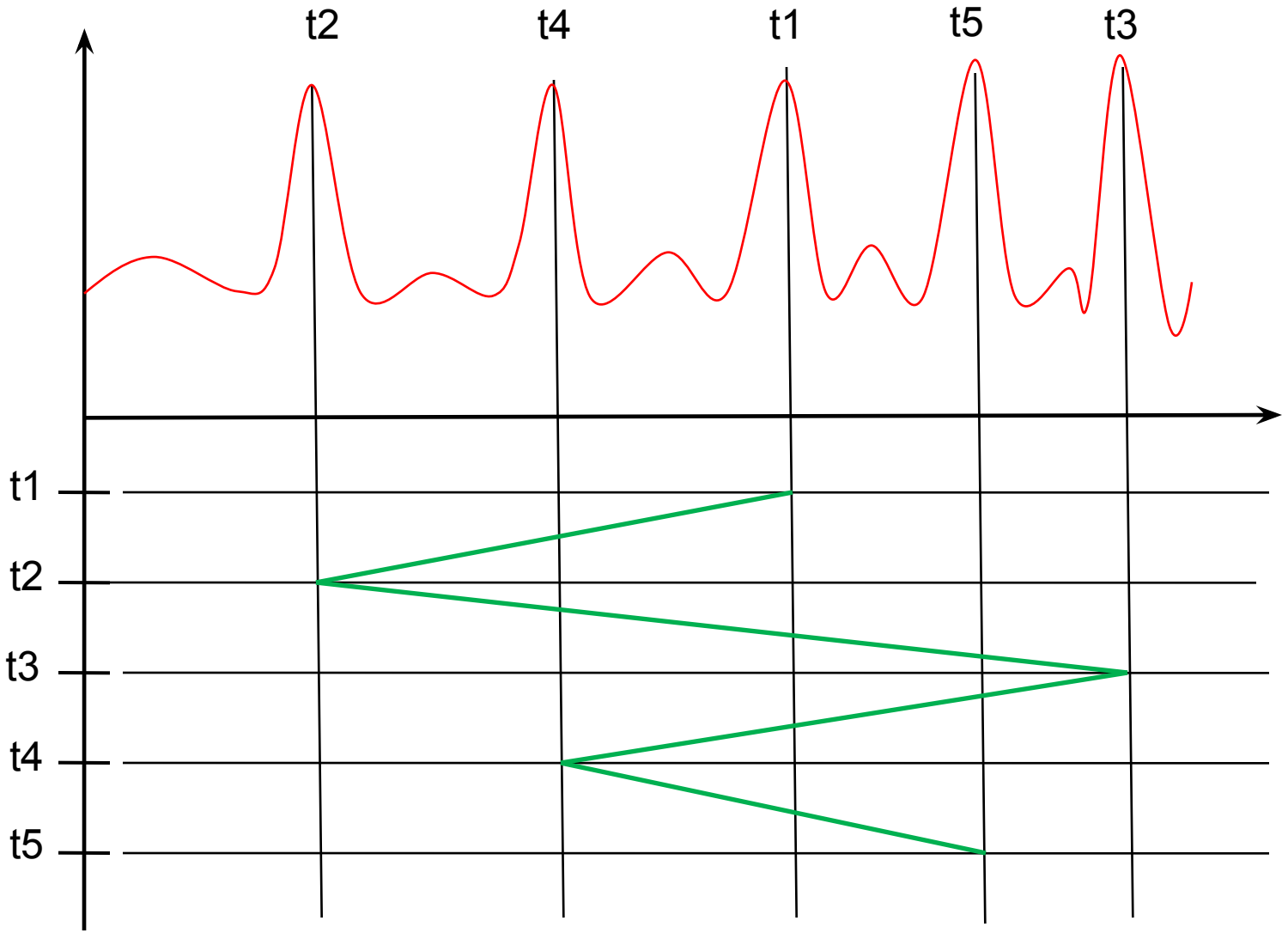
Лаборатория Информационной Безопасности

в) псевдослучайная перестройка рабочей частоты (ППРЧ)



Лаборатория Информационной Безопасности

Классификация технических средств негласного получения информации



Лаборатория
Информационной
Безопасности

Классификация технических средств негласного получения информации

г) устройства с накоплением и кратковременной передачей информации

Методы обнаружения специальных технических средств

1. Метод акустической обратной связи

Состав программно-аппаратного комплекса

Персональный компьютер со специализированным Программным обеспечением

Приемное устройство с антенной системой

Источник сигнала

Лаборатория Информационной Безопасности

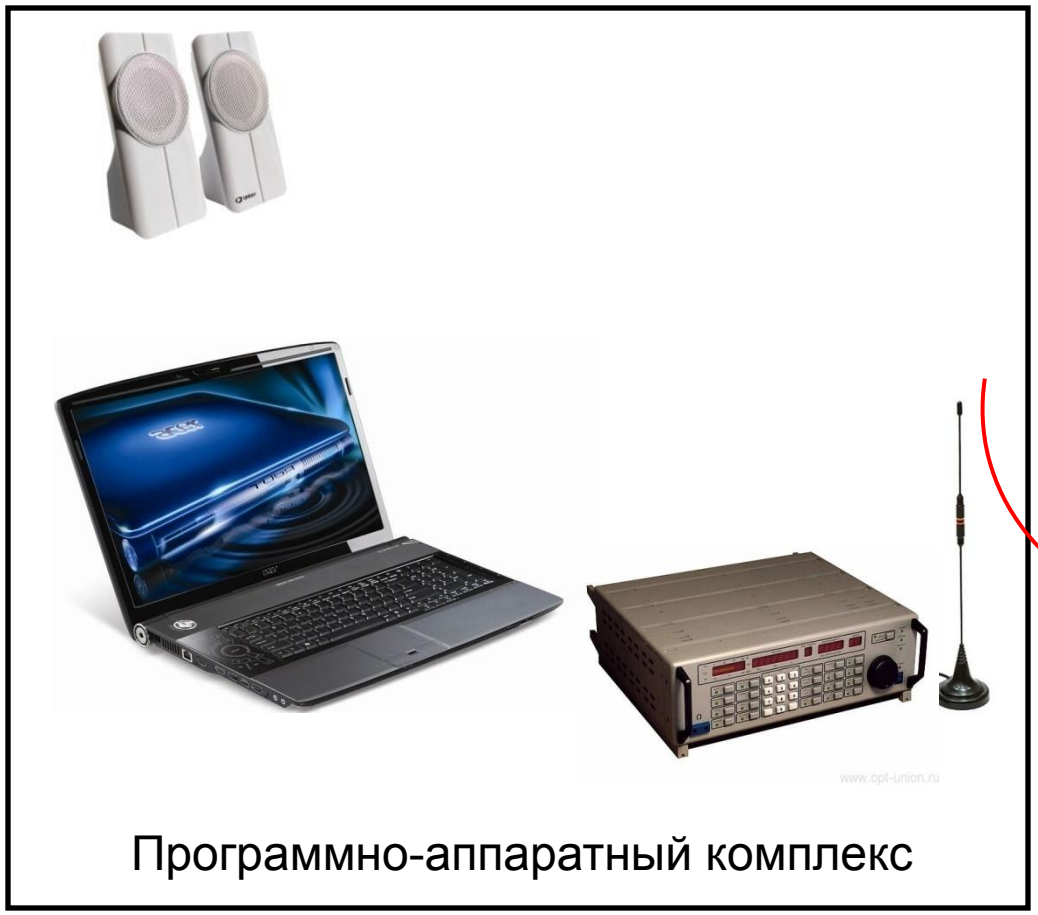
1. Метод акустической обратной связи

Программно-аппаратный комплекс

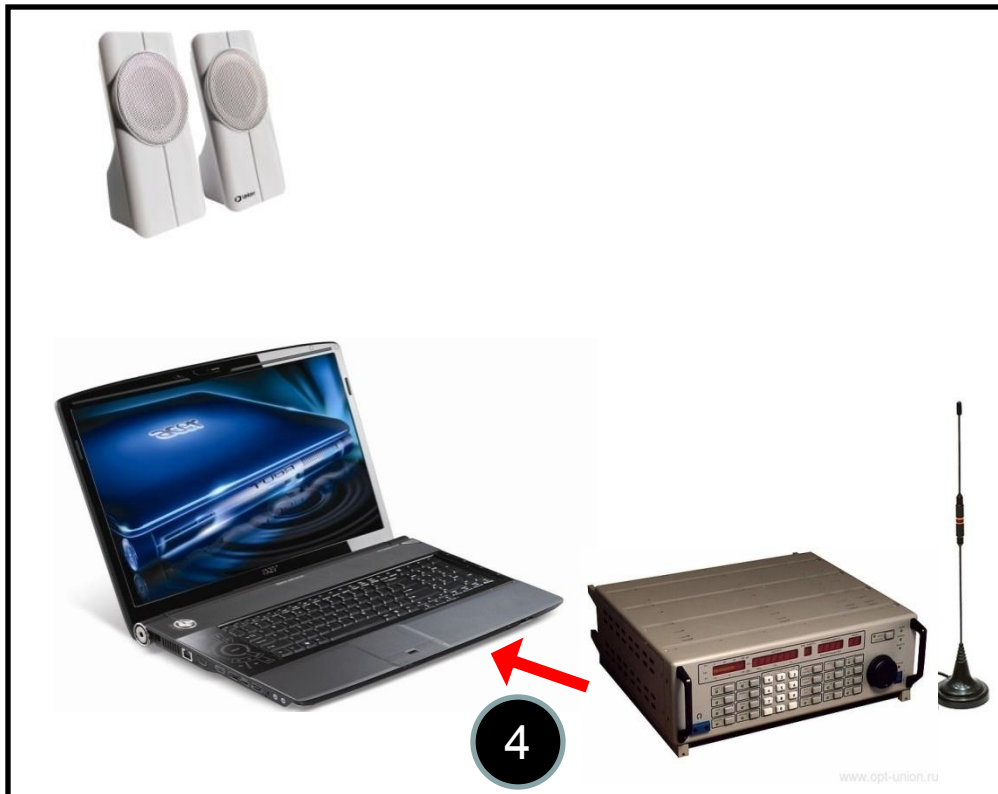
Лаборатория
Информационной
Безопасности

1. Метод акустической обратной связи

1. Метод акустической обратной связи



1. Метод акустической обратной связи



Программно-аппаратный комплекс

1. Метод акустической обратной связи

$$Correlation = \cos\propto = \frac{\sum_0^{n-1} x_i * y_i}{\sqrt[2]{\sum_0^{n-1} {x_i}^2}\sqrt[2]{\sum_0^{n-1} {y_i}^2}}$$

Программно-аппаратный комплекс

Лаборатория Информационной Безопасности

Дополнительная информация

Для определения степени похожести двух сигналов используется понятие **корреляции**.

Совокупность отсчетов сигнала можно считать вектором в N-мерном пространстве. Тогда можно определить корреляцию как угол между двумя векторами в N-мерном пространстве. Чем меньше угол, тем больше вектора похожи. На практике проще всего вычислять косинус угла. Вспоминая геометрию, получаем формулу:

$$Correlation = \cos\propto = \frac{\sum_0^{n-1} x_i * y_i}{\sqrt[2]{\sum_0^{n-1} x_i^2}\sqrt[2]{\sum_0^{n-1} y_i^2}}$$

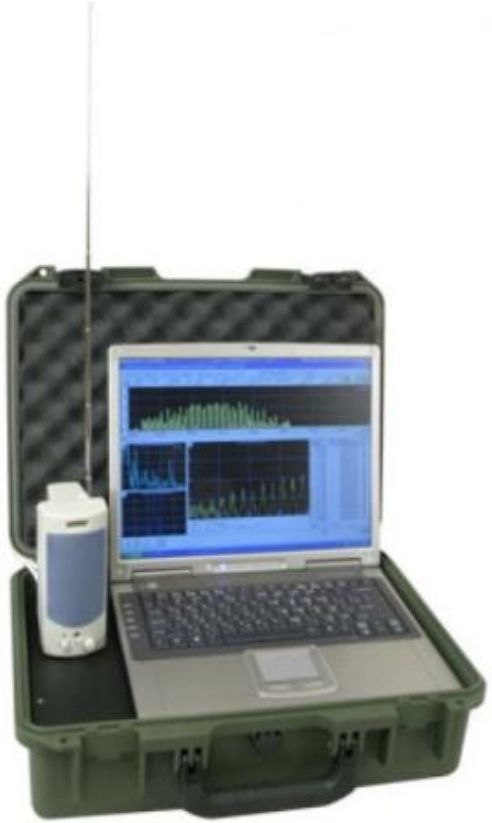
Удобство этой формулы в том, что она даёт нормированный результат в диапазоне -1 ... +1 независимо от диапазона входных значений сигналов.

1. Метод акустической обратной связи

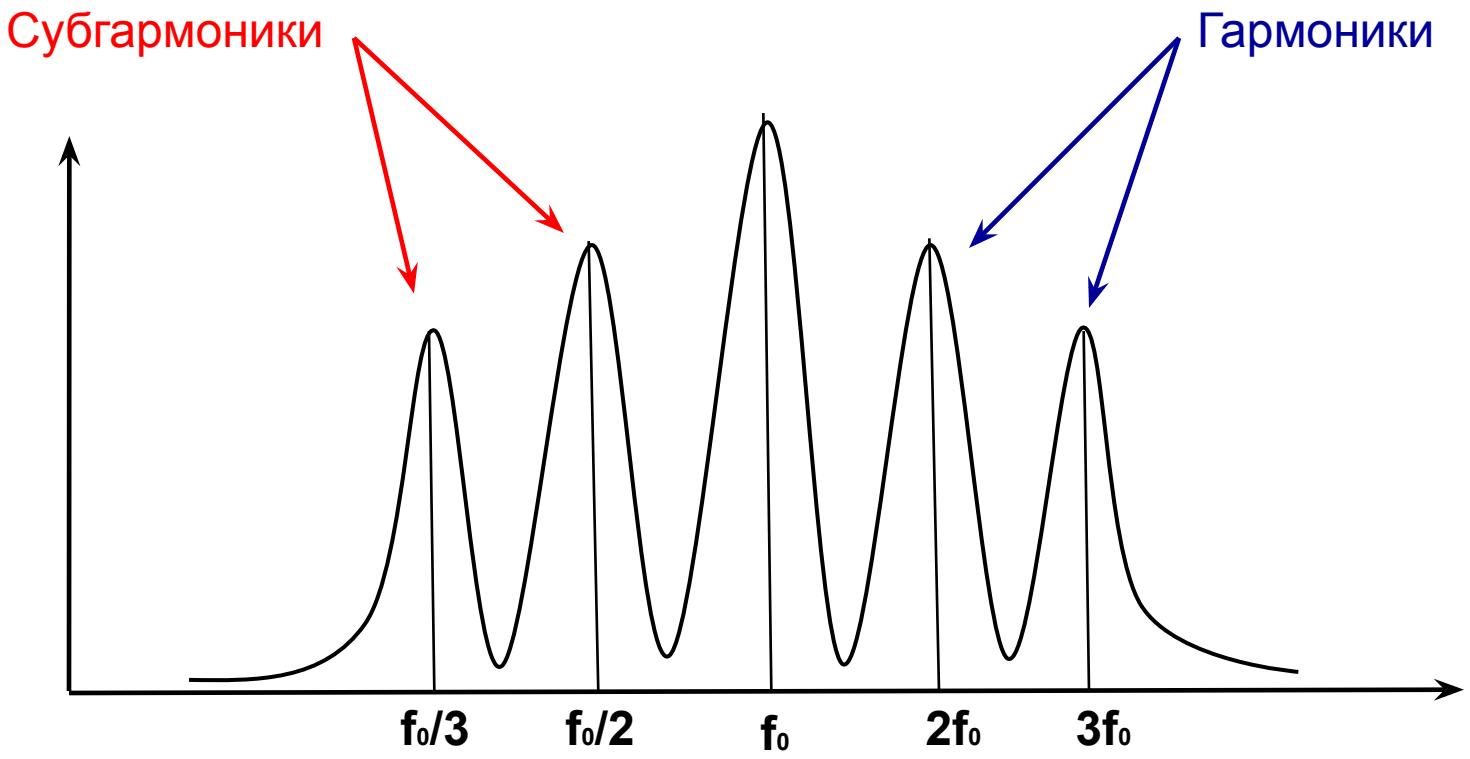
Программно-аппаратный комплекс

Методы обнаружения

Программно-аппаратный комплекс



2. Метод гармонических составляющих (гармоник)



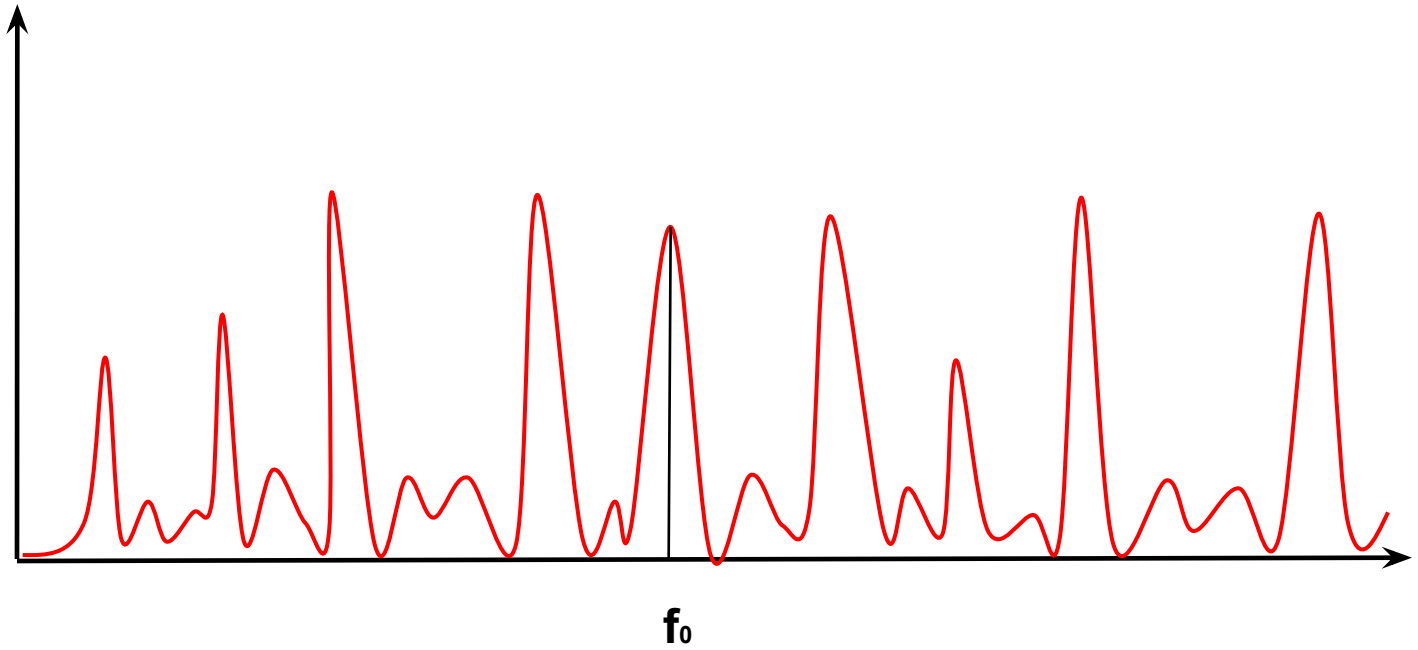
Гармоники – частоты, кратные основной частоте излучения

Лаборатория
Информационной
Безопасности

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОСТАНОВЛЕНИЕ
от 21 декабря 2011 г. № 1049-34

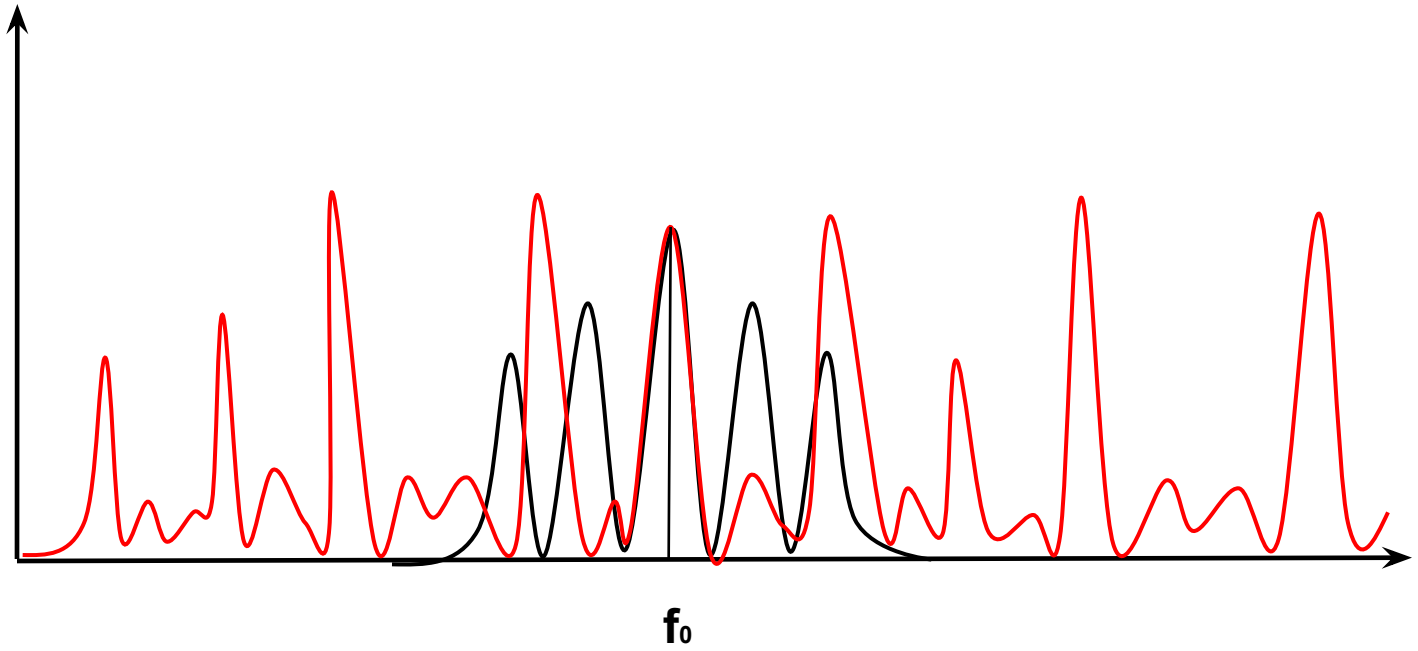
ОБ УТВЕРЖДЕНИИ ТАБЛИЦЫ РАСПРЕДЕЛЕНИЯ ПОЛОС РАДИОЧАСТОТ МЕЖДУ РАДИОСЛУЖБАМИ РОССИЙСКОЙ ФЕДЕРАЦИИ И ПРИЗНАНИИ УТРАТИВШИМИ СИЛУ НЕКОТОРЫХ ПОСТАНОВЛЕНИЙ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Дополнительная информация



Лаборатория
Информационной
Безопасности

Дополнительная информация



Лаборатория
Информационной
Безопасности

КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ от 30 декабря 2001 N 195-ФЗ

Статья 13.3. Самовольные проектирование, строительство, изготовление, приобретение, установка или эксплуатация радиоэлектронных средств и (или) высокочастотных устройств

Проектирование, строительство, изготовление, приобретение, установка или эксплуатация радиоэлектронных средств и (или) высокочастотных устройств без специального разрешения (лицензии), если такое разрешение (такая лицензия) обязательно (обязательна),

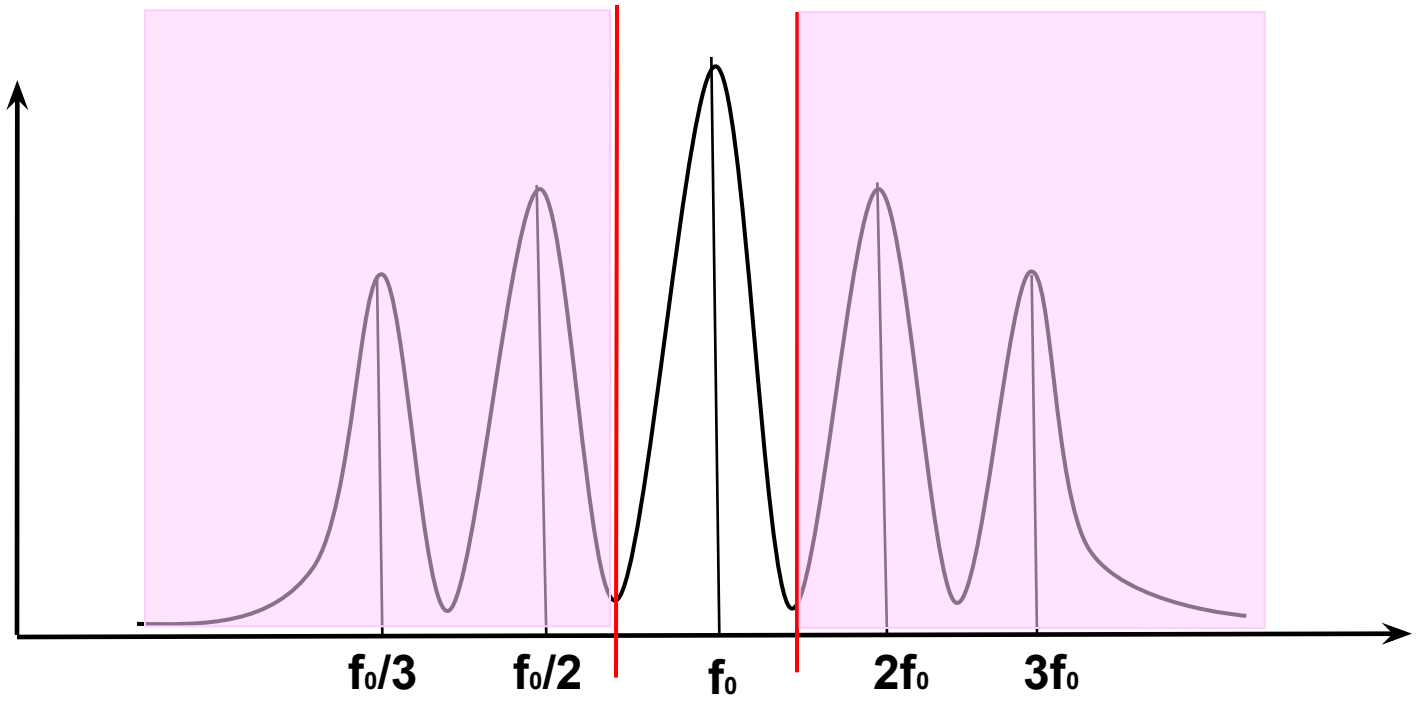
влечет наложение административного штрафа на граждан в размере от **пяти до десяти минимальных размеров оплаты труда** с конфискацией радиоэлектронных средств и (или) высокочастотных устройств или без таковой;

на должностных лиц - **от десяти до двадцати минимальных размеров оплаты труда** с конфискацией радиоэлектронных средств и (или) высокочастотных устройств или без таковой;

на юридических лиц - **от ста до двухсот минимальных размеров оплаты труда** с конфискацией радиоэлектронных средств и (или) высокочастотных устройств или без таковой.

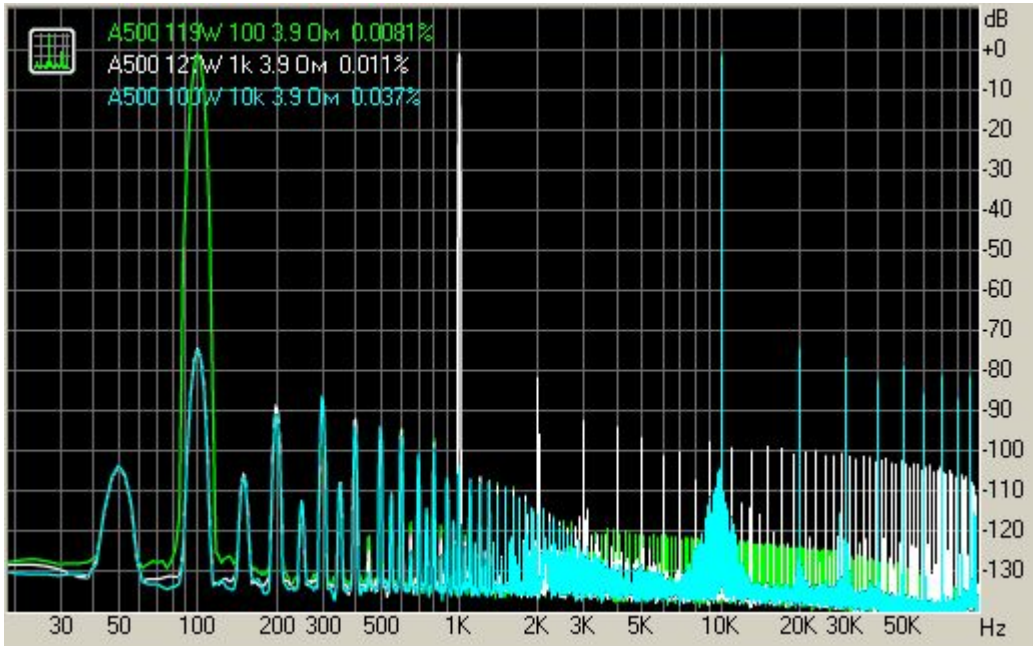
Лаборатория Информационной Безопасности

Дополнительная информация



Лаборатория
Информационной
Безопасности

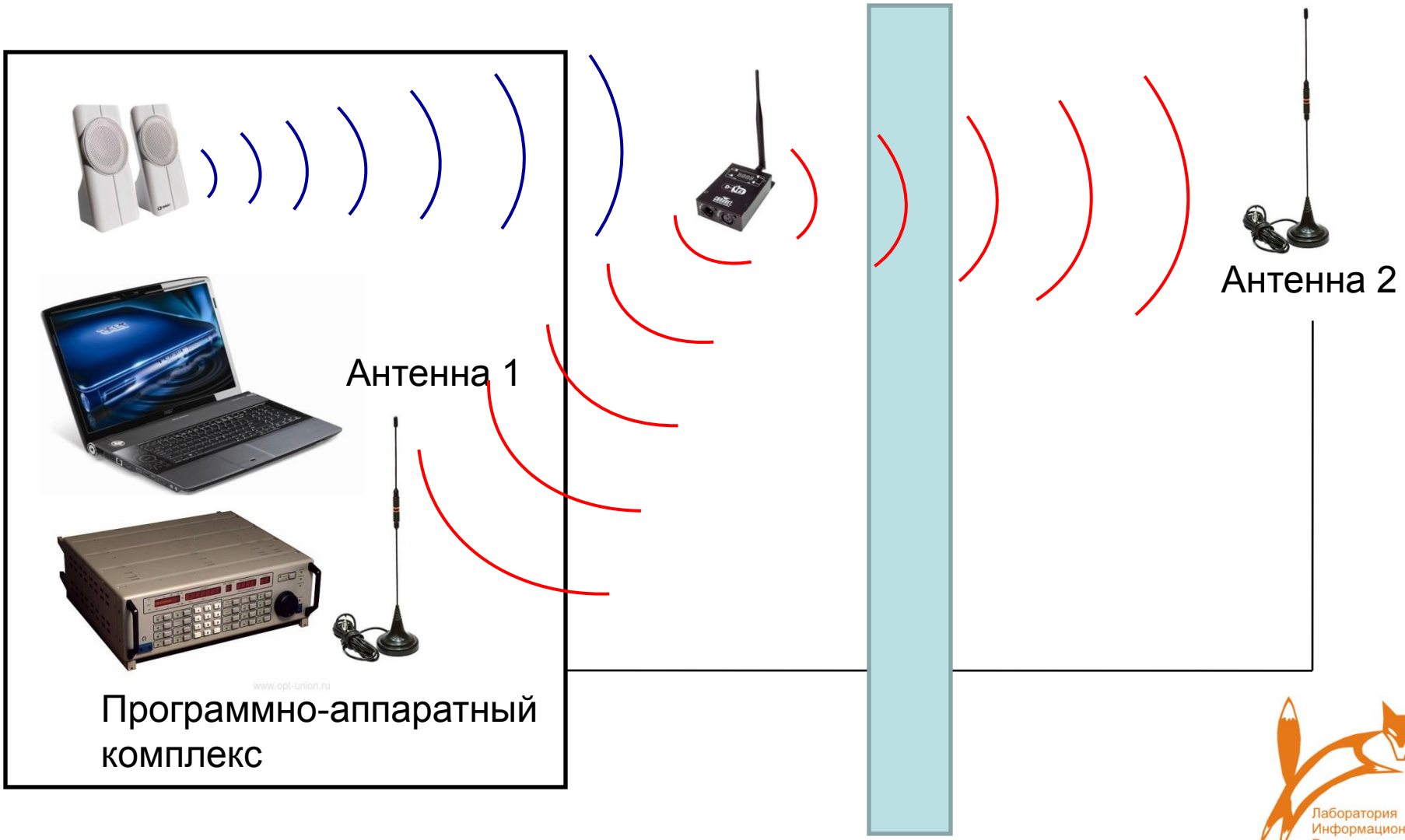
2. Метод гармонических составляющих (гармоник)



Программа настраивается на удвоенную или утроенную частоту исследуемого сигнала, и если обнаруживает на них информационный сигнал то выдает предупреждение о возможном наличии специальных технических средств негласного получения информации

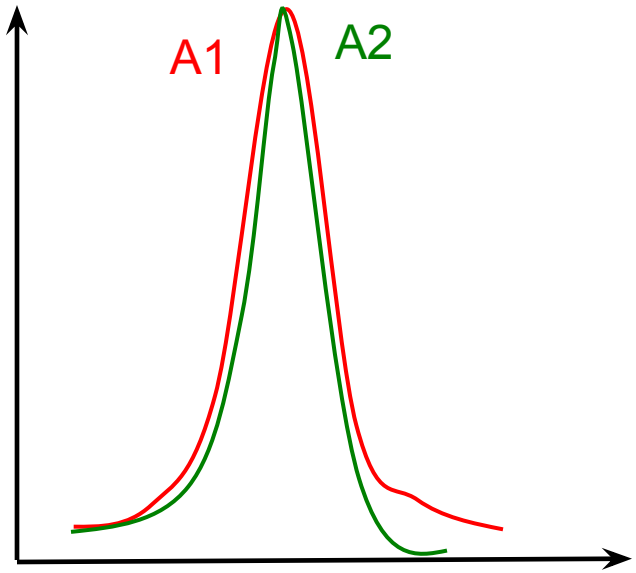
Лаборатория Информационной Безопасности

3. Метод разнесенного приема

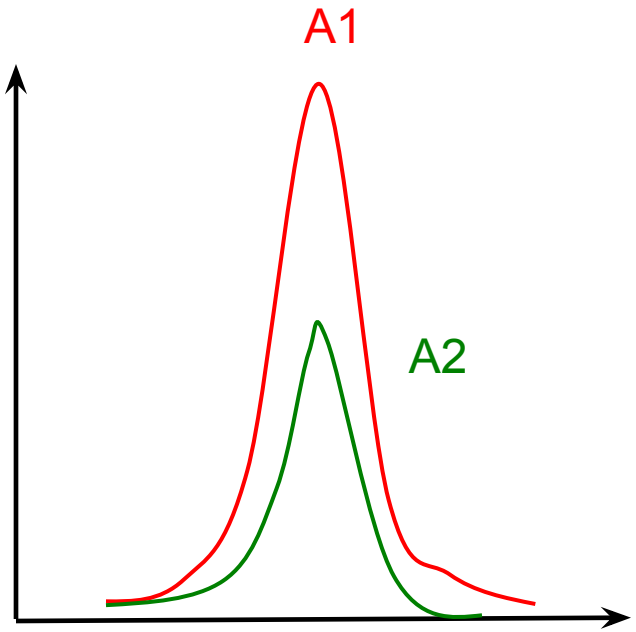


3. Метод разнесенного приема

а)



б)

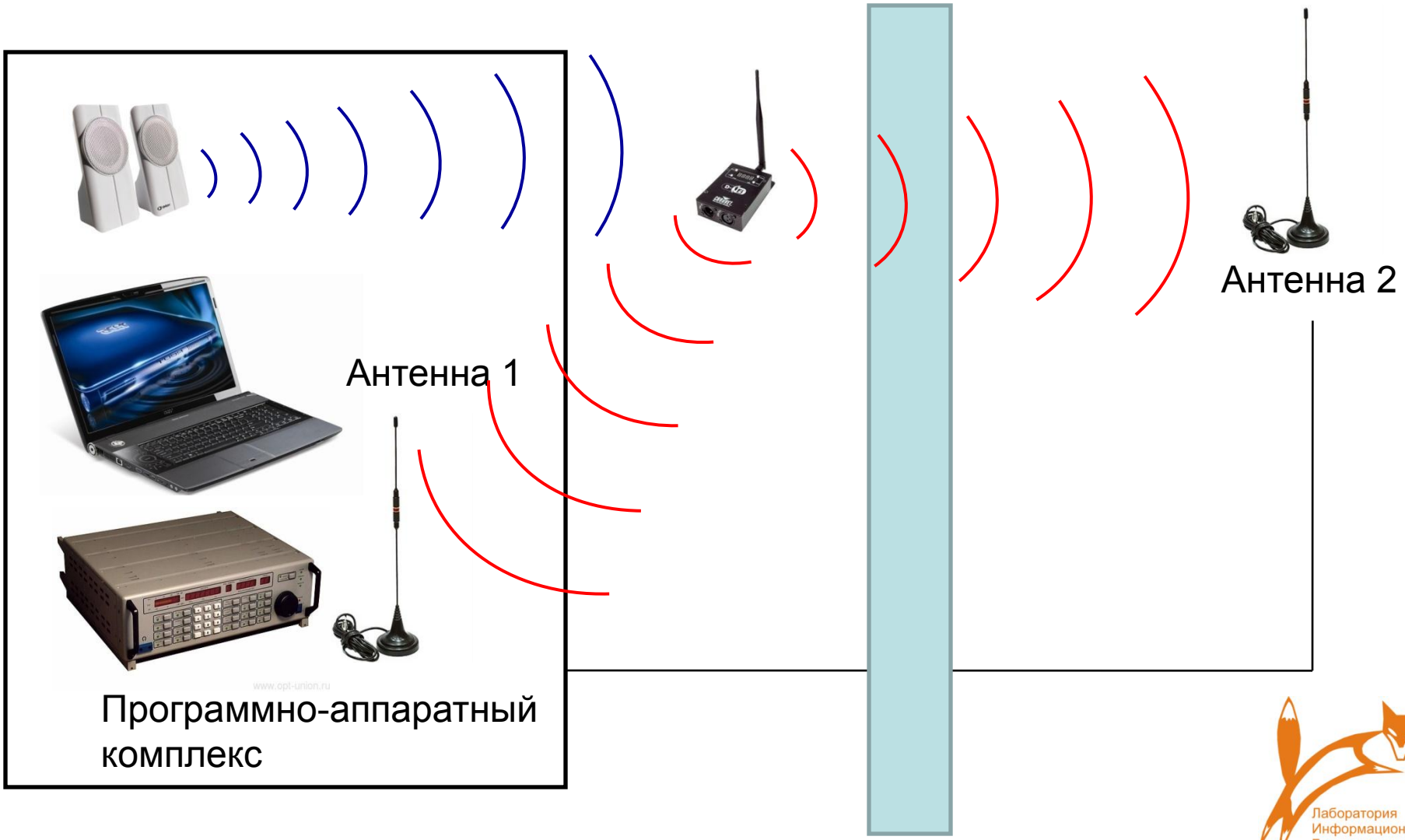


а – сигнал примерно одинаков на обоих антеннах, т.е. это мощный сигнал обычного ретранслятора;

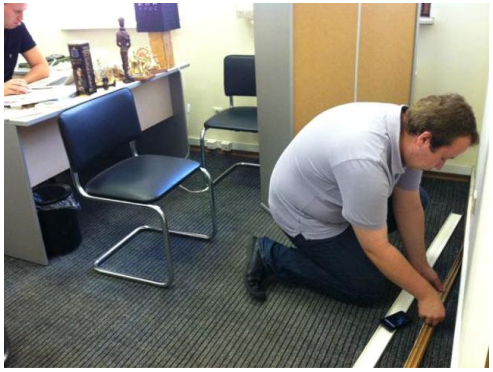
б – сигнал на вторую антенну поступает заметно более слабый, т.е. это маломощный сигнал внутри проверяемого помещения.

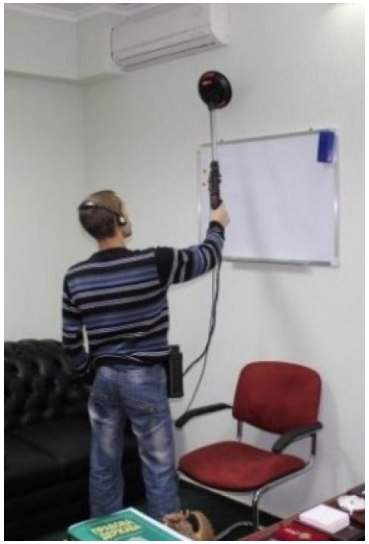
Лаборатория Информационной Безопасности

3. Метод разнесенного приема

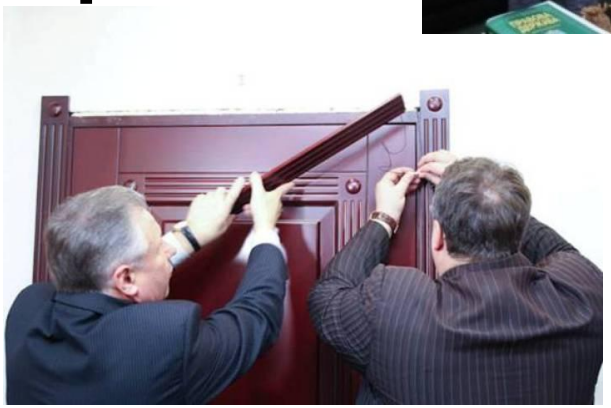


Лаборатория Информационной Безопасности





Организация проведения поисковых мероприятий

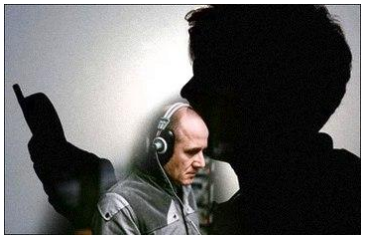


Проведение поисковых мероприятий

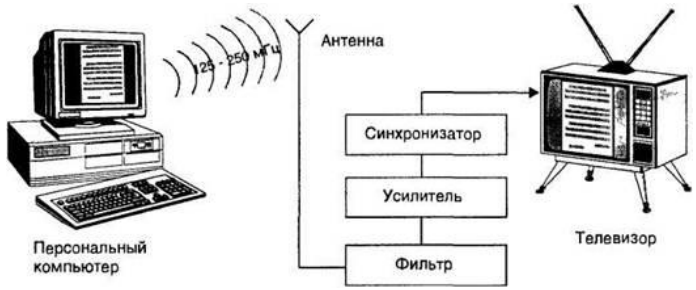
В настоящее время для проникновения в чужие секреты используются такие возможности, как:

подслушивание разговоров в помещении или в автомашине с помощью предварительно установленных радиомикрофонов, радиостетоскопов, миниатюрных магнитофонов и пр;

контроль телефонных переговоров, телексных и телефаксных линий связи, радиотелефонов и радиостанций;



дистанционный съем информации с различных технических средств, с мониторов и печатающих устройств компьютеров и др.



Лаборатория Информационной Безопасности

1. Подготовка поискового мероприятия

1.1 Изучение объекта

Цель изучения объекта перед проведением поискового мероприятия - определение вероятного противника, оценка его оперативных и технических возможностей по проникновению в объект с целью съема информации.

Этапы изучения объекта:

определение вероятного противника и оценка его оперативно-технических возможностей по проникновению в помещение;

изучение расположения помещения и его окружения;

изучение режима посещения помещения, порядка установки в нем предметов интерьера, мебели, проведения ремонтных работ;

установка всех фактов ремонта, монтажа или демонтажа коммуникаций, замены мебели или предметов интерьера;

изучение конструктивных особенностей здания и ограждающих конструкций помещения;

изучение всех коммуникаций, входящих в помещение или проходящих через него.

Лаборатория Информационной Безопасности

1.2 Подготовка к началу поисковых работ

Цель - выработать методику поиска на конкретном объекте и составить перечень поисковой аппаратуры.

Лаборатория Информационной Безопасности

Проведение поисковых мероприятий

Итоговыми документами при подготовке мероприятия являются:

1) план действий по прикрытию работы поисковиков;

2) план действий по локализации канала утечки информации при его обнаружении;

3) перечень лиц, посвященных в характер работ;

4) план проведения радиоконтроля с подобранными и проверенными местами установки радиоаппаратуры;

5) план прилегающей местности в радиусе до 1000 м с указанием по возможности принадлежности зданий, особенно находящихся в прямой видимости окон помещения;

Проведение поисковых мероприятий

6) поэтажные планы здания с указанием всех помещений, смежных с обследуемым, характеристики стен, перекрытий , материалов отделки и коммуникаций, а также сведения о лицах, занимающих смежные помещения и о режиме их посещения;

7) план-схема коммуникаций всего объекта с указанием всех щитов и разводных коробок;

8) план обследуемого помещения с указанием всех предметов интерьера, мебели и оборудования, электроустановочных изделий и средств связи;

9) план проведения работ с указанием сроков, последовательности и исполнителей;

10) перечень особо подозрительных мест и отдельный план их обследования;

Лаборатория Информационной Безопасности

Проведение поисковых мероприятий

11) модель ожидаемой на объекте спецтехники для проверки эффективности поиска;

12) легенда проведения поисковых работ;

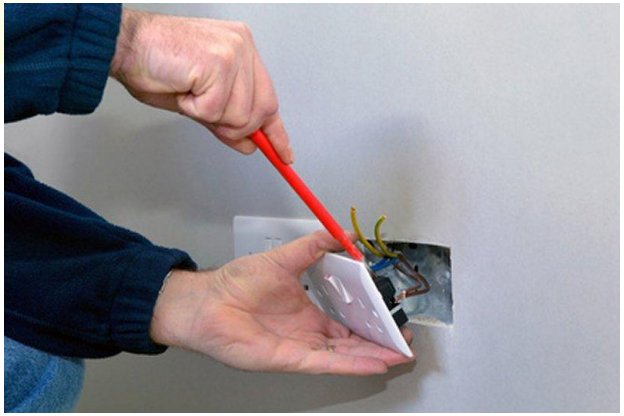
13) план действий на случай обнаружения спецтехники или канала утечки информации;

14) перечень поисковой аппаратуры.

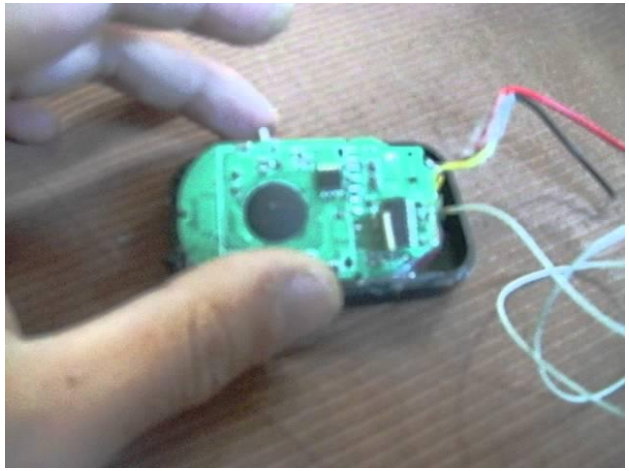
2. Проведение поискового мероприятия

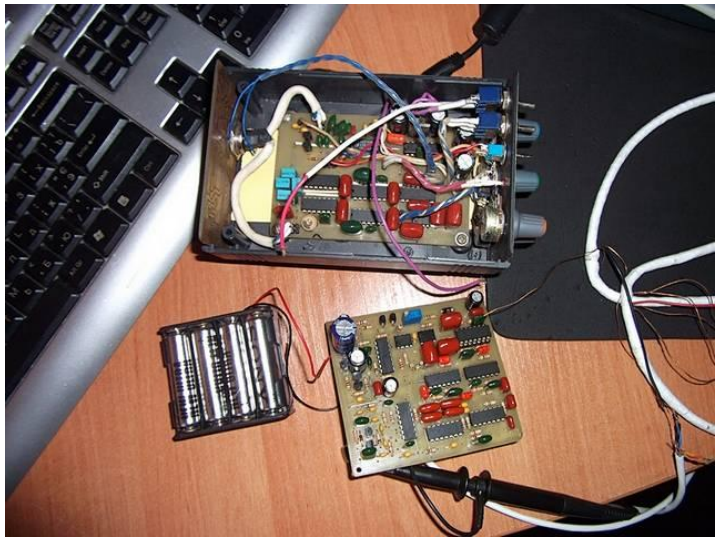
2.1 Контроль радиоэфира

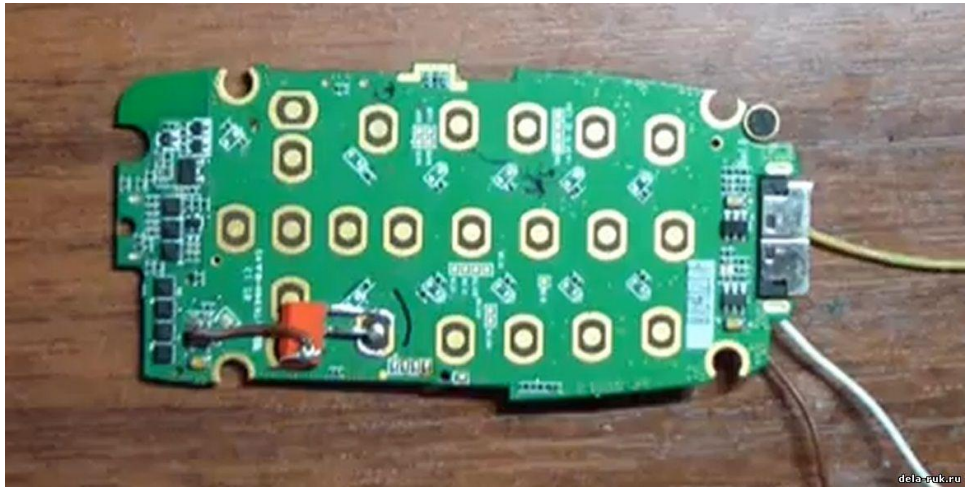
2.2 Визуальный осмотр



2.3 Проверка электронных приборов



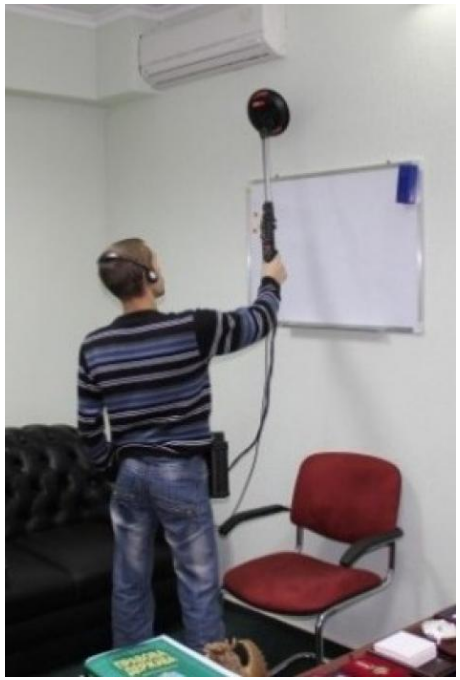




2.4 Проверка предметов интерьера и мебели

2.5 Проверка электроустановочных и коммуникационных изделий

2.6 Проверка ограждающих конструкций



2.7 Подготовка отчетных документов

Заключение

Специальные технические средства, предназначенные для негласного получения информации классифицируются **по пяти основным признакам**:

- по способу передачи информационного сигнала;
- по наличию системы голосовой активации;
- по наличию автономных источников питания;
- по наличию камуфляжа;
- по видам модуляции.

Существуют **четыре основных метода** обнаружения СТС:

- метод акустической обратной связи;
- метод гармонических составляющих;
- метод разнесенного приема.

Проведение поисковых мероприятий представляет собой сложный, многоуровневый процесс, подразумевающий комплексное применение всех имеющихся средств, мер, методов и способов.

Лаборатория Информационной Безопасности

Контрольные вопросы:

1. По каким признакам классифицируются специальные технические средства негласного получения информации?
2. Как классифицируются СТС по способу передачи информационного сигнала?
3. Какие методы обнаружения СТС Вы знаете?
4. Раскройте сущность метода акустической обратной связи.
5. Раскройте сущность метода разнесенного приема.
6. Раскройте сущность метода гармонических составляющих.
7. Назовите этапы проведения поисковых мероприятий.
8. Назовите этапы изучения объекта проверки.
9. Назовите итоговые документы при подготовке поисковых мероприятий.

Спасибо за внимание!

Лаборатория Информационной Безопасности

Методы обнаружения

Китайский полководец Сунь-Цзы советовал:
«разлагайте все хорошее, что имеется в стране вашего противника»;
«вовлекайте видных представителей вашего противника в преступные пред приятия»;
«подрывайте их престиж и выставляйте в нужный момент на позор обществ енности»;
«используйте сотрудничество самых подлых и гнусных людей»;
«разжигайте ссоры и столкновения среди граждан вражеской страны»;
«подстрекайте молодежь против стариков»;
«мешайте всеми средствами деятельности правительства»;
«препятствуйте всеми способами оснащению, обеспечению и наведению по рядка в вооруженных силах»;
«сковывайте волю противника бессмысленными песнями и музыкой; обесце нивайте все традиции и богов ваших врагов»;
«посылайте женщин легкого поведения с тем, чтобы дополнить дело разлож ения»;
«будьте щедры на предложения и подарки для покупки информации и сооб щников, не экономьте ни наденьгах, ни на обещаниях, так как они приносят богатые дивиденды».