

ВОЕННО-СПЕЦИАЛЬНАЯ ПОДГОТОВКА

ТЕМА №1:

**ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО
ТЕХНИЧЕСКИМ КАНАЛАМ**

Занятие № 20:

**Измерительные комплексы для
выявления каналов утечки
информации**

ЛИТЕРАТУРА:

А) ОСНОВНАЯ:

1. МЕНЬШАКОВ Ю. К. ОСНОВЫ ЗАЩИТЫ ОТ ТЕХНИЧЕСКИХ РАЗВЕДОК. УЧЕБНОЕ ПОСОБИЕ. - М.: ИПЦ "МАСКА", 2017.
2. В. А. ШАЛАГИНОВ И ДР.; ПОД ОБЩ. РЕД. В. А. ШАЛАГИНОВА. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ. УЧЕБНОЕ ПОСОБИЕ - ОРЕЛ: АКАДЕМИЯ ФСО РОССИИ, 2018.

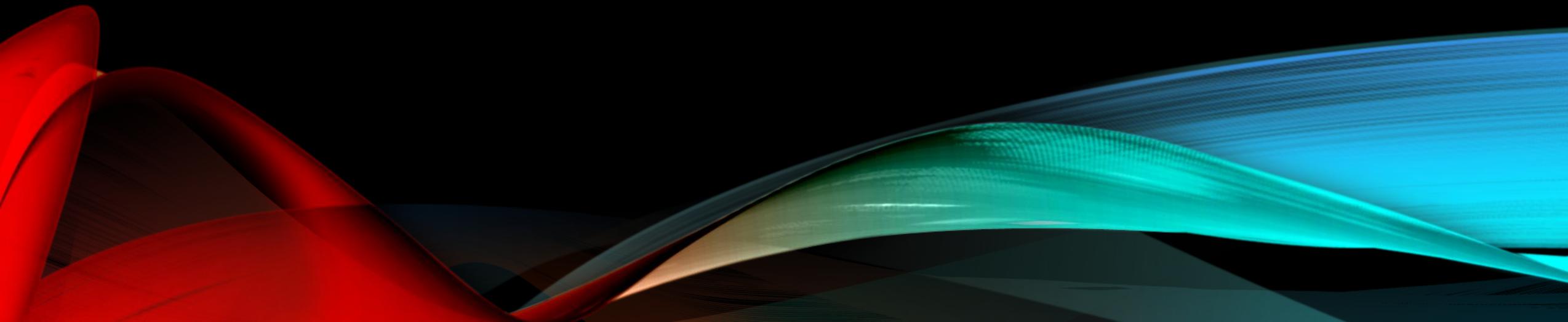
Б) ДОПОЛНИТЕЛЬНАЯ:

3. ЗАВОДЦЕВ И.В., ЗАХАРЧЕНКО Р.И., НАЗАРОВ И.В. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. УЧЕБНОЕ ПОСОБИЕ. – КРАСНОДАР: КВВУ, 2015.
4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. БАЗОВЫЙ ЭЛЕКТРОННЫЙ УЧЕБНИК. – М. ВА ГШ ВС РФ, 2017.

УЧЕБНЫЕ ВОПРОСЫ

1. КОМПЛЕКС RS TURBO
2. КОМПЛЕКСЫ ИЗМЕРЕНИЯ ПЭМИН
3. НЕЛИНЕЙНЫЕ ЛОКАТОРЫ
4. КОМПЛЕКС ДЛЯ ИЗМЕРЕНИЯ ХАРАКТЕРИСТИК АКУСТИЧЕСКИХ СИГНАЛОВ СПРУТ-7

1. КОМПЛЕКС RS TURBO



- **Предназначен** для автоматизации весьма трудоемких и требующих достаточно высокой квалификации персонала операций обнаружения, классификации, идентификации, локализации и нейтрализации источников несанкционированных радиоизлучений, например подслушивающих устройств.
- Время сканирования всего диапазона частот составляет 1,5 - 3 минуты.
- С помощью конвертера RS1000/L комплекс обнаруживает сигналы, которые передаются подслушивающими устройствами по сети электропитания или любым проводным линиям в диапазоне частот от 600 Гц до 10 МГц, а также в инфракрасной части оптического диапазона.
- Одновременно комплекс с достаточной точностью указывает местоположение обнаруженных радиомикрофонов с обычной частотной модуляцией, а при необходимости - нейтрализует их излучения с помощью программируемых генераторов сигналов RS1100/N и RS1110/N.



• Возможности комплекса RS Turbo

- Обнаружение излучений скрытно установленных в контролируемом помещении радиомикрофонов с любым типом модуляции и кодирования речевого сигнала.

- Обнаружение активных телефонных радиопередатчиков, подключенных к линиям телефонных аппаратов, находящихся в контролируемом помещении.

- Обнаружение сигналов подслушивающих устройств, передающих информацию на несущих частотах по сети электропитания, телефонным или любым другим проводным линиям.

- Обнаружение сигналов оптических передатчиков ИК-диапазона.

- Измерение расстояний до обнаруженных передатчиков со стандартной частотной модуляцией.

- Вычисление координат обнаруженных передатчиков, находящихся в контролируемом помещении.

- Статистический анализ загрузки заданного радиодиапазона.

- Блокировка одного или нескольких радиоканалов несанкционированной передачи или утечки информации из помещения.

• Возможности комплекса RS Turbo

- С появлением передающих устройств, работающих в режиме скачков по частоте, и систем, использующих накопление информации с последующей короткой передачей данных в широкой полосе, резко ужесточились требования к скорости работы поисковых комплексов и аппаратуры радиоконтроля. Программное сканирование эфира (30 - 40 минут) не может обеспечить сколь-либо приемлимую вероятность обнаружения таких устройств. Это связано с тем, что синтезатор приемника перестраивается достаточно быстро, но система команд управляющего контроллера приемника построена так, что все установки приемника производятся заново при каждом шаге, что и не позволяет быстро сканировать диапазон. Практически скорость работы комплекса ограничена величиной $N \times F$, где N - число шагов сканирующего приемника в секунду, а F - полоса анализа. Отсюда следует, что наибольшей скоростью работы обладают системы, имеющие широкую полосу анализа, которую можно получить лишь на выходе **промежуточной частоты** сканирующего приемника. Наиболее равномерной полосой ПЧ и отсутствием ложных частот из сканирующих приемников обладает AR-5000. Максимальная скорость поиска для систем построенных на его базе составляет $15 \times 8 = 120$ МГц в секунду. Однако и её достичь практически сложно, так как требуется время на программную обработку, отображение информации и т.д. Поэтому следует ориентироваться на общее время прохода всего диапазона сканера.

• Возможности комплекса RS Turbo

- Анализ по ПЧ может производиться либо последовательным сканированием, либо с использованием цифровой обработки сигналов по алгоритму быстрого преобразования Фурье (FFT). Аппаратный анализатор сигналов RS turbo является анализатором последовательного типа и предназначен для быстрого анализа диапазона с передачей данных по шине RS-232, либо через USB порт. Основная версия разработана для ПЧ 10,7 МГц под приемник AR-5000. Для работы с приемниками AR-8600 и AR-8200 разработаны версии RS Turbo под ПЧ 45,05 МГц. Время прохода диапазона от 10 МГц до 2,6 ГГц составляет 0,5 - 2,5 минуты. Кроме того, разрабатывается версия RS Turbo с прямым анализом низкочастотных сигналов в сети элетропитания, проводных коммуникациях и на выходе приемника ИК диапазона. Возможно управление по компьютерной сети или через модем. Поисковые комплексы серии RS Turbo полностью отвечают требованиям, предъявляемым к системам ближнего радиоконтроля, а по цене и возможностям не имеют аналогов на рынке подобных систем.



RS Turbo82



RS Turbo5

Модификации комплекса

RS Turbo5

RS Turbo82

RS Turbo86

Диапазон рабочих частот

10 кГц - 2600 МГц

500 кГц - 2040 МГц

100 кГц - 2040 МГц

Используемый приемник

AR-5000 (AOR, Япония)

AR-8200 (AOR, Япония)

AR-8600 (AOR, Япония)

• Сканирование

- Сканирование – это базовая операция, которая предшествует обнаружению, классификации и идентификации источников излучений (сигналов). В процессе сканирования выявляются занятые участки исследуемого частотного диапазона и оцениваются спектры присутствующих в нем сигналов. Частота настройки сканирующего приемника изменяется дискретно с фиксированным шагом 8 МГц и на каждом шаге вычисляемый контроллером RS turbo результат измерений уровней принимаемых во всем спектре сигналов заносится в компьютер. В анализаторе RS turbo быстрое сканирование выполняется с широким (200 кГц) или узким (12,5 кГц) шагом. По результатам сканирования компьютер формирует спектральную панораму исследуемого диапазона, в которой каждому значению частоты настройки соответствует измеренный спектр сигнала. Операции сканирования выполняются в порядке их размещения в списке операций задания. Это дает возможность в первую очередь просматривать те участки спектра, где вероятность найти излучения несанкционированных источников выше. Один частотный диапазон можно включать в задание несколько раз, чтобы реализовать различные алгоритмы идентификации и классификации излучений.

• Сканирование

- Выполнив один цикл сканирования, программа составляет таблицу, в которой каждому значению частоты настройки ставится в соответствие измеренный последовательным анализатором контроллера RS turbo спектр сигналов в полосе анализа 8 МГц, снятый для сигналов, превышающих заданный порог, с разрешением 12,5 кГц. Эта таблица называется спектральной панорамой. Программа комплекса RS turbo позволяет формировать спектральные панорамы с учетом данных, полученных в ходе текущего и любого числа предшествующих циклов сканирования. После выполнения первого цикла сканирования таблица спектральной панорамы сохраняется в памяти компьютера. На следующем цикле формируется новая (текущая) таблица, а значения уровней в таблице предыдущей панорамы модифицируются в соответствии с выбранным методом обработки:
 - –обновление (в таблицу записывается новое значение, а старое стирается);
 - –накопление (в таблицу записывается больший из двух уровней);
 - –усреднение (в таблицу записывается среднее двух уровней).

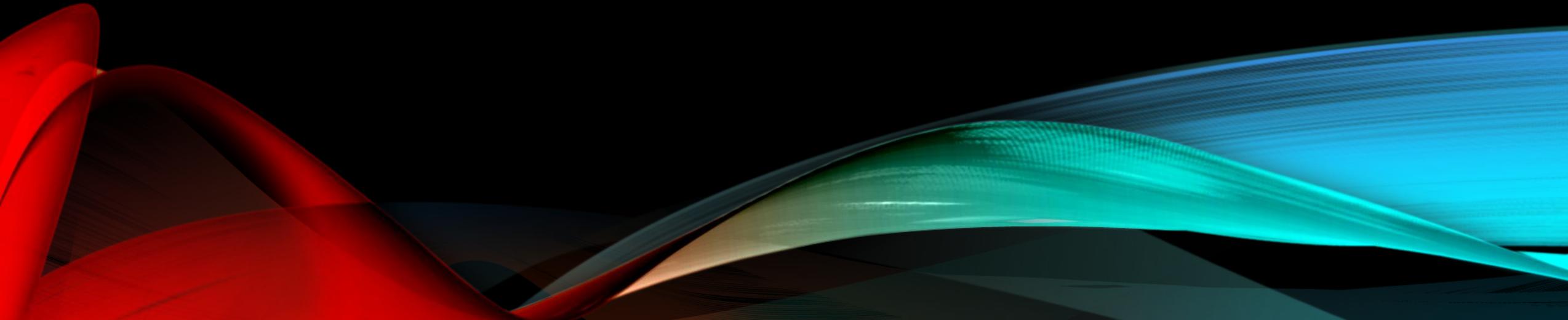
• Обнаружение

- Обнаружение – базовая операция выявления всех радиоизлучений (сигналов), уровень которых в заданном диапазоне превосходит установленное в задании пороговое значение (порог обнаружения). В процессе обнаружения программа оценивает параметры сигнала: ширину спектра, максимальный уровень, несущую частоту, а также классифицирует обнаруженные излучения, распределяя их по группам в соответствии с определенными признаками. Обнаруженные излучения автоматически классифицируются программой RS turbo по следующим признакам:
 - – «известные» и «неизвестные»;
 - – «обнаруженные ранее» и «вновь появившиеся»;
 - – «стандартные» и «нестандартные».

• Анализ

- Операции анализа необходимы для выявления среди множества обнаруженных сигналов «опасных» излучений, которые могут быть созданы передатчиками подслушивающих устройств. Идентификация (опознавание) сигналов подслушивающих устройств в программе RS turbo выполняется автоматически или в ручном режиме с помощью следующих операций:
 - –анализ гармонического состава излучений;
 - –корреляционный анализ откликов на акустические импульсы;
 - –спектральный анализ;
 - –временной и спектральный анализ сигналов на выходе демодулятора.
- Кроме того, в процессе анализа откликов на импульсы акустического зондирования программа измеряет расстояния от колонок акустической системы комплекса до микрофона и определяет местоположение микрофона в помещении (локализация источника излучения).

2. КОМПЛЕКСЫ ИЗМЕРЕНИЯ ПЭМИН.



- Программно-аппаратный комплекс **«СИГУРД»** представляет собой одну из самых совершенных систем оценки защищенности технических средств по каналу ПЭМИН и **предназначен** для проведения специальных исследований различных технических средств по выявлению, распознаванию и измерению сигналов их побочных электромагнитных излучений с максимальной степенью автоматизации процедур.

- **Основным отличием** данной системы от аналогичных разработок является четырёхэтапное обнаружение и измерение сигналов и полностью автоматическое, адаптивное распознавание частот (сигналов) ПЭМИН и автоматическое дистанционное управление параметрами тест-режимов на исследуемой ПЭВМ (на базе типового IrDA канала).



На **первом этапе** выполнения задания в автоматическом режиме осуществляется фильтрация всех входных сигналов по энергетическому критерию (превышение на заданную величину над уровнем шумов).

На **втором этапе** система выполняет коррекцию каждого выявленного сигнала, уточняя его частоту.

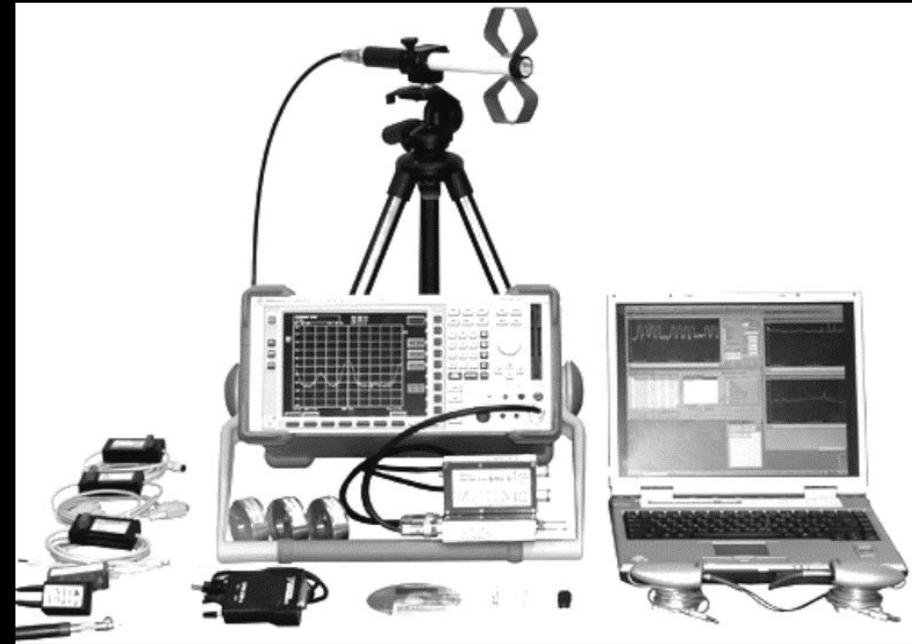
На **третьем этапе** осуществляется корреляционный двухступенчатый анализ сигналов в сравнении их с эталоном, хранящимися в файловой библиотеке.

На **последнем этапе** выполняется измерение выявленных «опасных» сигналов.

- Программно-аппаратный комплекс **«ЛЕГЕНДА»** предназначен для автоматизированного контроля побочных электромагнитных излучений и наводок, а также выявления и контроля акустоэлектрических преобразований в исследуемых технических средствах.

В состав комплекса входят:

- радиоизмерительный прибор «Agilente Technologies» E4411B, 9 кГц – 1,5 ГГц) с опциями;
- антенный коммутатор;
- система измерительная «Альбатрос» (9 кГц – 1 ГГц);
- эквивалент сети EMCO 3810/2;
- управляющая ЭВМ (обычно NoteBook) с интерфейсом GP-IB (National Instruments) и GP-IB кабелями;
- комплект для обнаружения акустоэлектрических преобразований;
- специальное программное обеспечение: управляющая программа, расчетные программы, комплект тестов для ПЭВМ (под WIN 95/98).



• ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ КОМПЛЕКСА:

- два этапа обнаружения ПЭМИН исследуемых технических средств в автоматизированном режиме (устранение «чужих сигналов»);
- выделение пика на фоне шумов («энергетический» критерий);
- распознавание образа сигнала (сравнение эталонного сигнала с сигналом приемного устройства в текущий момент);
- достоверность и повторяемость результатов измерений;
- возможность применения различных антенных систем в том числе и старого парка аппаратуры (RFT);
- возможность полуавтоматического обнаружения и измерения сигналов, измерения по сформированным шаблонам (наибольшая скорость проведения исследований);
- автоматическое формирование протоколов измерений;
- использование самых распространенных текстовых редакторов - «Microsoft Office», «Word Pad» и «Note Pad» при оформлении отчетных документов.

- Переносной комплекс для проведения инженерных исследований и исследований на сверхнормативные побочные электромагнитные излучения «**НАВИГАТОР-П6-Г**» (Е4407В).

- Предназначен для автоматического, автоматизированного и экспертного поиска сигналов ПЭМИН от проверяемых технических средств, измерения частоты и пикового значения амплитуды найденных сигналов, хранения, обработки и представления результатов поиска и измерений в удобном для оператора виде, и применяется на объектах сферы обороны и безопасности.



В программно-аппаратном комплексе реализованы четыре метода поиска ПЭМИН:

- метод сравнения панорам;
- аудио-визуальный метод;
- экспертный метод;
- параметрически-корреляционный метод.

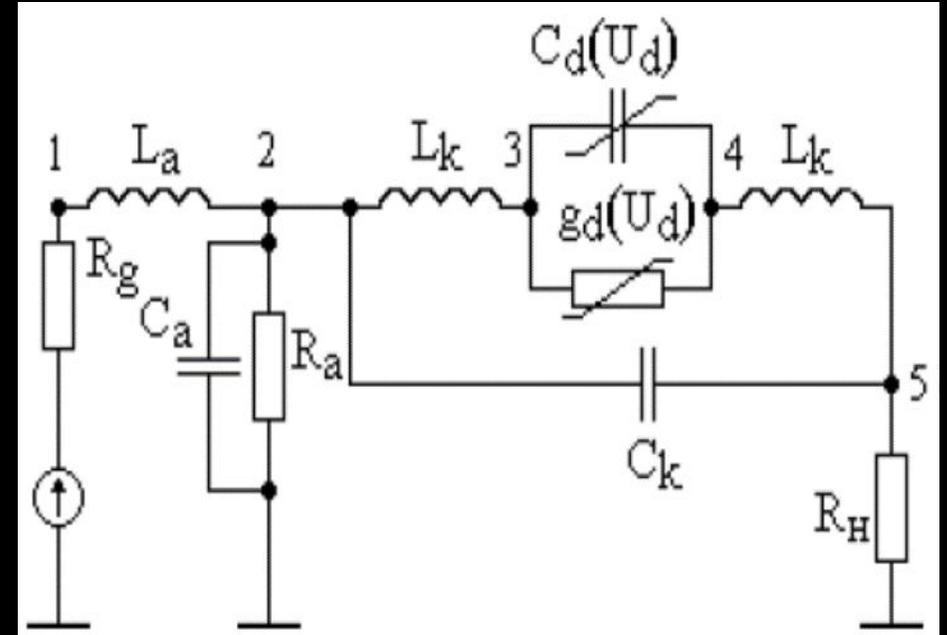
ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ПОЗВОЛЯЕТ:

- в автоматическом и автоматизированном режимах обнаруживать ПЭМИ тестируемой аппаратуры и формировать список обнаруженных ПЭМИ с регистрацией частоты, уровня ПЭМИ, полосы пропускания и антенны, при которых производилось обнаружение;
- в автоматизированном режиме верифицировать список обнаруженных ПЭМИ при включенном и выключенном тесте на исследуемой аппаратуре;
- отображать на мониторе компьютера спектры обнаруженных сигналов;
- проводить ручную верификацию списка обнаруженных ПЭМИ, используя осциллографический режим работы анализатора для наблюдения демодулированного тестового сигнала с одновременным прослушиванием теста в звуковом диапазоне частот на встроенных динамиках;
- проводить обработку полученных результатов и расчет зон разведдоступности ПЭМИ и коэффициента защищенности объекта в соответствии с утвержденными методиками;
- проводить инженерные исследования специальных технических средств (радиостанций, радиомикрофонов, систем съема информации и т.д.).

3. НЕЛИНЕЙНЫЕ ЛОКАТОРЫ.

МОДЕЛЬ РАДИОЛОКАЦИОННОГО НАБЛЮДЕНИЯ В УСЛОВИЯХ НЕЛИНЕЙНОЙ ЛОКАЦИИ

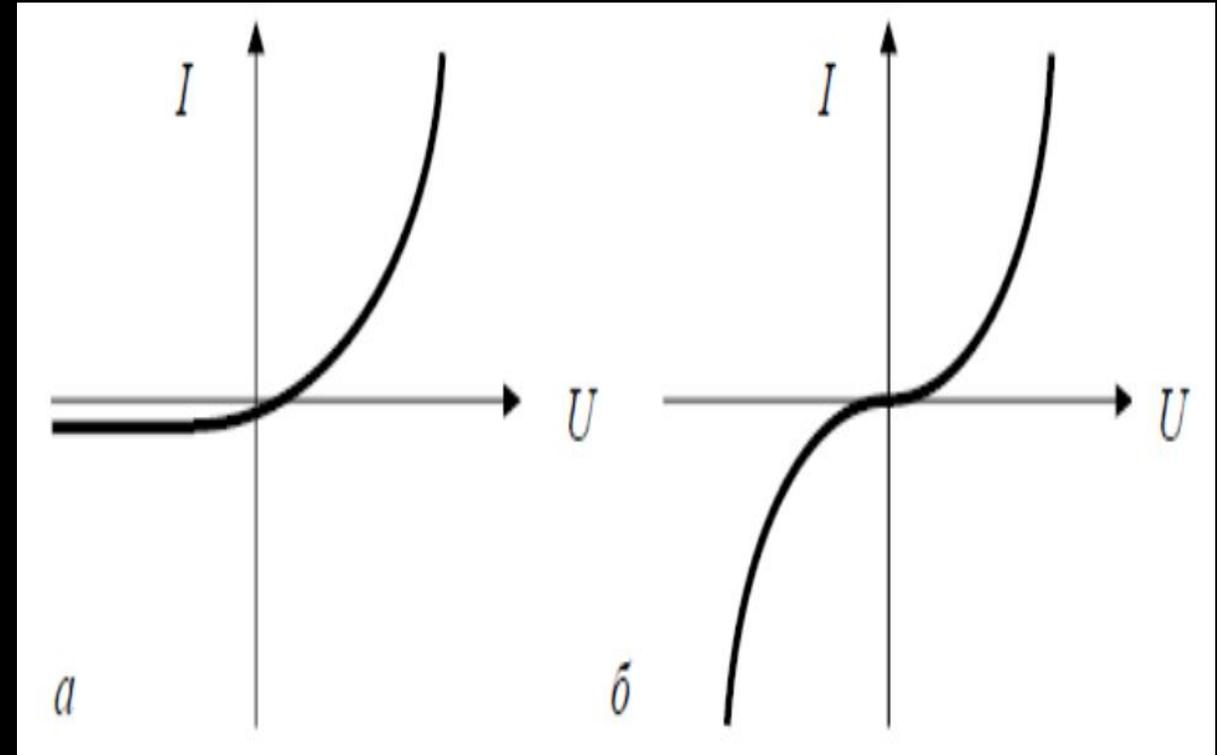
- Существенным отличием нелинейной локации от классического наблюдения (обнаружения) объектов с активным ответом является прямое преобразование падающей на объект энергии зондирующего сигнала в энергию высших гармоник. В связи с этим модель радиолокационного наблюдения (обнаружения) в условиях нелинейной локации можно классифицировать как наблюдение с полуактивным ответом, что связано с отсутствием потребления энергии объектом от специального источника питания.



- Электрическая схема замещения ЛН
- Мощность на гармониках, излучаемая объектом и, следовательно, эффективность обнаружения растет при увеличении мощности излучения локатора $P_{изл.}$, снижении частоты его излучения f и номера принимаемой гармоники N . Кроме того, чем ниже частота излучения локатора, тем меньшие значения имеют коэффициенты затухания, что также ведет к увеличению мощности сигнала от объекта.

ТЕХНОЛОГИЯ НЕЛИНЕЙНОЙ ЛОКАЦИИ

- Антенна ЛН облучает объект для определения наличия в нем электронных компонентов. Когда высокочастотный сигнал облучает полупроводниковые соединения, он возвращается на гармонических частотах с определенными уровнями, благодаря нелинейным характеристикам соединения. Но ложные срабатывания также могут возникнуть из-за того, что места соединения двух различных металлов или коррозионные металлические конструкции также вызывают гармонический отраженный сигнал вследствие своих нелинейных характеристик. Такие соединения называются ложными.



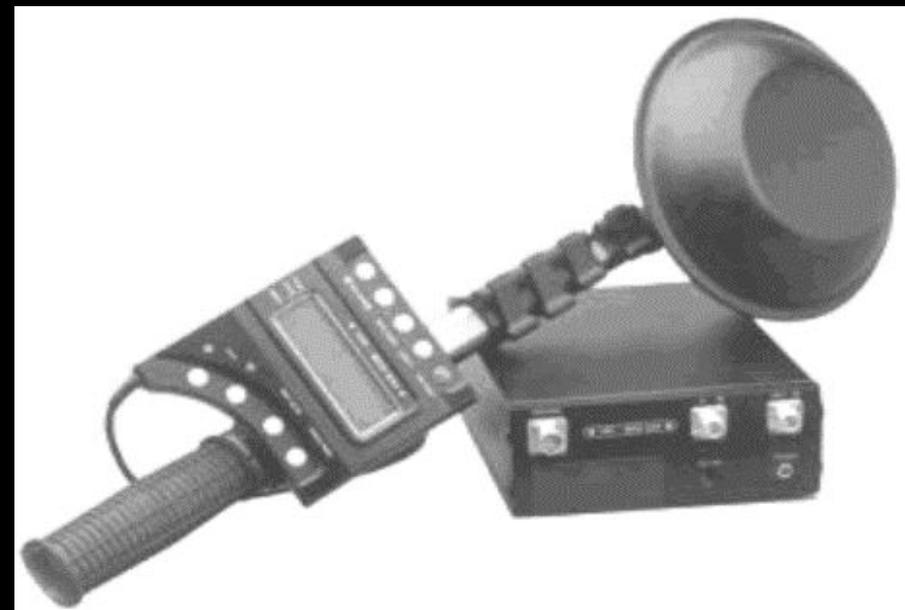
- Вольт-амперные характеристики полупроводникового и ложного соединений

ЭФФЕКТ ЗАТУХАНИЯ

- Большинство моделей ЛН использует непрерывное излучение в форме узкополосного сигнала. В последнее время все большее применение находят ЛН с импульсным режимом работы, имеющим ряд преимуществ. Преимущества заключаются в меньшем потреблении средней мощности от аккумуляторных батарей при большой скважности периодических зондирующих импульсов и в простоте демодулятора амплитудно-модулированного сигнала. Это объясняется следующими факторами. В импульсном режиме приемник принимает сигналы с частотой, приемлемой для восприятия человеческого слуха и зрения, при выключенном на этих интервалах времени передатчике, что обеспечивает снижение габаритов и энергоемкости источников питания. С другой стороны, для использования эффекта затухания ЛН непрерывного излучения обязательно должен иметь в приемном тракте высококачественные усилители с небольшим уровнем шума и хороший демодулятор для обеспечения качественного выделения аудио сигнала. При импульсном излучении с частотой следования импульсов выше порога частотного диапазона слышимости для качественной демодуляции аудио сигнала достаточно иметь простейший демодулятор амплитудно-модулированного сигнала.

- Измеритель вторичных полей (детектор нелинейных переходов) «NR 900 EM» предназначен для поиска²⁴ электронных устройств, содержащих полупроводниковые компоненты, независимо от их функционального состояния.

- Устройство обеспечивает возможность поиска радиомикрофонов, в том числе с дистанционным управлением, микрофонных усилителей проводных микрофонов, средств негласного контроля информации инфракрасного и ультразвукового диапазонов, средств звуко- и видеозаписи.

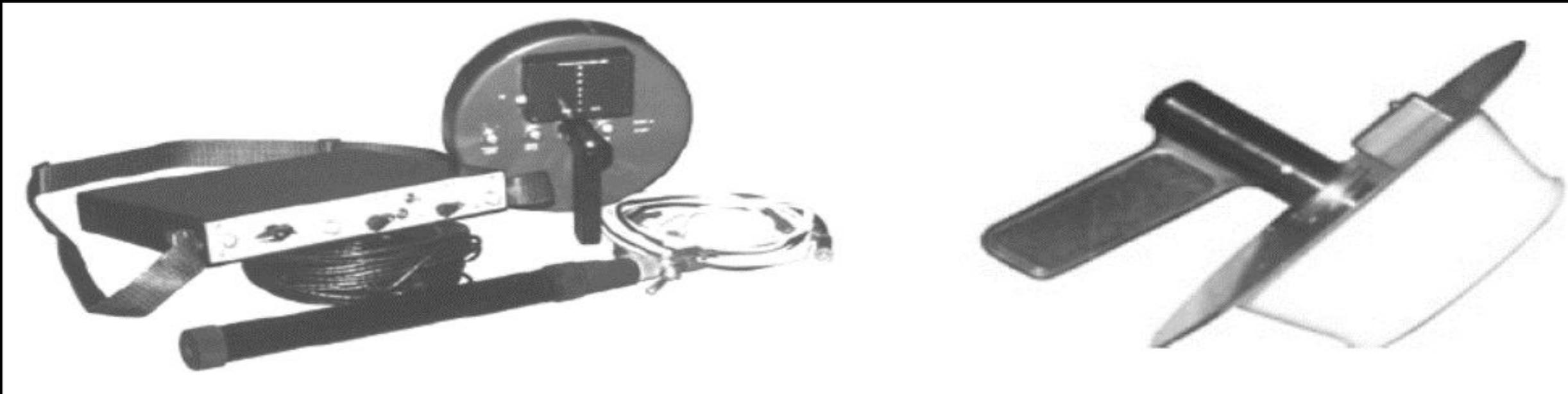


Устройство представляет собой портативный прибор, состоящий из антенной системы, передатчика и двух приемников, настроенных на удвоенную и утроенную частоты сигнала передатчика. Управление режимами работы осуществляется с помощью выносного пульта управления и индикации.

- Локатор состоит из **трех конструктивно независимых блоков**: приемопередатчика, антенной системы, пульта управления и индикации, соединяемых между собой кабелями. Антенная система и пульт управления и индикации в рабочем положении закреплены на раздвижной телескопической штанге.



- Нелинейные локаторы **«Октава»** рекомендуются для применения при проведении поисковых и досмотровых мероприятий, с целью обнаружения несанкционированной установки и проноса в помещение технических средств съема и передачи информации, для обнаружения предметов, не имеющих в своем составе полупроводниковых элементов, но снабженных специальными маркерами, с целью защиты от хищений.



- Нелинейные локаторы «Октава» являются сложными радиотехническими устройствами, состоящими из антенной системы (приемные и передающая антенны), передатчика и одного или двух приемников, настроенных на удвоенную (Октава-В, Октава-К, Октава-М) и утроенную частоту сигнала передатчика (Октава-3М).

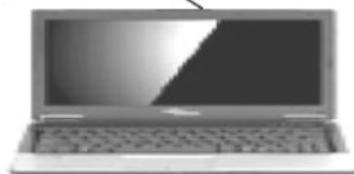
4. КОМПЛЕКС ДЛЯ ИЗМЕРЕНИЯ ХАРАКТЕРИСТИК АКУСТИЧЕСКИХ СИГНАЛОВ СПРУТ-7



- Комплекс **СПРУТ-7** обеспечивает проведение исследований характеристик и проверку эффективности систем акустического и виброакустического зашумления помещений, измерение уровней электрического и магнитного полей и наводок на проводные коммуникации, проведение статистической обработки результатов измерений.

- Комплекс может использоваться при измерении и гигиенической оценке шумов и вибрации в жилых и производственных помещениях на соответствие санитарным нормам.

Управляющий компьютер



Измерительный модуль



Модуль сопряжения



Дифференциальный усилитель



Модуль тестового акустического сигнала



Акустическая система



Источник питания



Антенна



В программно-аппаратный комплекс «Спрут-7» входят:

1. Измерительная подсистема на базе анализатора шума и вибраций 1-го класса точности SVAN в составе:

- измерительный модуль с октавным анализом, третьоктавным анализом и функцией БПФ;
- измерительный микрофон;
- измерительный акселерометр;
- измерительные щупы;
- измерительная пассивная антенна EMCO-6511 с рабочим диапазоном частот 0,2–5000 кГц либо аналогичная;
- адаптер – усилитель для подключения измерительных щупов и антенн; стойка для установки измерительного модуля;
- зарядное устройство.

В программно-аппаратный комплекс «Спрут-7» входят:

2. Подсистема источника тестового акустического сигнала в составе:

- модуль источника тестового акустического сигнала;
- экранированная акустическая система, используемая при проведении измерений акустоэлектрических преобразований;
- стойка для установки акустической системы;
- зарядное устройство.

3. Подсистема управления:

- модуль сопряжения с ПК;
- ПЭВМ типа «ноутбук»;
- специальное программное обеспечение.

4. Комплект оборудования для обеспечения автономного электропитания объектов ВТСС.

Благодарю за внимание!