

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего
образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 33

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ
ПРЕПОДАВАТЕЛЬ

доцент, к.т.н.

должность, уч. степень, звание

 01.11.22

подпись, дата

А.В. Воронов

инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

по курсу: Техническая защита информации

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. №

3931

 01.11.22

подпись, дата

К.В. Жук

инициалы, фамилия

Санкт-Петербург 2022

Цель работы:

Изучить методы противодействия техническим средствам добывания информации. Изучить принцип работы нелинейного локатора, и порядок действий при работе с данным техническим средством.

Ход выполнения работы:

Физические принципы работы нелинейного локатора

Способность нелинейного локатора обнаруживать радиоэлектронные устройства основана на следующем. Любые радиоэлектронные устройства (РЭУ), независимо от размера и функционального назначения, состоят из печатных плат с проводниками, которые представляют для зондирующего сигнала локатора набор элементарных антенн - вибраторов. В разрыв отдельных проводников включены полупроводниковые элементы: диоды, транзисторы, микросхемы.

В результате облучения РЭУ зондирующим сигналом на частоте f на его полупроводниковых элементах через элементарные антенны наводится переменная ЭДС. В силу нелинейного характера вольт-амперной характеристики (ВАХ) элементов РЭУ переменный сигнал высокой частоты локатора претерпевает нелинейное преобразование в набор гармоник, частоты которых равны кратному целому числу зондирующей частоты локатора ($2f$, $3f$ и т.д.). С помощью тех же самых проводников печатной платы (элементарных антенн) весь спектр, включающий сигналы как на основной частоте f , так и на частотах гармоник $2f$, $3f$ и т.д., переизлучается в эфир. Приемник локатора, принимая любую высшую гармонику переотраженного зондирующего сигнала локатора, устанавливает наличие в зоне облучения РЭУ. Так как амплитуда сигнала на гармонике резко убывает с увеличением ее номера, то в нелинейных локаторах в основном используют 2-ю и реже 3-ю гармоники.

Коэффициент преобразования энергии зондирующего сигнала в энергию высших гармоник очень мал, что относит нелинейные локаторы к системам ближнего действия. Существенное влияние на величину коэффициента преобразования оказывают значения мощности и частоты зондирующего сигнала локатора. Зависимость коэффициента преобразования от мощности зондирующего сигнала в первом приближении с точностью до 80% повторяет структуру ВАХ полупроводниковых элементов. Следовательно, на процесс преобразования влияет не величина средней мощности, а пиковая (импульсная) мощность сигнала.

Сам процесс преобразования не зависит от состояния РЭУ: активное (включенное) или пассивное (выключенное), но коэффициент преобразования, а, следовательно, и мощность сигнала гармоник, являются функцией состояния объекта. При активном режиме объекта поиска мощность переизлученного на гармониках сигнала возрастает.

Наличие нелинейности характерно не только для полупроводниковых элементов радиоэлектронных средств, но контактов между металлическими предметами с пленкой окислов на поверхности, например, ржавых прутьев в

железобетонных плитах домов. Все металлические контакты, в том числе и ржавчина, представляют собой нелинейный элемент с неустойчивым р-п переходом, поскольку он образован путем естественного прижима двух или более поверхностей. В физике полупроводников подобная структура известна как структура металл-окисел-металл, а нелинейный элемент подобной структуры называется МОМ-диод. Поэтому обнаружение 2-й гармоники в отраженном сигнале не является достаточным условием наличия закладного устройства. Одновременный анализ 2-й и 3-й гармоник позволяет приближенно провести селекцию их источников: полупроводников РЭУ и других металлических элементов с полупроводниковым эффектом. Только в результате последующего обследования места облучения достоверно выявляется закладное устройство.

Как правило, на индикаторном устройстве современного нелинейного локатора отображаются относительные уровни принимаемых сигналов на второй и третьей гармониках и их разница. Индикаторные устройства располагаются или на приемо-передающем блоке (локаторы SuperBroom, "Омега-3" и др.), или непосредственно на антенной штанге (локаторы NJE - 4000, NR-900E, "Энвис" и др.).

В нелинейных локаторах в основном используются передающие антенны с линейной поляризацией и приемные антенны - с круговой поляризацией.

Проникающая глубина зондирующего сигнала зависит от мощности и частоты излучения. Вследствие увеличения затухания электромагнитной волны в среде распространения с повышением частоты зондирующего сигнала (с ростом частоты наблюдается экспоненциальный рост затухания) и вследствие физической природы процесса преобразования частоты полупроводниковыми приборами, связанной с их частотными свойствами, и в частности с граничной рабочей частотой, уровень мощности преобразованного отраженного сигнала тем выше, чем ниже частота зондирующего сигнала локатора. Но для излучений с более низкой частотой ухудшаются возможности локатора по локализации места нахождения нелинейности, так как при приемлемых размерах его антенны расширяется ее диаграмма направленности. В основном в нелинейных локаторах используются частоты от 600 до 1 000 МГц.

При выборе частоты зондирующего сигнала необходимо учитывать и тот факт, что приемники нелинейных локаторов обладают высокой чувствительностью, поэтому на частотах приема не должно быть сигналов посторонних радиоэлектронных средств даже сравнительно небольшого уровня. В противном случае наличие мешающих сигналов значительно затрудняет процесс поиска закладных устройств. Например, в центре Москвы работа с нелинейным локатором "Энвис" может быть затруднена, так как в полосе приема отраженного сигнала на второй гармонике (около 1806 МГц) постоянно работает мощное радиоэлектронное средство.

Поэтому наиболее эффективно применение нелинейных локаторов, имеющих возможность перестройки рабочей частоты в некотором диапазоне.

Например, в нелинейном локаторе Orion (NJE - 400) фирмы ResearchElectronicsInternational (REI) предусмотрен автоматический режим выбора рабочей частота в диапазоне от 880 до 1000 МГц. При этом в качестве рабочей выбирается частота, на второй гармонике которой наблюдается наименьший уровень помех.

Состав НЛ

Обычно изделие состоит из следующих блоков:

- 1) Приемо-передающий блок с пультом управления, зарядным устройством и ремнем для переноски.
- 2) Антенный блок.
- 3) Телескопическая штанга.
- 4) Сетевой блок питания.
- 5) Кабель питания от сетевого блока.
- 6) Аккумулятор (находится внутри приёмно-передающего блока)

Конструктивно компоновка данных составляющих может отличаться от модели к модели, поскольку вариантов НЛ существует достаточно много.

Теоретические основы нелинейной локации

Антенна нелинейного локатора (НЛ) облучает объект для определения наличия в нем электронных компонентов. Когда ВЧ сигнал облучает полупроводниковые соединения (диоды, транзисторы и т.д.), он возвращается на гармонических частотах с определенными уровнями, благодаря нелинейным характеристикам соединения.

Однако ложные срабатывания также могут иметь при этом место, из-за того, что места соединения двух различных металлов или коррозионные металлические конструкции также вызывают гармонический отраженный сигнал вследствие своих нелинейных характеристик. Такие соединения мы будем называть ложными.

На рис.1 представлены вольт-амперные характеристики полупроводникового и ложного соединений.

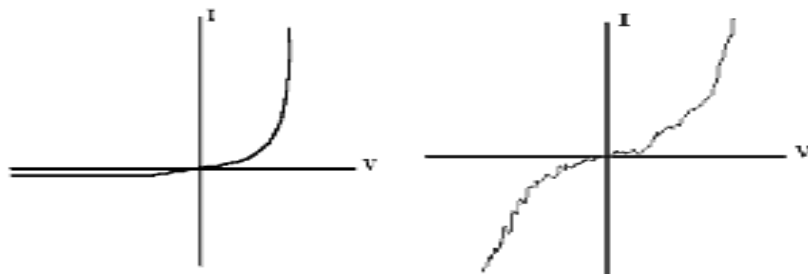


Рис.1. Вольт-амперные характеристики полупроводникового и ложного соединений.

Из-за различия в нелинейных характеристиках полупроводникового и ложного соединений, отклики 2-й и 3-й гармоник будут иметь различную интенсивность. Когда НЛ облучает полупроводник, отклик на второй

гармонике сильнее, чем на 3-ей. При облучении ложного соединения наблюдается обратный эффект: отклик на 3-ей гармонике сильнее, чем на 2-ой.

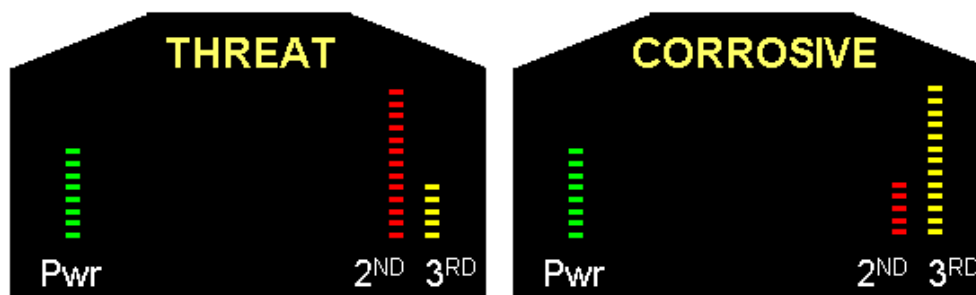


Рис.2. Сравнение уровней сигналов 2-ой и 3-ей гармоник при работе с НЛ (слева - полупроводник, справа - ложное соединение).

Эффект затухания

Большинство специалистов основываются на "эффекте затухания" при распознавании полупроводникового и ложного соединения. Этот эффект проиллюстрирован на рис.3. Если вы слушаете демодулированный аудиоотклик от настоящего полупроводника, то по мере приближения к нему антенны уровень шумов будет значительно понижаться. И напротив, по мере удаления от него уровень шума начнет возрастать и постепенно вернется к нормальному.

Демодулированный аудиосигнал достигает наименьшего значения непосредственно над полупроводниковым соединением и увеличивается до нормы в стороне от него.

При приближении антенны НЛ к ложному соединению, аудиосум может усилиться и достигнуть своего максимального значения непосредственно над ним или в некоторых случаях слегка уменьшиться. По мере удаления антенны НЛ аудиосум вернется к обычной норме.

Импульсное или непрерывное излучение

В зависимости от режима излучения нелинейные детекторы делят на детекторы с непрерывным и импульсным излучением.

Очевидно, что чем выше мощность излучения детектора, тем глубже проникает электромагнитная волна в облучаемую поверхность, и тем больше вероятность обнаружения помещенной в стену закладки. Но большая мощность излучения на высоких частотах оказывает вредное воздействие на оператора.

Для обеспечения его безопасности максимальная мощность излучения детектора в непрерывном режиме не должна превышать 3... 5 Вт. При импульсном режиме мощность в импульсе достигает 300 Вт, однако, средняя мощность очень мала. Например, в детекторах серии "Циклон" максимальная средняя мощность составляет 0,12 Вт, а детекторе "Октава" - от 0,45 Вт до 1,5 Вт.

Современные нелинейные локации имеют возможность изменения мощности зондирующего сигнала. Например, в локаторе NJE - 400 (непрерывного излучения) мощность регулируется в пределах от 10 мВт до 1 Вт, в SuperBroomPlus (непрерывного излучения) - от 1 мВт до 3 Вт, а в локаторе "Циклон-М" (импульсный) - от 80 до 250 Вт. Причем в некоторых локаторах (например, в SuperBroomPlus) мощность излучения устанавливается (снижается) автоматически в зависимости от мощности сигнала, принимаемого на второй гармонике, и тем самым предотвращается перегрузка приемника.

Приемники нелинейных локаторов с непрерывным излучением имеют чувствительность -120 ... 145 дБ, с импульсным - 110 ... 120 дБ и обеспечивают дальность обнаружения полупроводниковых элементов 0,5 ... 1 м и более. Максимальная глубина обнаружения объектов в маскирующей среде (строительных конструкциях) составляет десятки сантиметров. Например, локаторы серии "Циклон" обнаруживают радиоэлектронные изделия в железобетонных стенах толщиной до 50 см, в кирпичных и деревянных стенах - до 70 см.

В большинстве современных локаторов используются приемники с регулируемой чувствительностью. Например, в нелинейном локаторе "Энвис" диапазон регулировки чувствительности приемника составляет 45 дБ, а в NR-900E - 50 дБ.

Точность определения местонахождения РЭУ составляет несколько сантиметров (например, в локаторах "Родник" и "Циклон" - 2 см).

Радиолокаторы «Родник-ПМ», «Переход», «Энвис», SuperBroom и др. обеспечивают дополнительный режим прослушивания модулированных сигналов локатора, отраженных от полупроводниковых элементов закладок. Принцип модуляции аналогичен модуляции при высокочастотном навязывании.

Современные нелинейные локаторы имеют небольшие размеры, вес и позволяют работать как от электросети, так и от автономных источников питания (аккумуляторов).

Например, у нелинейного локатора "Омега" вес приемно-передающего блока составляет 2 кг, а антенны со штангой - 0,8 кг. Вес нелинейного локатора "Циклон-М" в упаковке (кейсе) - 5,5 кг (при этом вес приемно-передающего блока составляет 1,2 кг). У нелинейного локатора Orion (NJE - 400) приемно-передающий блок и антенна закреплены на одной телескопической штанге, и общий вес конструкции не превышает 1,8 кг. Для удобства работы в этом локаторе используются беспроводные инфракрасные наушники.

Ряд закладных устройств выполняются по МОП-технологии, в экранированных корпусах. Поэтому их обнаружение даже с использованием нелинейных локаторов затруднено, так как уровень переизлученных сигналов на второй и третьей гармониках незначителен.

Большинство моделей НЛ, производимых в мире, используют непрерывное излучение (CW), т.е. излучают непрерывный узкополосный сигнал. Однако существуют НЛ, которые работают в импульсном режиме, что

дает ряд преимуществ. Одно из них - меньшее потребление тока аккумуляторных батарей при хорошей конструкции передатчика. Таким образом, приемник принимает сигналы с частотой, приемлемой для восприятия человеческого слуха и зрения, в то время как передатчик выключается на значительные интервалы времени. Это позволяет уменьшить габариты и энергоемкость аккумуляторных батарей и источников питания. Кроме того, для использования эффекта затухания, описанного выше, НЛ непрерывного излучения обязательно должен иметь высококачественные малошумящие усилители в приемном тракте и хороший демодулятор для обеспечения качественного аудио. Еще одним методом аудиодемодуляции сигналов является импульсное излучение. Если частота следования импульсов выше порога частотного диапазона слышимости, то в этом случае для качественной демодуляции аудио сигнала достаточно простейшего АМ демодулятора. Не имеет значения, какой тип излучения использует НЛ импульсный или непрерывный, если он прост в обращении и обеспечивает хорошую аудио демодуляцию. НЛ «Катран» позволяет прослушать АМ и ЧМ аудио, используя импульсное излучение для амплитудной демодуляции и непрерывное для частотной, что максимально использует "эффект затухания".

Важно понимать, что при работе с НЛ имеют место 2 процесса:

1. Обнаружение нелинейного соединения.
2. Распознавание типа соединения (полупроводник или ложное).

Методика работы с нелинейными локами

При работе локатор должен иметь не только значительную дальность обнаружения, но и возможность регулировки его основных параметров (как правило мощность излучения или, как в случае с «Катраном» уровень интеграции цифровой обработки сигнала) для достижения необходимой глубины обнаружения в исследуемом материале.

Однако, не менее важно использовать методы анализа демодулированного аудио, основанные на эффекте затухания и вибрационном физическом воздействии.

Для максимальной надежности хороший НЛ должен иметь несколько способов определения различия между настоящим полупроводником и ложным соединением.

В «Катране» реализованы: режимы импульсного и непрерывного излучения, позволяющие достичь максимальной дальности обнаружения; сравнение уровней сигналов 2-й и 3-й гармоник; а также различные способы, позволяющие отличить полупроводник от ложного соединения. В «Циклоне» реализован импульсный многочастотный режим.

При проведении поисковых мероприятий вероятность обнаружения (или не обнаружения) закладных устройств напрямую зависит от возможностей используемого оборудования и наличия у поисковой бригады практического опыта по работе с ним.

Первый и главный признак – наличие электронной составляющей, или в упрощении **p-n** перехода, который является обязательным составным

элементом любой электронной схемы. Транзистор, диод, микросхема— везде есть р-п переход.

При выполнении определенных требований (особенностей установки и изготовления) возможен пропуск закладного устройства при поиске его с помощью НЛ.

Примеры сложных ситуаций:

1. Изделие выполнено в корпусе, надежно изолирующем электронику от воздействий зондирующего сигнала. Если сигнал не получен элементом схемы, то соответственно, и откликов от него нельзя получить.

На сегодняшний день такие изделия не так часто встречаются, но все же они присутствуют на рынке специальных технических средств (СТС) и нельзя исключать возможность их применения.

Как пример можно привести несколько разработанных в России цифровых диктофонов в экранированных корпусах и уже появившиеся радио-закладки с исполнением фильтрации по антенному входу с экранированием корпуса.

2. Изделие установлено в электронное средство, легально размещенное в проверяемом помещении (например, радиозакладка в элементе питания кварцевых часов).

Способов обнаружения этих средств **несколько**:

- 1) визуальный осмотр,
- 2) рентгенография,
- 3) сравнение с проверенным аналогом,
- 4) контроль изменения различных физических параметров.

3. Изделие установлено в сложной помеховой обстановке. Например, в железобетонной стене за сеткой-рабицей (возможна установка электронного стетоскопа) выявление таких средств весьма сложно, так как НЛ получает смесь сигналов закладки и коррозии сетки-рабицы.

4. При определенной ширине металлических конструкций (например, балки) зондирующий сигнал может отразиться от нее и не дойти до закладки. Выявление металлодетектором покажет прямую из металла, проходящую вдоль стены. Объект идентифицируется как балка. Способы выявления – контроль за строительством объекта, постоянный мониторинг возможных технических каналов утечки информации.

5. Отсутствие в закладном устройстве, расположенном в проверяемом помещении, электронной составляющей, расположенной в зоне действия НЛ (например, микрофон типа СОМ, звуковод на удаленном окончании которого расположен микрофон с высококачественным усилителем. Способы обнаружения— тщательный визуальный осмотр проверяемого помещения.

6. Использование естественных каналов перехвата информации (радиотелефоны, вентиляционные шахты, ПЭМИН электронных средств). Способ выявления—оценка эффективности защищенности контролируемого помещения.

Одной из наиболее важных характеристик НЛ является его мощность, а точнее возможности глубины регулировки мощности и чувствительности. Большой диапазон таких регулировок дает возможность эффективно проводить работы в различных условиях помеховой обстановки.

В большинстве случаев приходится уменьшать мощность, чтобы «не поймать», например, телевизор, расположенный за двумя стенами.

Отличие коррозионного диода или МОМ-диода от р-п перехода

Если при простукивании объекта наблюдается треск, что нехарактерно при получении сигнала р-п перехода, то обнаружен МОМ-диод (например, ключи, скрепки, или монеты, положенные одни на другие). Для более качественно получения отклика рекомендуется использовать резиновый молоток.

Иногда после удара молотком МОМ-диод разрушается и сигнал пропадает. Например, часто в местах пересечения направляющих подвесных потолков происходит образование МОМ-диода. Достаточно легкого удара, чтобы его разрушить.

Еще одной сложностью при нелинейной локации, является наличие в помещении электронных средств. В некоторых случаях нет возможности вынести из помещения оборудование и его переносят из угла в угол. В таких условиях может появиться так называемый «призрак». Вы наводите антенну на стену и получаете четкий отклик, который идентифицируется по всем признакам как р-п переход. Для убедительности обнаружения направьте антенну НЛ на обнаруженный объект под другим углом. Если сигнала нет, то возможной причиной его появления может стать компьютер, стоящий в трех метрах позади.

Несмотря на направленную антенну, у всех НЛ существует задний лепесток диаграммы направленности. В некоторых случаях могут быть захвачены электронные средства, расположенные в четырех метрах позади. Передвиньте электронику в другое место, и, если сигнал пропал, то это «призрак», то есть прием сигнала полученного из-за наличия обратного лепестка диаграммы направленности.

Направив антенну на объект, с двух разных точек, можно определить, находится он непосредственно за стеной или на удалении.

Возможно, получение сигнала отклика при наводке зондирующего сигнала на проводные линии, в окончании которых находятся электронные средства. Например, Вы можете поймать ретранслятор или телевизор, в который вставлена антенна, и сигнал наводится по коаксиальному кабелю. Достаточно выдернуть проводник из электронного устройства и сигнал пропадет.

Вывод:

Выполнение данной теоретической лабораторной работы дало понимание физических принципов работы нелинейных локаторов, было дано объяснение различий между импульсными НЛ и НЛ постоянной мощности. Также был разобран процесс работы с НЛ. Кроме этого были обозначены различные трудности и особенности, которые могут возникнуть у оператора во время поиска электронных закладных устройств.