Фазированная антенная решетка — тип антенн, в виде группы антенных излучателей, в которых относительные фазы сигналов изменяются комплексно, так, что эффективное излучение антенны усиливается в каком-то одном, желаемом направлении и подавляется во всех остальных направлениях.

Управление фазами (фазирование) позволяет радару с применяемой ФАР:

а) формировать (при весьма разнообразных расположениях излучателей) необходимую диаграмму направленности(ДН) антенны (например, остронаправленную ДН типа луч);

б) изменять направление луча неподвижной антенны, таким образом осуществляя быстрое (в ряде случаев практически безынерционное) сканирование — качание луча;

в) управлять в определенных пределах формой ДН — изменять ширину луча, интенсивность (уровни) боковых лепестков и т.п. (для этого в ФАР иногда осуществляют также управление и амплитудами волн отдельных излучателей).

Применение подобных антенных решеток дает следующие преимущества:

а) решетка из N элементов позволяет увеличить приблизительно в N раз коэффициент направленного действия (КНД) (и, соответственно, усиление) антенны по сравнению с одиночным излучателем, а также сузить луч для повышения точности определения угловых координат источника излучения в навигации и радиолокации.

б) с помощью решетки удается поднять электрическую прочность антенны и увеличить уровень излучаемой (принимаемой) мощности путем размещения в каналах решетки независимых усилителей;

в) важным преимуществом решетки является возможность быстрого (безынерционного) обзора пространства за счет качания луча антенны электрическими методами (электрического сканирования).

г) имеется ряд конструктивно-технологических преимуществ, по сравнению с другими классами антенн. Так например, улучшение массогабаритных характеристик бортовой аппаратуры происходит за счет использования печатных антенных решеток. Снижение стоимости больших радиоастрономических телескопов достигается благодаря применению зеркальных антенных решеток.

Целью данной работы является разработка метода калибровки многолучевой антенны. В соответствии с поставленной целью были решены следующие задачи:

а) проведен обзор аналогичных многолучевых антенн и методов их настройки.

б) разработана блок схема алгоритма метода калибровки;

в) рассчитана диаграмма направленности антенной решетки, состоящей из шестнадцати элементов;

г) сформирована диаграмма направленности с учетом наличия мешающих сигналов;

д) описан алгоритм метода калибровки, предполагающий использование шумоподобного сигнала.

Список использованных источников:

1. Цифровое формирование луча в системах связи: будущее рождается сегодня /В.И. Слюсар– Электроника: НТБ.–2001.–№ 1.–С. 6–12.

2. Идеология построения мультистандартных базовых станций перспективных систем связи /В.И. Слюсар–Радиоэлектроника (Изв. вузов).–2001.–№ 4.–С. 3–12.

3. Активные фазированные антенные решетки /Под ред. Д.И. Воскресенского. М.: Радиотехника,2003.–448с.

4. Устройства СВЧ и антенны. Проектирование фазированных антенных решеток: учеб. пособие / Под ред. Д.И. Воскресенского. М.: Радиотехника. 2003.–592с.

5. Антенны с обработкой сигнала: учеб. пособие/Д.И. Воскресенский.М.: САЙНС-ПРЕСС. 2002.–80с.

ПРОГРАММНАЯ ПОДДЕРЖКА СИСТЕМ ПЕРЕДАЧИ ЗАШИФРОВАННЫХ ДАННЫХ ДЛЯ МОБИЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кальченко А.Н.

Геливер О.Г

Информационная сфера играет возрастающую роль в обеспечении безопасности всех сфер жизнедеятельности общества. Через эту сферу реализуется значительная часть угроз национальной безопасности государства. Одними из основных источников угроз информационной безопасности являются деятельность иностранных разведывательных и специальных служб, преступных сообществ, организаций, групп, формирований и противозаконная деятельность отдельных лиц, направленная на сбор или хищение ценной информации, закрытой для доступа посторонних лиц. Последствия недооценки вопросов безопасности могут оказаться весьма печальными. В настоящее время и в ближайшем будущем наибольшую опасность представляет информационная незащищенность. Поэтому при обеспечении информационной безопасности необходимо учитывать, что обмен информацией является первейшим условием жизнедеятельности каждой организации. Известно, что система обеспечения информационной безопасности включает в себя сбор, классификацию, анализ, оценку, защиту и распространение актуальной информации для обеспечения защиты ресурсов с целью оптимальной реализации ее целей и интересов. Расширение применения современных информационных технологий делает возможным распространение различных злоупотреблений, связанных с

использованием вычислительной техники (компьютерных преступлений). Для противодействия им или хотя бы уменьшения ущерба необходимо грамотно выбирать меры и средства обеспечения защиты информации от умышленного разрушения, кражи, порчи, несанкционированного доступа, несанкционированного чтения и копирования. Необходимо знание основных законодательных положений в этой области, организационных, экономических и иных мер обеспечения безопасности информации. За последнее время все чаще формы, методы и способы ведения различных видов шпионажа, применяемые в информационных войнах, приводят к прямым вооруженным конфликтам. Примером информационного противостояния российских политиков с сепаратистами могут служить события (развертывание испытательного полигона новых технологий информационной войны) в Чеченской республике. Эта война началась как непонимание или различие в трактовке понятий о суверенитете, а закончилась вооруженной борьбой с организованной преступностью, террористами и радикальным исламизмом. В Уставе МО США дано следующее определение: «Информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в интересах национальной военной стратегии и определяемых путем влияния на информацию и информационные системы противника, при одновременной защите собственной информации и своих информационных систем». Информационное оружие наносит максимальный урон в том случае, если оно применяется против информационно – телекоммуникационных сетей постоянно и осмысленно. Причем, мишенью являются все элементы информационных технологий, ресурсов и систем, мыслительная часть человеческой деятельности, имеющие потенциальную возможность для перепрограммирования (воздействия на психику). Заставить противника или конкурента изменить свое поведение можно лишь с помощью создания информационной угрозы (риска). На основании факторов является целесообразно и актуально рассмотрение вопроса по программной поддержке систем передачи зашифрованных данных для мобильных операционных систем.

Список использованных источников:

1. Одом У. Компьютерные сети. Первый шаг = Computer Networking:First-step / Пер. В. Гусев. — СПб.: «Вильямс», 2006. — 432 с.

2.Касперски К. Техника и философия хакерских атак. - СОЛОН-Р-М. -1999г.

3.Хоникатт, Джерри Использование Internet; М.: Вильямс; Издание 3-е,1998. - 270 с.

4.Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. –М.: КУДИЦ-ОБРАЗ, 2001, - 368 с.

5.Пол Мак-Федрис. Microsoft Windows 7. Полное руководство Microsoft Windows 7 Unleashed. — М.: Вильямс, 2012

6. Виджэй Боллапрагада, Кэртис Мэрфи, Расс Уайт Структура операционной системы Android = Inside Android. — М.: «Вильямс»,2002.

ИСТОРИЯ РАЗВИТИЯ ВООРУЖЕНИЯ ПРОТИВОВОЗДУШНОЙ ОБОРОНЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Каплярчук Е.А.

Денисевич А.В.

Приведена краткая история справка по развитию отечественных и зарубежных средств ПВО.

В первой половине 70-х годов было завершено создание системы вооружения и военной техники (ВВТ) войск ПВО Сухопутных войск первого поколения, которая включала в себя совокупность зенитных ракетных и артиллерийских комплексов, радиолокационных средств обнаружения СВН, наведения ЗУР и наводки зенитных пушек, а также в определенной мере автоматизированных средств управления войсками ПВО СВ в оперативном и тактическом звеньях. Система ВВТ войсковой ПВО первого поколения была способна обеспечить намного более эффективную борьбу с аэродинамическими СВН вероятного противника в период 70-х начала 80-х годов по сравнению с существовавшими до нее вооружением и военной техникой ПВО СВ первого послевоенного десятилетия. После принятия на вооружение новых образцов ВВТ началось их массовое серийное производство, оснащение ими войск ПВО СВ и освоение их личным составом этих войск.

Хотя совокупность средств ПВО СВ первого поколения создавалась как система вооружения практически без научного системного обоснования, она получилась достаточно эффективной на всех уровнях войсковой иерархии (от фронта до батальона). С ее помощью войска ПВО СВ могли не только полностью перекрыть огнем ракетных и ствольных зенитных комплексов весь диапазон высот боевого применения авиации вероятного противника по Сухопутным войскам в пределах их оперативного построения, но и противодействовать пролету ее в наш глубокий тыл.

Достаточно высокая эффективность ряда образцов ВВТ ПВО СВ («Куб»-«Квадрат», «Стрела-2», «Шилка») была подтверждена в боевых действиях, в частности на Ближнем Востоке.

Система вооружения войск ПВО СВ первого поколения создавалась примерно одновременно с разработкой подобных зенитных комплексов в странах НАТО. По своим боевым характеристикам отечественная система вооружения ПВО СВ практически была на одном уровне с системой вооружения войсковой ПВО стран НАТО. Наши основные ЗРК «Круг» и «Куб» несколько уступали по размерам зон поражения американским прототипам - ЗРК «Найк-Геркулес» и «Хок», но значительно превосходили их по мобильности, что было особенно важно для вооружения и военной техники Сухопутных войск. Следует отметить, что существенным недостатком указанных отечественных комплексов ПВО была не вполне достаточная