**Радиоэлектронная разведка виды:**

• Радиоразведка - Communication Intelligence (COMINT)

• Радиотехническая разведка - Electromagnetic Intelligence (ELINT)

• Радиолокационная разведка - Radar Intelligence (RADINT)

• Телевизионная разведка - Television Intelligence (TELINT)

• Разведка с помощью устройств инфракрасной техники -Infrared Sets Reconnaissance

**Радиоразведка - самый старый вид радиоэлектронной разведки. Она нацелена против различных видов радиосвязи. Основное содержание радиоразведки - обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций, пеленгование их сигналов, анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения источников излучения. Сведения радиоразведки о неприятельских станциях, системах их построения и о содержании передаваемых сообщений позволяют выявлять планы и замыслы противника, состав и расположение его группировок, установить местонахождение их штабов и командных пунктов управления, место размещения баз и стартовых площадок ракетного оружия и др.**



**Радиотехническая разведка - вид радиоэлектронной разведки по обнаружению и распознаванию радиолокационных станций (РЛС), радионавигационных и радиотелекодовых систем, использует методы радиоприема, пеленгования и анализа радиосигнала. Средства радиотехнической разведки позволяют:**

• Установить несущую частоту передающих радиосредств,

• Определить координаты источников излучения,

• Измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры),

• Установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная),

• Определить структуру боковых лепестков излучения радиоволн,

• Измерить поляризацию радиоволн,

• Установить скорость сканирования антенн и метод обзора пространства РЛС,

• Проанализировать и записать информацию.

**Радиоэлектронная разведка - ее структура, особенности и возможности**



**Этот вид разведки обладает следующими особенностями:**

• Действует без непосредственного контакта с объектами разведки,

• Охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн разных частот,

• Функционирует непрерывно в разное время года и суток и при любой погоде,

• Обеспечивает получение достоверной информации, поскольку она исходит непосредственно от противника (за исключением случаев радиодезинформации)

• Добывает большое количество информации различного характера и содержания,

• Получает информацию в кратчайшие сроки и чаще всего в реальном масштабе времени,

• Малоуязвима и во многих случаях недосягаема для противника,

• Действует скрытно. Противник, как правило, не в состоянии установить факт разведки.



**Радиоэлектронная разведка в зависимости от ее целевого назначения подразделяется на стратегическую и тактическую.**

Стратегическая радиоэлектронная разведка ведется в интересах правительственных органов и высшего военного командования с целью добывания всесторонней информации о разведываемой стране через его радиоэлектронные средства. Такая информация необходима для подготовки вооруженных сил и ресурсов страны к войне, принятия решения о начале военных действия и умелого ведения стратегических операций.



Тактическая радиоэлектронаая разведка считается одним из основных видов обеспечения войск информацией путем непрерывного слежения за электромагнитным излучением многочисленных военных устройств и система противника. Она в состоянии добывать важные сведения для ведения боевых действий силами соединений, частей и подразделений.

Различают наземную, морскую, воздушную и космическую радиоэлектронную разведку. По своему содержанию информация, добываемая этим видом разведки, делится на оперативную и техническую.



Оперативная информация включает сведения, которые необходимы для решения оперативных задач военного командования. К ним относятся:

• Открытая или зашифрованная смысловая информация, передаваемая противоборствующей стороной по различным каналам радиосвязи,

• Тактико-технические данные и особенности разведываемых активных радиоэлектронных систем (частота настройки, вид модуляции и манипуляции, диаграммы направленности антенн, мощность излучения и т.п.), состовляющие их "электронный почерк",

• Типы радиоэлектронных систем: радиосвязи, радиолокации, радионавигации, наведения ракет и дальнего обнаружения, различные телеметрические систмы передачи данных,

• Количество обнаруживаемых радиоэлектронных систем противника,

• Местоположение и территориальная плотность размещения источников излучения электромагнитной энергии противника.

Изучая технические характеристики и особенности радиоэлектронных систем противника, можно определить область их применения и принадлежность. Сопоставляя эти данные с уже известными, полученными разведкой по другим каналам, можно сделать вывод о назначении разведываемых технически средств. Зная это и определяя типы и количество радиоэлектронных средств противника, можно установить дислокацию войсковых частей, военных баз, аэродромов и других объектов. Так, например, зная число радиолокационных станций наведения управляемых зенитных ракет в какой-либо зоне ПВО противника, можно сделать правильные выводы о количестве батарей зенитных ракет, установленных в этой зоне.

… для анализа и обработки добываемой информации очень важное значение имеют точная фиксация времени начала и конца работы излучающих радиоэлектронных средств и правильное определение их местоположения. Эти данные позволяют установить степень активности противника в определенной территориальной зоне. Указывается, что перед запуском межконтинентальных баллистических ракет с мысла Каннаверал наблюдалось заметное увеличения числа источников электромагнитных излученийв этом районе за счет повышения активности работы радиолокационных станций сопровождения и наведения, средств радиосвязи и передачи данных, а также телеметрических сетей.

Техническая информация содержит сведения о новых системах оружия и управления радиоэлектронными устройствами и об их электрических характеристиках, используемымми разведываемой страной впервые. Целью добывания технической информации является своевременная разработка аппаратуры и методов радиоэлектронной разведки новых систем оружия и средств управления противника. По мнению американских специалистов, техническая информация о новой радиоэлектронной аппаратуре потенциальных противников особбенно нужна для создания эффективных технических средств и методов радиопротиводействия и контррадиопротиводействия.

Для получения такой информации средстваи радиоэлектронной разведки ведется систематическая разведка новых, ранее неизвестных источников радиопередач, отличающихся диапазоном частот, видами модуляции и манипуляции, параметрами импульсного сигнала, диаграммой направленности антенны и другими характеристиками. Зарубежные авторы указывают следующие наиболее важные источники радиоэлектронной разведки:

• Активные средства радиосвязи, используемые во всех видах вооруженных сил и в интересах управления государством,

• РЛС разных типов и назначений, применяемые, главным образом, в противовоздушной обороне,

• Автоматизированные системы управления, слежения и наведения ракетного и противоракетного оружия, а также космических объектов,

• Радионавигационные системы, используемые в морской, воздушной и космической навигации,

• Различные телеметрические системы передачи информации.

**Технические средства радиоэлектронной разведки**

**В комплекс технических средств радиоэлектронной разведки входят следующие устройства:**

• Приемные антенны направленного и ненаправленного действия,

• Радиоприемники,

• Радиопеленгаторы,

• Устровства панорамного обзора,

• Анализаторы спектра принимаемых сигналов,

• Устровйства для автоматического отсчета сдвигов пеленга и частоты,

• Выходные устройства для приема сигналов телефонных и телеграфных уплотненных каналов радиосвязи,

• Оконечные устройства слухового приема (телефоны, динамики)

• Устровйства документирования сигналов,

• Приборы расшифровки, обработки и хранения принятой информации,

• Средства управления, связи и передачи добываемой информации.



**Перехват информации после 2000 года**

С середиты 90-х годов разведывательные агенства начали испытывать значительные трудности в обеспечении глобального доступа к системам коммуникации. Эти трудности будут продолжать увеличиваться во время и после 2000 года. Главной причиной является сдвиг телекоммуникаций в область оптических линий связи высокой пропускной способности. Проблема состоит в обеспечении физического доступа. За исключением случаев, когда линия проходит через территорию дружественного государства, эффективный перехват возможен только путем вмонтирования специальных устройств в повторители (где они есть). Данное ограничение скорее всего выведет многие зарубежные высокопропускные линии связи из разряда прослушиваемых. Физические размеры оборудования, необходимого для обработки данных, вместе с системами энергообеспечения, передачи информации и записи делает скрытое прослушивание непрактичным и опасным занятием.Даже в тех случаях, когда доступ уже есть (как в случае КОМСАТ), распространение новых систем связи ограничит собирание информации с помощью новых способов, частично по бюджетным ограничениям, частично из-за невозможности доступа, скажем к спутниковым сиcтемам типа Иридиума.

В последние 15 лет значительное технологическое преимущество, в свое время имеющиеся у агенств сбора информации, полностью испарилось. Их главные системы покупаются в готовом виде и равны, если не хуже, систем, используемых в крупных промышленных или академических организациях. Различаются они только в степени защиты от излучения электромагнитных сигналов, по которым можно анализировать их работу. Разведывательные агенства, занимающиеся перехватом информации признают, что длительная война против гражданских и коммерческих шифровальных систем проиграна. Академическое и промышленное сообщество высококвалифицировано в вопросах криптографии и криптологии. Интернет и глобальный рынок создали свободный поток информации, компьютерных систем и алгоритмов. NSA не смогла сломать криптозащиту путем обязательного хранения ключей от шифров под предлогом охраны правопорядка.

**Оборудование систем перехвата информации**

Десятки работающих на оборону предприятий США в Силиконовой Долине или в Мэрилендском поясе возле Вашингтона выпускают слжнейшую аппаратуру для NSA. Основные корпорации США, такие как Локхид Мартин, Спейс Систем, ТРВ, Рейтеон и Бендикс также получают контракты от NSA по оснащению основных узлов сбора информации. Полный перечень производимого оборудования находится за пределами данного отчета. Состояние дел в технологии современной электронной разведки, однако, может быть продемонстрировано на примере некоторых технологий обработки двух специализированных поставщиков NSA: Applied Signal Technology Inc (AST, Sunnyvale, California) и The IDEAS Operation of Columbia, Мэриленд (часть Science Applications International Corporation (SAIC)). Обе компании имеют директорами бывших старших сотрудников NSA. Когда это явно не указано, предназначение оборудования для перехвата информации может быть идентифицировано по маркировке "TEMPEST screened". AST утверждает, что "оборудование используется для сбора сигналов с зарубежных средств телекоммуникаций правительством США". Одни ведущий специалист по криптографии емко описал корпорацию AST как "магазин `все для ЭШЕЛОНА`".

• Выделение и анализ сигнала из широкополосных линий связи

• Фильтрование, обработка и анализ факсов

• Анализ траффика, распознавание ключевых слов, получение текста и анализ тем

• Системы распознавания речи

• Непрерывное распознавание речи

• Идентификация говорящего и другие методы выбора голосовых сообщений

• Снижение нагрузки или подрыв криптографических систем



**Спецслужбы, чьи функции включают ведение радиошпионажа**

• Россия - Федеральное агентство правительственной связи и инфомрации (ФАПСИ), третий главк (ГУРРСС)

• США - Агентство национальной безопасности

• Великобритания - Центр правительственной связи

• Франция - Управление военной разведки DRM

• Канада - Бюро безопасности связи

• Германия - Центр радиомониторинга федеральных вооруженных сил (AFMBw)

• Китай - Третий департамент НОК и 11 бюро МГБ КНР

А также:

• Европейский проект электроного шпионажа Enfopol

Между тем, уже несколько лет в мире действует никому не подконтрольная организация, которая в состоянии соперничать с самыми успешными спецслужбами мира именно в области радиоперехвата. Члены этой организации действуют по всему миру, прослушивая эфир в поисках шпионских сигналов.

Так работают самые обыкновенные и добропорядочные жители США, Франции, Германии, Голландии и т.п., по совместительству радиолюбители и члены клуба WUN (Worldwide UTE News). UTE означает, что клуб интересуют радиостанции, работающие в частотном диапазоне до 30 Мгц. Официально клуб был создан в январе 1995 года. 11 человек из США, Европы, Японии, Новой Зеландии и т.д. составляют штаб WUN. Простых членов клуба насчитывается уже много больше сотни. На сегодняшний день почти не осталось мест на планете, которые не попали бы в поле зрения членов клуба. Подробнее.

Самые известные российские наземные станции радиоперехвата находятся на Кубе (Российский электронный центр в Лурдесе) и Въетнаме (база Кам Ранк Бэй), другие расположены на территории России и стран СНГ. Против Соединенных Штатов работал кубинский центр, который управлялся совместно ГРУ, ФАПСИ и Кубинской службой разведки. На комплексе работало около тысячи русских сотрудников, которые отслеживают коммерческую и правительственную информацию, циркулирующую в сетях связи на территории США, а также между США и Европой. Считается, что база Лурдес способна контролировать все военные и гражданские спутники США. По утверждению американского Интернет-ресурса FAS, в качестве станций перехвата наши спецслужбы используют территории российских посольств и консульств. По их мнению, в былые времена для радиоразведки использовались даже самолеты Аэрофлота, летавшие в Штаты. Кроме того, есть еще корабли Шестого управления ГРУ, самолеты, которые постоянно находятся в воздухе… Кроме того, мы обладаем значительным флотом разведывательных спутников. Серийным спутником радиоэлектронной разведки является "Целина-2", радиоразведки - "Космосы" различных модификаций. По сведениям американцев, как минимум с 1994 года ровно половина ежегодно запускаемых Россией спутников - военного назначения. Кроме того, в нужный момент мы вполне в состоянии "повесить" несколько спутников над интересующей разведку территорией.

**Спецслужбы РФ, обеспечивающие защиту от технических средств разведки:**

• Федеральное агентство правительственной связи и информации

• Гостехкомиссия

**Системы глобальной радиоразведки :**

• Эшелон

• СОУД