**Федеральное агентство по образованию РФ**

Брянский государственный технический университет

 **Брянский государственный технический университет**

Кафедра: Электронные, радиоэлектронные и электротехнические системы.

Реферат

по дисциплине «Системы и средства технического обеспечения обработки, хранения и передачи информации»

 на тему:

«Методы и средства радиоэлектронной разведки»

 Руководитель: Дракин А. Ю.

Выполнил: студент гр. 10-ОЗИ Хандожко Г. С.

Брянск 2012

Содержание.

1). Введение………………………………………………………………………………………………..…….3

2). Классификация РЭР……………………………………………………………………………..……… 4

3). Радиоэлектронные каналы утечки информации……………………………………..…6

4). Радиоэлектронная разведка - ее структура, особенности и возможности..7

5). Технические средства радиоэлектронной разведки…………………………………10

6). Система РЭР «Onyx»…………………………………………………………………………………….13

7). Система РЭР «Эшелон»…………………………………………………………………………..…..14

8). Система РЭР «СОУД»……………………………………………………………………………………16

9). Радиолокационные станции дивизионной артиллерии……………………………17

10). Список литературы…………………………………………………………………………………….18

**Введение.**

Радиоэлектронная разведка (РЭР) – это обширная и многогранная область разведки, которая добывает информацию о противнике с помощью специальных радиоэлектронных средств.

Радиоэлектронная разведка является важнейшей частью государственной и военной разведки различных стран.

По мнению зарубежных специалистов, РЭР представляет собой основной и во многих случаях единственный способ добывания разведывательной информации.

Глобальный вопрос возникновения техногенной катастрофы подводит современное общество к своей защите, путем создания комплексной системы безопасности в собственных странах. Лидирующее положение в создании системы безопасности принадлежит Израилю, обладающему самой мощной современной системой безопасности в мире и тратящему на ее совершенствование и развитие до 30 % своего бюджета.

Современная РЭР отличается большим разнообразием используемых технических средств и способов их применения. Применяются пассивные (неизлучающие) и активные средства РЭР. В первом случае информация добывается путем обзора пространства в целях обнаружения источников радиоизлучения и приема их сигналов своими приемными (пассивными) устройствами; во втором случае – путем облучения пространства своими активными источниками радиоизлучения и приема своих же сигналов, отраженных от объектов разведки.

В зарубежной печати радиоэлектронную разведку определяют как “электронные глаза и уши” государства и вооруженных сил, действующие в мирное и военное время независимо от времени суток метеорологических условий. Отмечается также, что радиоэлектронная разведка, кроме того, является основой радиоэлектронной борьбы в период военных действий. Только пользуясь данными радиоэлектронной разведки, можно применить радиопротиводействие для подавления работы радиоэлектронных средств управления оружием и войсками противоборствующей стороны.

**Классификация РЭР.**

Радиоэлектронная разведка классифицируется по нескольким признакам:

- по целевому назначению;

- по месту базирования (по местонахождению) средств разведки;

- по характеру добываемой информации;

- по используемым принципам и средствам разведки.

Техническую основу радиоэлектронной разведки составляют:

- пассивные устройства поиска, перехвата и анализа сигналов и пеленгования источников электромагнитных излучений;

- активные радиолокационные и лазерные средства наблюдения, обнаружения и распознавания;

- оптико-электронные приборы;

- средства регистрации (индикации) и передачи добываемой информации;

- аппаратура обработки поступающей разведывательной информации, в том числе ЭВМ различных типов и классов.

Важной особенностью современной РЭР спецслужб является её глобальный характер. Это означает, что она ведется повсеместно, в том числе в воздухе и в космосе, охватывая все регионы планеты. Существенной чертой разведки является её тотальный характер. Это выражается в том, что сферой деятельности разведки становится политическая, экономическая, военная, идеологическая и другая деятельность государств. Более того, к получению разведывательной информации помимо специальных служб привлекаются различные правительственные, военные и дипломатические ведомства, а так же некоторые гражданские министерства.

Рассмотрим следующие основные виды РЭР:

радиоразведка,

радиотехническая,

радиолокационная,

лазерная,

инфракрасная,

телевизионная,

фоторазведка.

*Радиоразведка* – это один из наиболее распространенных видов пассивной РЭР. Она ведется с использованием сигналов радиосвязи (телефонной телеграфной и др.). Основная задача радиоразведки – добывание сведений путем обнаружения, перехвата открытых, кодированных передач радиостанций, пеленгование источников радиосигналов и определения их местонахождения, обработки и анализа перехваченной информации в целях вскрытия ее содержания.

*Радиотехническая разведка* – относится к пассивному виду РЭР, предназначается для обнаружения и распознавания сигналов РЛС, телеметрических и телекомандных систем.

*Радиолокационная разведка* – основной активный вид РЭР. Она предназначается для добывания информации с помощью специальных радиолокационных станций. Излучаемые ими сигналы отражаются (переизлучаются) от разведываемых объектов и поступают обратно в приемное устройство РЛС.

*Лазерная разведка* – добывает информацию с помощью лазерных локаторов. Лазерные локационные системы используют оптические сигналы и работают в режиме импульсного зондирования. Они в определенных условиях позволяют обнаруживать и подслушивать на расстоянии переговоры, ведущиеся в помещениях.

*Инфракрасная разведка* – особый вид РЭР добывает сведения об объектах по их инфракрасному излучению с помощью ИК приборов. В зависимости от используемой аппаратуры она может носить активный и пассивный характер. Разновидностью ИК разведки является радиотепловая разведка, добывающая сведения по радиотепловому излучению.

*Телевизионная разведка* – пассивный вид РЭР, предназначается для получения сведений с помощью телевизионной разведывательной аппаратуры. Может действовать как самостоятельно, так и во взаимодействии с аппаратурой ИК разведки и фоторазведки.

*Фоторазведка* – основной компонент наземной, воздушной и космической разведки.

Научно технический прогресс в области радиоэлектроники, микроэлектроники, ЭВТ, оптоэлектроники и телекоммуникаций позволяет использовать новейшие достижения для добывания информации через различные физические среды.

**Радиоэлектронные каналы утечки информации.**

В радиоэлектронном канале передача носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц.

***1. Радиоэлектронный канал*** относится к наиболее информативным каналам утечки в силу следующих его особенностей:

* независимость функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;
* высокая достоверность добываемой информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев дезинформации);
* большой объем добываемой информации;
* оперативность получения информации вплоть до реального масштаба времени;
* скрытность перехвата сигналов и радиотеплового наблюдения.

В радиоэлектронном канале производится перехват радио и электрических сигналов, радиолокационное и радиотепловое наблюдение. Следовательно, в рамках этого канала утечки добывается семантическая информация, видовые и сигнальные демаскирующие признаки. Радиоэлектронные каналы утечки информации используют радио, радиотехническая, радиолокационная и радиотепловая разведка.

***2. Структура радиоэлектронного канала утечки информации*** в общем случае включает (см. рис. 1) источник сигнала или передатчик, среду распространения электрического тока или электромагнитной волны и приемник сигнала.

 

 Рис. 1. Структура радиоэлектронного канала утечки информации.

В радиоэлектронных каналах утечки информации источники сигналов могут быть четырех видов:

- передатчики функциональных каналов связи;

- источники опасных сигналов;

- объекты, отражающие электромагнитные волны в радиодиапазоне;

- объекты, излучающие собственные (тепловые) радиоволны.

Средой распространения радиоэлектронного канала утечки информации являются атмосфера, безвоздушное пространство и направляющие - электрические провода различных типов и волноводы. Носитель в виде электрического тока распространяется по проводам, а электромагнитное поле - в атмосфере, в безвоздушном пространстве или по направляющим - волноводам. В приемнике производится выделение (селекция) носителя с интересующей получателя информацией по частоте, усиление выделенного слабого сигнала и съем с него информации - демодуляция.

При перехвате сигналов функциональных каналов связи передатчики этих каналов являются одновременно источниками радиоэлектронных каналов утечки информации. В общем случае направления распространения электромагнитной волны от передатчика к санкционированному получателю и злоумышленнику отличаются. В функциональных каналах связи максимум излучения энергии электромагнитной волны ориентируют в направлении расположения приемника санкционированного получателя. Поэтому мощность источника сигналов радиоэлектронного канала утечки информации, как правило, существенно меньше мощности излучения в функциональном канале связи.

**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 радиоэлектронная 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.), составляющие их "электронный почерк".

Типы радиоэлектронных систем: радиосвязи, радиолокации, радионавигации, наведения ракет и дальнего обнаружения, различные телеметрические системы 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 мыса Канаверал наблюдалось заметное увеличения числа источников электромагнитных излучений 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, используемыми 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 особенно нужна для создания эффективных технических средств и методов радиопротиводействия и контр противодействия.

Для получения такой информации средствами 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;

устройства панорамного обзора;

анализаторы спектра принимаемых сигналов,;

устройства для автоматического отсчета сдвигов пеленга и частоты;

выходные устройства для приема сигналов телефонных и телеграфных уплотненных каналов радиосвязи;

оконечные устройства слухового приема (телефоны, динамики);

устройства документирования сигналов;

приборы расшифровки, обработки и хранения принятой информации;

средства управления, связи и передачи добываемой информации.

Перехват информации после 2000 года.

 С середины 90-х годов разведывательные агентства 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 системам типа Иридиума.

 В последние 15 лет значительное технологическое преимущество, в свое время имеющиеся у агентств 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 агентства, 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.

Шпионская радиостанция времен Второй мировой (из книги Ultimate Spy Book)

 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 работает кубинский центр, который управляется совместно ГРУ, ФАПСИ и Кубинской службой разведки. На комплексе работают 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.

**Система РЭР «Onyx».**

Onyx — система радиоэлектронной разведки, оператором которой является Федеральная разведывательная служба Швейцарии. Аналог систем Эшелон и Frenchelon, но имеет гораздо меньшие масштабы. Ввод системы в эксплуатацию начат в 2000 году, первоначально под названием SATOS-3 (системы SATOS-1 и SATOS-2, предназначенные, в частности, для перехвата факсовых сообщений, вступили в строй в 1992 году), и был завершён в конце 2005 года.

Задачей системы является мониторинг как гражданских, так и военных коммуникаций, включая телефонные переговоры, передачу факсовых и Интернет-сообщений с помощью спутников. Onyx использует списки ключевых слов для фильтрации контента передаваемых сообщений, в целях перехвата информации, представляющей интерес. Выбор ключевых слов для фильтрации должен быть одобрен независимой комиссией. Система не должна контролировать внутренние коммуникации, при этом допускается мониторинг сообщений, которыми швейцарские абоненты обмениваются с иностранными. Правительство Швейцарии указало, что Onyx не связана с иностранными системами радиоэлектронной разведки, такими как Эшелон; согласно заявлению правительства, путаница в этом вопросе возникла из-за продажи в 2000 году швейцарской компанией Swisscom компании Verestar (в настоящее время SES Americom) наземной спутниковой станции в Лёке (кантон Вале), расположенной рядом с одной из станций Onyx.

Использование системы Onyx контролируется независимым органом управления, который состоит из представителей, назначенных правительством страны.

8 января 2006 года швейцарская газета Sonntagsblick опубликовала секретный доклад швейцарского правительства, который использовал данные, перехваченые Onyx. В докладе сообщалось о факсе министерства иностранных дел Египта, направленном в египетское посольстве в Лондоне, в котором шла речь существовании секретных тюрем ЦРУ в Восточной Европе. Швейцарское правительство официально не подтвердило существование доклада, но начало судебное преследование в отношении газеты по факту утечки секретных документов. Хотя подлинность факса была подтверждена в ходе судебного разбирательства лишь косвенно, с репортера и газеты были сняты все обвинения 17 апреля 2007 года.

**Система РЭР «Эшелон».**

«Эшелон» — общепринятое название глобальной системы радиоэлектронной разведки, работающей в рамках соглашения о радиотехнической и разведывательной безопасности Великобритания — США.

Система упоминалась в большом количестве открытых источников. В своем докладе, опубликованном в 2001 году, Европейский Парламент упоминает, что название «Эшелон» используется в разных контекстах, но имеется ряд свидетельств указывающих на то, что это название системы радиоэлектронной разведки. В докладе заключается, что на основе представленной информации «Эшелон» имеет возможность перехвата и анализа телефонных переговоров, факсов, электронных писем и других информационных потоков по всему миру путём подключения к каналам связи, таким как спутниковая связь, телефонная сеть общего пользования, СВЧ-соединения.

Электронная разведывательная система "Эшелон" - это более ста спутников-шпионов, наземные станции слежения и подслушивания, большое количество суперсовременных и мощных компьютеров (по некоторым данным, сегодня в АНБ работают до 10 только сверхмощных компьютеров "Крей" стоимостью в десятки миллионов долларов каждый).

 В упрощенном виде "Эшелон" работает примерно следующим образом. Источниками информации служат Интернет, электронная почта, телефон, факс, телекс. Сообщения, переданные этими путями, сканируются сверхмощными компьютерами, так называемыми "словарями "Эшелона", по ключевым словам, выражениям, тембру голоса (например, из 100 миллионов перехваченных сообщений отбирается 10 тысяч). Эти ключевые слова и выражения постоянно обновляются. Принцип похож на тот, который используют интернетовские поисковые системы, но в отличие от них "Эшелон" работает в реальном времени и уже в процессе, скажем, телефонного разговора решает: интересно ему это сообщение или нет.

 "Эшелон" владеет множеством языков, знаком с профессиональным сленгом (например, торговцев наркотиками или оружием) и специальной лексикой, знает клички или прозвища крупных политических деятелей ведущих стран мира. К тому же, как считают эксперты, АНБ научилось получать "отпечаток голоса", который, по их мнению, так же уникален, как и отпечаток пальца. По имеющемуся в памяти компьютера образцу голоса можно быстро идентифицировать любой голос в потоке звуков. Другими словами, если "Эшелон" однажды зарегистрировал голос какого-то человека, то потом может отследить его разговор с любого телефонного аппарата в мире. Что же касается Интернета, то, по мнению экспертов, АНБ получило от "Майкрософт", "Нетскэйп" и других фирм - производителей компьютерных программ ключи или так называемые "закладки", позволяющие заинтересованным лицам идентифицировать все, даже анонимные, сообщения. При этом "Эшелон" способен отслеживать практически весь информационный поток (трафик) в мире.

 На втором этапе сообщения, отобранные сканирующими компьютерами со всего мира, попадают в блок накопления информации. Там они записываются, сортируются по темам (например, "военные дела", ракетные или ядерные технологии, терроризм, политики, оружие, наркотики, контрабанда и так далее) и направляются на дальнейший анализ.

 Потом специально разработанные для каждой темы программы анализируют полученную информацию по заданным темам. Из, скажем, отобранных на первом этапе 10 тысяч сообщений остается только 100-200 действительно важных.

 Четвертым этапом, после которого материалы, как правило, попадают на стол крупных чинов в администрации США, становится уже экспертная оценка сотрудников профильных отделов АНБ в штаб-квартире спецслужбы в Форт-Миде по каждому из полученных 100-200 сообщений. Сомнительные случаи остаются в памяти компьютеров АНБ, а поскольку эта память практически бесконечна, то все больше людей (а следовательно, и правительственных структур, фирм, компаний, концернов и так далее) в мире попадают в поле зрения "Эшелона".

 Эксперты утверждают, что система способна проанализировать и запомнить до 3 миллиардов сообщений в день. По их мнению, в службах АНБ, занятых в "Эшелоне", работают до 30 тысяч сотрудников по всему миру - математики, программисты, лингвисты, криптологи. Иногда большинство из них и не подозревает, чем они занимаются. Так было, например, как сообщали британские СМИ, с группой из порядка 40 сотрудников компании British Telecom. Как выяснилось, эти люди не имели никакого отношения к АНБ или британской радиоэлектронной разведке, но тем не менее ими перехватывалось все - от посольской почты и деловых сообщений до личных поздравлений с днем рождения.

**Система РЭР «СОУД».**

СОУД (система объединенного учёта данных о противнике) — засекреченная система перехвата информации, созданная СССР и странами Варшавского договора для ведения глобальной радиоэлектронной разведки.

Договор о создании СОУД странами Варшавского договора был подписан в 1977, сооружали её в преддверии московской Олимпиады 1980 для того, чтобы не допустить возможных террористических актов против спортсменов и гостей-иностранцев. Полностью вступила в строй СОУД уже в 1979.Контроль за ней осуществляли 16-е Управление КГБ и 6-е Управление ГРУ.

СОУД объединяла все средства радиоэлектронной и космической разведки СССР, Болгарии, Венгрии, Польши, Чехословакии, ГДР, Вьетнама, Монголии и Кубы. Собранная информация направлялась для анализа и обработки в два главных компьютерных центра. Первый находился (и находится по сей день) в Москве, а второй располагался в ГДР. Но после объединения Германии в 1990 году компьютерный центр, принадлежавший Штази, достался западногерманской разведке БНД, из-за чего СОУД лишилась половины своих возможностей в обработке данных.

В 1990-х оставшуюся часть СОУД реорганизовали в новую российскую разведывательную систему, объединявшую поначалу все комплексы радиоэлектронной разведки на территории России и некоторых стран СНГ, Российский радиоэлектронный центр в Лурдесе (Куба), базу радиоперехвата в районе аэродрома Камрань (Вьетнам) и специальную радиоаппаратуру в консульствах и посольствах России по всему миру.

**Радиолокационные станции дивизионной артиллерии.**

Радиолокационные станции дивизионной артиллерии предназначены в основном для определения координат огневых позиций минометов и артиллерийских батарей противника и корректировки огня своей артиллерии и могут использоваться для обнаружения других наземных целей.

Станция А1М/МРО. Привозимая, используется в дивизионной артиллерии в интересах артиллерийской инструментальной разведки. Станция размещается на двух одноосных прицепах.

Работает на волне длиной около 2 см, обнаруживает цели на дальностях от 170 до 10 000 м и обеспечивает точность определения дальности ±10 м и направления ± (0,05-0,08)°. Время развертывания станции из походного в боевое положение 15—30 минут.

Засечка огневых позиций стреляющей артиллерии может быть произведена по одному выстрелу. С момента первой засечки летящего артиллерийского снаряда (мины) до открытия огня своей артиллерии или минометов требуется 4—5 минут.

Боевая работа станции включает три этапа: засечку мины (снаряда) на траектории полета, определение координат в точках засечки и вычисление координат огневой позиции артиллерии противника или места разрыва снарядов (мин) своей артиллерии. Принцип работы станции основан на последовательной засечке летящей мины (снаряда) в двух точках траектории с помощью двухлучевой диаграммы направленности антенны, совершающей сканирование по азимуту. В момент пересечения лучей миной (снарядом) на экране индикатора на электронно-лучевой трубке появляются две смещенные относительно друг друга отметки. Оператор накладывает на каждую отметку визирные линии азимута и дальности и нажатием кнопок вводит координаты двух точек засечки в аналоговое счетно-решающее устройство. Это устройство на основании введенных данных и времени между появлением отметок на экране индикатора вычисляет координаты огневой позиции, а при корректировке огня — координаты точки разрыва.

**Список литературы.**

1). Радзиевский В.Г., Сирота А.А. Теоретические основы радиоэлектронной разведки. Издательство: Радиотехника. 2004год - 432стр.;

2). В.А.Вартанесян. Радиоэлектронная разведка. Издательство: Воениздат. 1975год – 255стр.;

2). http://ru.wikipedia.org/wiki/Эшелон\_(секретная\_служба);

3). http://ru.wikipedia.org/wiki/Onyx\_(радиоэлектронная\_разведка);

3). http://tehn-s.ru/?p=419;

4). http://northropgrummna.com/category/radioelektronnaya-texnika;