Основы радиоэлектронной борьбы

В современном бою одним из решающих факторов победы над противником является устойчивое и непрерывное управление войсками, достигаемое в том числе использованием радиоэлектронных средств и строящихся систем на современных информационных технологиях. Широкое применение РЭС привело к резкому росту эффективности боевых средств и повышению качества управления войсками. В армиях ведущих государств радиоэлектронные средства не только используются в системах управления войсками, но и являются составными частями новейших систем вооружения и военной техники.

Сегодня насыщение поля сражения информационными системами определяет исключительно важную роль радиоэлектронной борьбы (РЭБ) в современных и будущих войнах. Опыт военных учений последнего времени показал, что даже если одна из противоборствующих сторон преобладает наличием качественного высокоточного оружия, оно не может гарантированно рассчитывать на победу, если его система управления будет обнаружена и подавлена средствами РЭС.

Военные эксперты уверены: в современных войнах радиоэлектронная борьба – ключевой элемент. Чтобы побеждать необходимо обязательно иметь не только современные средства огневого поражения, но и современные средства. РЭБ.

– операция многонациональных сил (БНС) во главе с США в Ираке «Буря в пустыне», начавшаяся 17 января 1991 года, где РЭБ отыграла ключевую роль.

Еще до начала массированного ракетно-авиационного удара БНС в районе конфликта сосредоточили 60 наземных станций и 37 вертолетов РЭС, способных проводить разведку и радиоэлектронное подавление на дальности до 150 км.

За сутки до начала операции наземные системы РЭБ начали мощное угнетение препятствиями иракских каналов связи. Сама операция началась с нейтрализации вертолетами РЭБ двух иракских станций ПВО раннего предупреждения. Они сумели пробить в иракской ПВО коридор пролета, в который сразу ввели самолеты БНС. ПВО Ирака стало их первой целью. Для ее подавления использовались самолеты F-4G с высоко точными противорадарными ракетами HARM, самолеты радиоэлектронного подавления EF-111. Они ставили препятствия, обманывали головки самонаведения ракет, подавляли радиосвязь. Уже через 9 суток 80% всех РЛС были выведены из строя, и ПВО Ирака перестало представлять угрозу.

В Ираке США впервые провели эксперимент по подавлению информационного потенциала противника: теле- и радиостанций, ретрансляторов, редакций электронных и печатных СМИ, которые использовались для освещения войны. Информационно-пропагандистская машина Ирака была подавлена радиоэлектронными средствами борьбы США.

Военно-политическим руководством РФ также уделяется значительное внимание развитию и совершенствованию как технических средств РЭС, так

и тактики применения частей и подразделений войск РЭС.

В 2009 году части и подразделения радиоэлектронной борьбы были превращены в войска РЭБ вооруженных сил РФ, включающие соединения, части и подразделения РЭБ в составе оперативно-стратегических командований и развернутые в составе 1, 2 корпусов, сформированных на востоке Украины.

Сейчас очень быстро происходит дальнейшее совершенствование технических средств и методов РЭБ вооруженными силами стран НАТО и РФ. В ходе войны на востоке Украины хорошо отработаны методики одновременной или поэтапной нанесения ударов по противнику огневыми средствами в тесном взаимодействии со средствами РЭБ, стратегической и тактической маскировки, дезинформации и психологической войны.

Радиоэлектронная борьба как вид боевого довольствия. Составные части РЭБ

В современных условиях, когда радиоэлектронные системы и средства используются во всех родах и видах ВС Украины, от надежности их работы в значительной степени зависит качество управления войсками, эффективность боевого использования оружия и боевой техники.

Под РЭЗ понимают устройства, работа которых основана на излучении и приеме электромагнитной энергии (рис. 3.1).

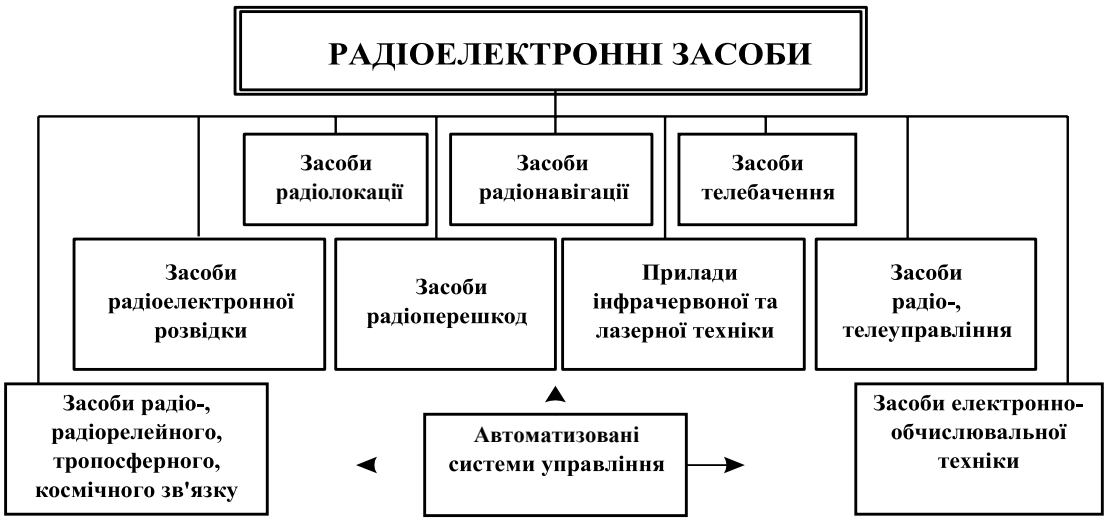

Рис. 1. **Классификация радиоэлектронных средств**

Активные радиоэлектронные средства различных систем и видов оружия передают информацию, излучая электромагнитную энергию, которая может быть обнаружена и перехвачена радиоприемными устройствами соответствующего диапазона волн.

Кроме того, работа РЭС может быть нарушена умышленными радиопомехами, которые могут привести к потере управления войсками и оружием.

Сущность РЭБ состоит в дезорганизации систем управления войсками и оружием противника, а также временном или постоянном снижении эффективности применения средств разведки, оружия, боевой техники

противника путем радиоэлектронного или огневого подавления (уничтожения) его радиоэлектронного оборудования, систем управления, разведки, связи.

Таким образом, РЭБ может включать в себя как временную дезорганизацию работы радиоэлектронных систем противника путем постановки помех, так и полное уничтожение данных систем (огневое поражение или захват). Также РЭС включает меры по обеспечению устойчивой работы своих радиоэлектронных средств снижением возможностей противника по ведению радиоэлектронной разведки, радиоэлектронного подавления, поражения самонаводящимся на излучение оружием, а также защиты от взаимных помех.

Итак, **радиоэлектронная борьба** (Electronic Warfare) – это один из видов боевого обеспечения общевойскового боя, являющийся совокупностью взаимосвязанных по целям, задачам, месту и времени мер и действий войск, направленных на нарушение систем и средств управления войсками и оружием противника , а также направлен на радиоэлектронную защиту своих систем и средств управления войсками и оружием, противодействия техническим средствам разведки (ПТЗР) противника.

Радиоэлектронная борьба ведется в тесном сочетании с огневым поражением и уничтожением основных радиоэлектронных средств управления подразделениями и оружием противника, мероприятиями по разведке, маскировке и заключается в выполнении отдельных задач радиоэлектронного подавления и радиоэлектронной защиты.

При организации радиоэлектронной борьбы командир подразделения обычно указывает: какие ПУ и радиоэлектронные объекты противника и в какое время подлежат огневому поражению или захвату (выведению из строя), силы и средства, которые для этого привлекаются; порядок применения средств радиоэлектронное подавление; задачи по радиоэлектронной защите; сроки готовности Для выполнения определенных тактических задач механизированному батальону могут из состава рот радиоэлектронной борьбы бригад передаваться в подчинение сводные подразделения радиоэлектронной борьбы или отдельные радиостанции радиопомех КХ, УКВ. радиосвязи.

Для прикрытия батальона (роты) от поражения артиллерийскими боеприпасами с радиовзрывателями они могут прикрываться подразделениями помех радиовзрывателям. К основным объектам прикрытия относятся КСП батальона (роты), артиллерийские подразделения.

Радиоэлектронная защита подразделений батальона (роты) от поражения радиоуправляемыми взрывными устройствами обеспечивается путем включения в них колонны техники подразделений РЭБ, которые оснащены малогабаритными передатчиками помех (МЧП), или оснащение вооружения и военной техники батальона (роты) передатчиками помех.

Основными задачами РЭБ в боевых действиях являются:

- дезорганизация функционирования радиоэлектронных средств систем управления противника путем радиоэлектронного подавления наиболее важных линий радиосвязи и радиоэлектронных средств систем управления

авиации, ПВО, ракетных частей и артиллерии, разведочно-ударных и разведывательно -огневых комплексов, частей разведки и РЭБ, командных пунктов противника;

- радиоэлектронное прикрытие подразделений от воздушной радиолокационной разведки с целью снижения эффективности прицельных ударов с воздуха по пунктам управления, районам сосредоточения механизированных, танковых войск, частям ракетных войск и артиллерии, аэродромам ударной авиации и другим объектам;

- радиоэлектронное прикрытие подразделений от артиллерийских снарядов и мин противника с радиовзрывателями и радиоуправляемыми фугасами на маршрутах выдвижения подразделений для выполнения боевых задач;

- радиоэлектронная защита радиоэлектронных средств своих войск от радиоэлектронной разведки и радиоэлектронных помех противника, от их поражения самонаводящимся на излучение оружием и от взаимных помех.

Перспективными задачами РЭБ в боевых действиях являются:

- функциональное поражение (временное или полное выведение из строя) энергией мощного высокочастотного импульсного излучения основных управляющих радиоэлектронных элементов средств;

- влияние на локальные вычислительные сети автоматизированных систем управления войсками и оружием распространяемым боевым программным обеспечением (компьютерными вирусами и т.п.) радиоканалы.

Согласно целям и задачам, возлагаемым на РЭС, она включает:

- радиоэлектронное подавление (РЭП) радиоэлектронных (электронных) средств противника;

- радиоэлектронная защита (РЕЗах) своих систем и средств управления войсками и оружием.

Радиоэлектронное подавление (Electronic Attack) – влияние на радиоэлектронные средства систем управления войсками и оружием противника радиоэлектронными помехами, дезинформацией, отводом самонаводящихся и управляемых средств поражения от прикрываемых объектов и изменения условий распространения электромагнитных волн и радиолокационной контрастности местности.

В зависимости от решаемых задач РЭП включает:

- радиоподавление (ЭМ jamming);
- оптико-электронное подавление;
- электронное обеспечение РЭП (electronic warfare support).

Радиоподавление состоит в срыве или нарушении работы систем и средств управления войсками и оружием противника путем воздействия активных и пассивных радиопомех на линии радио-, радиорелейной , тропосферной и космической связи, а также на системы и радиолокационные и радионавигации.

Подавление РЭС, по мнению специалистов, может быть осуществлено:

- огневым или ядерным поражением радиоэлектронных средств;
- постановкой активных радиоэлектронных помех радиоэлектронным

средством;

- передачей ложной информации в своих сетях связи, рассчитанной на перехват радиоразведкой, и созданием ложной радиоэлектронной обстановки с целью введения в заблуждение (дезинформации) противника;

- вхождение в сети связи (передачи данных) противника с целью навязывания ложной информации, а также захвата (вывода из строя) радиоэлектронных объектов.

Подавление активными радиоэлектронными помехами основано на свойствах радиоприемных устройств принимать не только полезные сигналы, но и электромагнитные излучения одинаковой с ними частоты. В результате этого на выходе приемного устройства происходит выделение как полезного сигнала, так и других совпадающих с ними сигналов по частоте (помех). В зависимости от энергетических соотношений полезных сигналов и помех, их взаимодействия в конечных устройствах прием полезной информации становится невозможным или происходит ее извращение, задержка и уменьшение объема.

Мощные излучения (помехи) характеризуются тем, что они полностью исключают возможность использования РЭС для приема необходимой информации.

Оптико-электронное подавление состоит в срыве или нарушении работы инфракрасных, телевизионных, лазерных, оптико-визуальных систем и средств разведки, наблюдения, связи и управления оружием противника путем воздействия активных и пассивных оптикоэлектронных помех на оптические и фоточувствительные элементы.

В механизированном подразделении для оптико-электронного подавления средств разведки и управления оружием противника могут применяться штатные средства: комплексы оптико- электронного подавления, термодымовая аппаратура, системы пуска дымовых гранат, инфракрасные прожекторы, дымовые шашки и гранаты, а также дымообразующие устройства и др. материалов.

Для введения в заблуждение систем наблюдения противника используются средства понижения заметности военной техники:

- «двойная крыша» над моторным отделением ВВТ;

- фальшборт из резинокорда над нагреваемыми элементами ходовой части;

- легкосмываемые пены с разными присадками, которые быстро наносятся;

- быстросъемные теплоизолирующие материалы и экраны. Радиоэлектронное подавление существенно дополняет огневое поражение. По сравнению с физическим уничтожением радиоэлектронных объектов противника радиоэлектронное подавление позволяет практически мгновенно влиять на радиоэлектронные объекты с меньшими затратами . При этом не нужно знать координаты объектов с большой точностью.

Радиоэлектронное подавление, как одна из составляющих РЭС, осуществляется специальными частями и подразделениями, самолетами и

кораблями РЭС. При этом для повышения эффективности РЭБ в технологически развитых государствах предполагается вести борьбу не с отдельными РЭС, а с системами управления войсками и оружием.

Особое внимание уделяется организации и ведению РЭБ в воздушно-наземных операциях с поражением противника на всю глубину оперативного построения его войск при комплексном применении ядерного, химического, бактериологического, высокоточного оружия и средств РЭП Сухопутных войск.

Способы применения РЭП:

1. Сосредоточенно-массированный – может использоваться главным образом в наступательных операциях и при наличии достаточных сил и средств РЭП. Этот способ предполагает одновременное подавление на определенное время наиболее опасных систем и средств радио-, радиорелейной связи и радионавигации на выбранном направлении или направлении главного удара войск во всю глубину оперативного действия, в тыловых районов объединений.

2. Выборочный применяется по всей полосе или по отдельным направлениям боевых действий. При этом способе осуществляется последовательное РЭП после тщательной разведки РЭС. Этот способ считается наиболее эффективным в обороне, а также в случаях, когда неизвестные направления сосредоточения главных усилий войск противника или количество сил и средств РЭП ограничено. В обороне (с началом проведения огневой подготовки наступающих войск) подавляются средства радиосвязи, радиолокации систем управления ракетных частей, артиллерии и авиации, после чего последовательно подавляются РЕЗ противника, переходящего в атаку. При этом способе наибольшее использование находят станции прицельных радиопомех.

3. Сосредоточенно-выборочный – это сочетание первых двух. При его реализации часть сил и средств РЭП используется массированно на главном направлении, а вторая часть – для выборочного подавления РЭС . Считается, что этот способ наиболее эффективен в условиях, когда неизвестно направление действия главной группировки, а местность, состояние путей и время не позволяют перегруппировать и объединить силы и средства РЭП на главном направлении. При этом способе все силы и средства РЭП используются в комплексе и совместно с действиями по поражению и захвату РЭЗ разведывательно-диверсионными. подразделениями.

Для подавления радиосредств, по подсчетам специалистов, необходимо на площади 1 км ^{2} примерно 200 передатчиков помех с мощностью 1Вт или 25-50 передатчиков с мощностью 5 Вт, или 1 тактическая ракета, которая может перенести передатчик препятствий одноразового использования с возможностью подавить работу РЭС на площади 10-15 ^{км2} .

Радиоэлектронное подавление в тактическом подразделении, ввиду наличия средств РЭБ, производится, в основном, с целью нарушения работы инфракрасных и лазерных средств разведки и управления оружием, подавление

радиолиний управления радиоуправляемыми взрывными устройствами противника путем применения устанавливаемых штатных и добавленных средств активных и пассивных помех. на вооружении и военной технике и прикрывающихся от поражения объектах.

Радиостанции тактического подразделения, не задействованные в управлении, могут использоваться для передачи в ложных радиосетях и радиосетях противника дезинформирующих команд, сигналов, а также создания радиопомех.

Радиоэлектронная защита организуется и осуществляется для защиты своих радиоэлектронных средств от радиоэлектронной разведки, огневого и радиоэлектронного воздействия противника, от взаимных помех.

То есть, **радиоэлектронная защита** – это комплекс мер, направленных на обеспечение эффективного и устойчивого функционирования своих (союзников) радиоэлектронных систем (средств) в условиях ведения РЭБ противником. Эти меры охватывают прежде всего все виды маскировки излучений радиоэлектронных средств от радиоразведки противника, защиту от радиопомех и защиту от поражения самонаводящимся оружием противника.

Радиоэлектронная защита своих (союзников) радиоэлектронных систем и средств **включает :**

- защита от радиоэлектронной разведки противника;
- защита радиоэлектронных средств от поражения самонаводящейся на излучение оружием;
- защиту от радиоэлектронных помех противника и атмосферных помех;
- защита от ионизирующего и электромагнитного излучение;
- защита от электромагнитного (направленного) и других видов оружия на «новых» физических принципах;
- защита от взаимных помех в пунктах управления и в боевых порядках войск (от средств радиоэлектронной атаки против РЭС противника и обеспечения электромагнитной совместимости своих и союзников РЕЗ).

Обеспечение РЭЗ достигается комплексом организационных и технических мероприятий. Рассмотрим составляющие.

Организационные мероприятия заключаются в выборе целесообразных способов боевого применения и размещения радиоэлектронных объектов и средств на местности в группировках войск, регламентировании работы радиоэлектронных средств по территории, частотам, режимам и времени, а также в выявлении источников непреднамеренных (взаимных или т.н. дружественных)) препятствий и принятия мер по исключению (уничтожению при необходимости) их воздействию.

Технические мероприятия состоят в применении специальных устройств, схем защиты и режимов работы радиоэлектронных средств.

Защита от радиоэлектронной разведки противника обеспечивается: проведением комплекса мер и действий, направленных на снижение ее возможностей извлечения информации о радиоэлектронных средствах войск по их электронному (акустическому) излучению . Он предполагает устранение

(ослабление) или предусмотренное воспроизведение демаскирующих признаков своих радиоэлектронных средств (объектов) путем введения противника в заблуждение (радио и акустические демонстративные действия или имитация действий, радиоэлектронная дезинформация).

Защита от поражения самонаводящимся на излучение оружием обеспечивается:

- комплексным применением радиоэлектронных средств разных диапазонов рабочих частот и принципов действия;
- применением специальных устройств защиты и режимов работы РЭС;
- сокращением времени излучения или периодического выключения РЕЗ;
- периодической сменой рабочих частот;
- эффективным выбором позиций и пространственным разнесением радиоэлектронных объектов (средств связи) на местности и их инженерным оборудованием;
- строгой регламентацией работы радиоэлектронных средств, их дублированием и резервированием;
- применением ложных целей и ловушек (применяемых для имитации целей на экранах РЛС, перегрузки приемных устройств разведывательных РЕЗ и отвертывания на себя наводимого на излучение оружия) – источников электромагнитного и акустического излучение;
- снижением эффективной отражающей площади (radar cross-section) военной техники – сухопутной, морской и воздушной, а также снарядов и ракет на траекториях полета.

Защита от радиоэлектронных помех противника обеспечивается:

- созданием разветвленной опорной сети связи;
- комплексным применением РЕЗ разных (более высоких) диапазонов частот;
- оптимальным распределением и использованием частот;
- сменой (по команде) рабочих частот;
- применением специальных (помехо- и разведзащищенных) режимов работы РЕЗ;
- организацией скрытых радиосетей и дублируемых радионаправлений , использованием обходных направлений (каналов) связи и ретрансляционных пунктов;
- созданием скрытых и резервных радиоэлектронных объектов;
- поиском и уничтожением передатчиков помех одноразовой действия;
- организацией взаимного оповещения и обмена информацией о препятствия;
- использованием специальных схем и устройств защиты РЕЗ от помех и других мер.

Воздействие ионизирующего и электромагнитного излучения на РЭС (в условиях применения ядерного оружия)

На качество связи оказывает существенное влияние изменение условий

распространения радиоволн при высотном ядерном взрыве. Искусственные ионизированные области, вызванные высотными ядерными взрывами, могут нарушить радиосвязь и работу РЭС на значительном удалении от места взрыва.

Короткие радиоволны (КВ) за счет последовательного многократного отражения от ионосферы распространяются на расстоянии в несколько тысяч километров. Так как каждое отражение сопровождается поглощением энергии волны, то КВ радиосвязь пространственными волнами под действием излучений ядерных взрывов может нарушаться в результате интенсивного поглощения и отражения волн ионизированными участками атмосферы на длительное время.

Так, после высотных ядерных взрывов, проведённых США над островом Джонстон в 1962 г., КВ радиосвязь между радиостанциями, расположенными на Гавайских островах и в Мельбурне, была нарушена на 7 час. Несколько часов не было приема сигналов точного времени в некоторых точках Японии от радиостанции на Гавайских островах.

Длительное нарушение КВ радиосвязи наблюдалось также между Австралией, Новой Зеландией и западным побережьем США. Под влиянием ядерных взрывов КВ радиосвязь между Токио и Калифорнией была прервана на 18 часов.

В ультракоротковолновом (УКВ) диапазоне повышенная ионизация не оказывает существенного влияния на работу РЭС, работающих наземной волной в пределах прямой видимости. Но энергия УКВ радиоволн отражается от ионосферы, что увеличивает взаимные помехи между РЕЗ на дальности до 1000 км.

Отражения от областей повышенной ионизации также создают помехи РЛС систем ПВО.

Ионизирующие излучения высотных ядерных взрывов могут значительно ухудшить характеристики и даже вывести из строя радиоэлектронную аппаратуру вследствие конфигурации физических и химических параметров её частей. Под действием радиоактивного излучения изменяются емкости конденсаторов, значения сопротивлений, параметры полупроводниковых приборов .

В процессе ядерных взрывов одновременно с ионизирующим излучением образуются кратковременные электромагнитные импульсы (ЭМИ). Распространяясь воздухом, грунтом, проводными линиями связи, линиями электропередач, ЭМИ приводят в них большие токи и высокие напряжения. Токи приводятся также в антенных устройствах и в элементах РЛС. Эти токи способны плавить провода, пробивать изоляцию, повреждать детали, а иногда и поражать обслуживающий персонал.

Защита от электромагнитного и других видов оружия на новых физических принципах

В современных условиях оружие на новых физических принципах или нетрадиционное оружие (НЗ), как правило, применяется в комплексе с

традиционными средствами поражения. Примерами могут быть нанесение авиационных ударов обычными авиабомбами, крылатыми ракетами, неуправляемыми реактивными снарядами, нанесение танковых ударов одновременно с применением электромагнитных бомб, боеприпасов, генераторов электромагнитного импульса. Другим примером может служить применение средств РЭБ в сочетании с оружием ЭМИ и средствами информационно-технического воздействия информационного оружия. То есть комбинации вариантов применения нетрадиционного и традиционного оружия могут быть самыми разными. Самостоятельно нетрадиционное оружие пока используется изредка, в основном для решения отдельных локальных задач.

Техническая реализация классов ЧП определяет выбор типа средств непосредственного поражения (генераторы ЭМИ, электромагнитные бомбы, химические фугасы, твердотельные или газовые лазеры, вихревые акустические генераторы, бомбы с обедненным ураном и многие другие).

Угроза применения ЧП уже теперь стала реальностью, поэтому актуальными задачами в настоящее время и на перспективу является создание средств защиты от нее и разработка способов их применения.

Средствами защиты от НЗ разных классов могут быть:

- лазерного оружия – постановщики активных и пассивных помех, ложные цели, аэрозольные завесы и образования, системы защиты оптики, глаз;
- химического и биологического оружия – средства обезвреживания микроорганизмов, химических соединений, комплексное обмундирование (например, военная форма нового поколения для армии США, в которой будут применяться особые нанотрубки, хорошо пропускающие воздух, но защищающие от действия химического и биологического оружия) для личного состава, средства снятия болевых синдромов;
- от информационного оружия – программы обнаружения вирусов, средства кодирования, резервирования, защиты от несанкционированного доступа к информации;
- от радиологического, пучкового, химического, биологического оружия – средства индикации и защиты от поражения ионизирующей радиацией, ядовитыми веществами, биологическими агентами разных типов, борьбы с шокоподобными состояниями вследствие инфекционного и лучевого заболеваний, ожогов, травм тому подобное.

Следует отметить, что те же средства могут использоваться и как оружие, и как средство защиты от него.

Защита от взаимных электромагнитных помех (электромагнитная совместимость своих РЭЗ)

Электромагнитная совместимость (Electromagnetic compatibility) – действия, направленные на обеспечение способности своей радиоэлектронной аппаратуры систем связи и управления оружием функционировать в определенных условиях без заметного ухудшения качества работы в результате непреднамеренного электромагнитного излучения.

К основным мерам радиоэлектронной защиты от взаимных помех можно

отнести применение направленных антенн, выбор выгодных (устойчивых) для данных условий частот, своевременный и четко установленный переход с одной частоты на другую (по сигналу или по времени) и маневр радиоданными, работу радиосредств на пониженных мощностях , расположение работающих радиосредств с учетом экранирующих свойств местности, места и мощности соседних радиостанций и других источников электромагнитных излучений

Одним из самых простых, но эффективных мер защиты своих радиоэлектронных средств от помех противника является *строгое соблюдение правил (требований) пользования средствами связи и ведения радиообмена* , максимальное сокращение времени выхода в эфир на передачу за счет лаконичной речи, использование в основном коротких сигналов и команд , а также дублированием каналов электросвязи и сигнальных средств

Эффективное решение задач каждой из составных частей РЭБ, решаемой командиром полевого подразделения, возможно только при своевременном обнаружении (разведке) радиоэлектронных систем и средств противника.

В интересах РЭБ силами и средствами армейской разведки добываются данные о принадлежности, назначении, местоположении (координате), режимах работы, основных характеристиках, составе систем и средств управления войсками (силами) и оружием, радиоэлектронной борьбе, технической разведке, пунктах управления и радиоэлектронных. объектов других систем противника

В целях уточнения полученных данных о радиоэлектронных системах и средствах противника, контроля за их работой, целеуказания и наведения на них станций помех проводится доразведка этих систем и средств частями РЭС и армейской разведки. Кроме того, полученные от них данные могут быть использованы для решения задач по огневому поражению РЕЗ противника.

Задачи радиоэлектронной борьбы в мирное время и во время боевых действий выполняются силами и средствами, организационно сведенными в специальные военные формирования – части и подразделения РЭБ, или штатными средствами РЭБ, находящимися на вооружении подразделений (индивидуальные и групповые средства постановки препятствий, установленные на самолетах, вертолетах, корабельные средства РЭБ, специальные устройства (приборы) радиоэлектронной защиты радиоэлектронных средств), а также соединениями, частями, подразделениями родов войск и специальных войск.

Основными мерами РЭБ в тактических действиях механизированных подразделений могут быть следующие:

- быстрое огневое поражение обнаруженных радиоэлектронных объектов (КП, СП, РЛС) противника);
- ограничение работы радиостанций на передачу в определенное время (при выдвижении, подготовке наступления тому подобное);
- продвижение для выхода к рубежу перехода в атаку с использованием укрытых от наблюдения со стороны противника участков местности, опушка

рощ, лощин, обратных склонов и т.п.;

- отстрел дымовых шашек и гранат в сторону радиотехнических средств разведки и наблюдения противника, в том числе применяющих атакующих вертолетов ПТУР;
- ведение боя под прикрытием дымовых завес перед передним краем и на флангах;
- маневр частотами при радиообмене и переход на применение сигнальных систем управление;
- применение маскировочных средств и укрытий.

Возможности армейских технических изысканий и средств РЭБ армий иностранных государств. Особенности применения РЭБ по опыту участия ВС Украины на востоке Украины

Прежде чем уничтожить радиоэлектронное средство противника, его нужно разведать, это задача *радиоэлектронной разведки* (РЭР), а именно: выявить в радиоэфире работу РЭС противника, перехватить его излучение, сделать анализ перехваченного излучения и определить местоположение излучателя и его тип.

Анализируя перехваченные сигналы, можно установить принадлежность излучателя к звену управления, виду, роду вооруженных сил и т.п. Таким образом, разведка радиоэлектронных средств является неотъемлемой и необходимой составной частью радиоэлектронного противостояния (Electronic Warfare) и может вестись в любое время суток и года, при любых метеоусловиях и любых условиях боевой обстановки.

Техника РЭР обеспечивает перехват всех видов радиопередач (радиоизлучений), в том числе линий (сетей) связи с *помехозащищенными* (скрытыми) режимами работы, с различными видами модуляций и манипуляции, а также обеспечивает определение амплитудных, временных, частотных и фазовых характеристик сигналов , в том числе и местоположения и принадлежность излучателя к ПУ или военной технике.

Одним из основных видов разведки является РЭР, которая разделяется по взглядам партнеров из НАТО на несколько видов:

1. Радиоразведка – Communication Intelligence (COMINT).
2. Радиотехническая разведка – Electromagnetic Intelligence (ELINT).
3. Радиолокационная разведка – Radar Intelligence (RADINT).
4. Телевизионная разведка – Television Intelligence (TELINT).
5. Разведка с использованием квантово-оптических приборов – Quantum Optical Intelligence (QOINT).
6. Разведка с использованием устройств инфракрасной техники – Infrared Sets Reconnaissance (ISR).

Больше информации о системе связи и управления военными можно получить благодаря радио- и радиотехнической разведке (РТР).

Радиоразведка собирает разведывательную информацию по излучению средств связи. Радиоразведка ведется с помощью радиоэлектронной аппаратуры, позволяющей:

- выявлять источники радиоизлучения, определять место их нахождения и распознавать средства связи, передачи данных, радиотелеметрии ;
- идентифицировать системы управления по характеру излучений их РЕЗ и радиообмена;
- определить характер деятельности войск по расположению, составу, перемещению средств радиосвязи, интенсивности и характеру радиообмена.

РЭР наиболее перспективна в вопросах получения разведывательной информации. Это объясняется тем, что:

- во-первых, радиоразведка имеет возможность вести разведку на любую глубину;
- во-вторых, эта разведка ведется скрыто, непрерывно и, главное, в масштабе реального времени.

Задания радиоразведки:

- наблюдение и контроль за радиоэфиром;
- прослушивание каналов связи противника;
- радиоперехват информации с последующим дешифрованием.

Радиоразведка нацелена на все виды радиосвязи. Она за короткое время даже без дешифрования перехваченной информации определяет интенсивность работы станций противника и плотность размещения в заданном районе, и на основании анализа этих данных может быть сделан вывод об группировке и цели противника.

Радиотехническая разведка – это вид радиоэлектронной разведки по выявлению и распознаванию РЛС, радионавигационных и радиорелекодовых систем. РТР использует способы радиоприема, пеленгирования и анализа радиосигналов.

Задания РТР:

- обнаружение любых источников электромагнитных излучений противника и измерение их параметров;
- определение местоположений РЭС и их ТТХ;
- определение типов и систем управления войсками радиотехническими средствами и оружием.

Средства РТР позволяют:

- определить несущую частоту радиопередатчиков;
- определить параметры, координаты источников излучение;
- измерять параметры импульсных сигналов;
- установить вид модуляции сигнала;
- измерять поляризацию радиоволн.

По результатам анализа полученных данных есть возможность определить систему ПВО противника, расположение его ПУ и других военных объектов.

РЭР делится на *стратегическую* и *тактическую* по ее назначению.

Стратегическая РЭР проводится правительственными органами высшего военного командования с целью получения всесторонней информации о стране через ее радиоэлектронные средства. Используя разведданные, разведорганы обнаруживают месторасположение военных

объектов, перемещение войск и т.п.

Тактическая РЭР считается одним из главных видов обеспечения войск информацией путем без прерывного слежения за электромагнитным излучением военных устройств и систем противника. Она применяется непосредственно при планировании и ведении боевых действий.

Объектами тактической РЭР являются:

- средства радиосвязи;
- РЛС воздушных и наземных целей;
- навигационное оборудование;
- системы наведения ракет и управления огнем артиллерии;
- инфракрасные лазерные и телевизионные приборы и системы;
- статические, звуковые и другие виды датчиков первичной информации.

За характером и частотой радиообмена, количеством радио- и радиотехнических средств возможно составить полное воображение о положение и деятельность противника Поэтому считается, что в ходе разведки главное – разоблачить организацию радиосетей противника вообще. Средства РЭР приводятся в действие еще к начала активной работы радио- и радиотехнических средств, т.е. момент приведение их в боевую готовность, засекая «паразитные» электромагнитное излучение работающих генераторов.

В качестве примера специалисты по радиоразведке утверждают, что расположение военных кораблей можно установить по их РЭС на расстоянии до 800 км.

Командование США считает (по открытым данным), что в полосе действий армейского корпуса РФ за 10 час. к началу операции они могут разоблачить до 82% основных сетей радиосвязи и подавить до половины КХ сетей радиосвязи, а также значительную часть радиорелейной связи.

С началом операции за 3-4 часа. силами и средствами радио и РТР может быть разоблачена система управления армейского корпуса РФ. А через 50-60 мин после начала работы РЭС противника на передачу, наземными средствами радиопомех подавляется работа радио, РРС и РЛС на глубину до 20-, 30 км средствами, расположенными на летательных аппаратах, – на глубину до 80-100 км.

Борьба с радиоэлектронными помехами и защита от радиоразведки противника

Защита РЭС от преднамеренных и непреднамеренных радиоэлектронных помех достигается использованием технических мер, обеспечивающих помехозащищенность, а также осуществлением организационных мер, повышающих помехоустойчивость систем управления.

Помехозащищенность – способность РЭС работать с соответствующим качеством, которое требуется от них при воздействии радиоэлектронных помех.

Помехоустойчивость – способность совокупности РЭЗ (развернутая система средств связи), системы управления войсками выполнять задачи в

условиях радиоэлектронных помех.

К техническим способам и средствам повышения помехозащищенности относят реализуемые в принципах построения РЭС и систем, в способах передачи, приема и формирования сигналов, а также в электронных схемах (алгоритмах) защиты от радиопомех. Их реализация основана на сравнении полезных сигналов РЭС и сигналов от радиопомех по частоте, ампулитуде, фазе, длительности, импульсной последовательности, направлению действия помехи, поляризации ЭМХ, а также случайным изменениям параметров радиосигналов.

Техническими средствами и способами борьбы с препятствиями есть:

- получение необходимого соотношения сигнал/помеха в приемном устройства;
- накопление сигналов в радиоприемном устройства;
- предотвращение перегрузки приемных устройств;
- селекция и фильтрация сигналов;
- помехоустойчивое кодирование;
- использование излучений средств препятствий;
- использование аппаратуры адаптации и адаптированных радиолиний в комплексе с модемы.

Повышение помехоустойчивости РЭС и систем управления достигается проведением организационно-технических мероприятий:

- противодействие техническим средствам разведки;
- оптимальное расположение РЕЗ на местности;
- распределение рабочих и запасных частот;
- комплексное использование РЕЗ при выполнении боевого Задание;
- подготовка экипажей для работы в условиях радиоэлектронных помех.

К основным мерам **радиоэлектронной защиты** РЕЗ тактического подразделения принадлежат:

– строгая регламентация работы радиосредств на излучение (по частоте, времени, месту);

– своевременное изменение рабочих частот;

– применение ложных источников электромагнитных излучений;

– использование штатных средств защиты от радиоэлектронного оружия.

радиотехнической разведке противника состоит в проведении мероприятий, направленных на исключение или существенное усложнение извлечения противником посредством технических средств разведки достоверных сведений о подразделениях, объектах и осуществляемых действиях войск.

К мерам противодействия техническим средствам разведки относятся:

- уничтожение средств радио- и радиотехнической разведки;
- радиоэлектронное подавление средств радиоразведки;
- защита от средств радиоразведки;

- соблюдение режима секретности в военных частях.

К мерам по защите от радиоразведки противника относится:

- укрытие (устранение или ослабление демассирующих признаков) объектов от средств радиоэлектронной разведки, оптической и радиолокационной разведки и акустической разведки противника;
- техническая дезинформация (обнародование ложных сведений об оружии, технике, личном составе, местонахождении ПУ тому подобное).
- специальная защита технических средств передачи информации.

Укрытие подразделений и боевой техники *мб* достигается устранением демаскирующих признаков объектов и проведенных мероприятий, применением инженерно-технических средств маскировки и имитации *военной* техники , использованием маскировочных свойств местности, выполнением правил скрытого управления войсками , созданием препятствий техническим средствам разведки, применением дымов. и аэрозолей, снижением уровня теплового излучения боевой техники, а также умелым использованием для перемещения условий ограниченной видимости (ночь, дождь, туман, снегопад), лесных массивов, обратных от противника склонов высот , оврагов и лощин, насыпей дамб, придорожных посадок деревьев и т.д.

К мерам технической дезинформации можно отнести передачу ложных сведений в радиосетях, имитацию работы пунктов управления (командно-штабных и командирских машин) в ложном месте (районе), применение кочующих ложных РЕЗ.

Специальная защита технических средств передачи информации в механизированных подразделениях организуется путем строгого соблюдения правил передачи сообщений по радио и выполнением следующих рекомендаций:

- работа излучающих средств с минимально необходимой мощностью или в режиме радиомолчание;
- сокращение времени работы средств связи на излучение;
- применение защищенных видов передачи (техническая маскировка, использование режима ППРЧ тому подобное);
- перевод радиосетей (радионаправлений) из симплексного в дуплексный режим работы;
- своевременная смена радиоданных;
- использование направленных антенн;
- использование кабельных линий связи для дистанционного управления радиопередатчиками;
- централизованное использование передаточных радиосредств;
- исключение работы главным лепестком диаграммы направления антенны в сторону противника;
- использование антенн радио- и радиорелейных станций на мачтах минимально допустимой высоты;
- организация оперативного контроля безопасности связи при ведении радиообмена и своевременного прекращения нарушений безопасности связи;
- применение переговорных таблиц и кодируемых топокарт для

передачи информации по средствам связи.

Важнейшей *организационной мерой* является установление одного из трех *режимов работы радиосредств* :

I режим – полный запрет работы средств радиосвязи на передачу (режим радиомолчания).

II режим – частичное ограничение работы средств радиосвязи на передачу.

III режим – работа средств радиосвязи без ограничений (работа на передачу за необходимости).

Противодействие радиоуправляемым боеприпасам и другим радиоуправляемым ВВТ с учетом опыта участия ВС на востоке Украины.

В ходе проведения АТО (ООС) было отмечено большое количество случаев применения различных радиоуправляемых взрывных устройств, как в ходе передвижения подразделений, так и при проверке транспортных средств на блокпостах. Использование этого способа подрыва обусловлено возможностью влиять на ситуацию дистанционно и в реальном масштабе времени.

На начальном этапе конфликта такой способ должен был характеризовать "партизанский" характер действий , в дальнейшем, с провалом "революции", к таким действиям приобщились диверсионные группы противника.

Основную часть радиоуправляемых боеприпасов, применяемых в зоне АТО (ООС) против военных, составляют самодельные, приводимые в действие по радиоканалу с использованием легко доступных радиосредств, не имеющих военного назначения.

В целях защиты от самодельных радиоуправляемых боеприпасов при подготовке к маршу, маршрут которого проходит через районы действий диверсионно-разведывательных сил противника и незаконных вооруженных формирований, военная техника подразделений оснащается малогабаритными передатчиками помех (МЧП).

Принцип радиоэлектронного прикрытия объектов МЧП состоит в создании шумового заградительного препятствия, которое не дает возможности радиоприемникам взрывных устройств принять команду на подрыв боеприпаса.

Во время выполнения боевых задач в Республике Ирак украинский контингент использовал передатчики радиопомех РП-377АМ, которые устанавливались на военной технике.

Сегодня на вооружении ВС Украины более современный передатчик радиопомех МПП-1, который устанавливается на все виды техники, выполняющей задачи в зоне АТО (ООС).

В своем составе МПП-1 имеет 4 независимых блока подавления радиолиний (БПРЛ), а также пульты дистанционного управления и устройства автономного включения в заданное время для каждого БПРЛ. При одновременной работе всех блоков достигается постановка препятствий по

всему диапазону рабочих частот комплекса МПП-1, что обеспечивает защиту от различных технических средств взрыва.

На вооружении подразделений РЭБ ВС Украины в 2014 г. в основном находились именно эти средства (приложение 10).

Рекомендации по применению МПП-1:

- блоки МПП-1 целесообразно размещать на двух БТР (БМП), по два на каждом и подключать их к бортовым. АКБ;
- блоки МПП-1 целесообразно располагать в разных углах кузова транспортных автомобилей; автомобиль с МПП-1 размещать в середине колонн;
- после включения МЧП-1 обязательно проводить проверку обеспечения связи в подразделении;
- проводить тренировку (обслуживание) аккумуляторов МПП-1 перед их применением;
- создавать запас антенн и кабелей подключения блоков МПП-1 к бортовой сети питания, которые чаще всего испытывают повреждения, ремонтные принадлежности (паяльники, припой, термопаста, силикон тому подобное);

РЭБ и Международное гуманитарное право

Командир (начальник) и штаб при организации и в ходе ведения военных действий должны учитывать нормы Международного гуманитарного права, как того требуют международные обязательства Украины.

Военнослужащие Вооруженных сил Украины должны твердо знать в объеме занимаемой должности и точно выполнять требования положений Международного гуманитарного права.

При организации и ведении радиоэлектронной борьбы необходимо предусматривать:

- введение запрета на радиоэлектронное подавление радиоэлектронных средств и линий связи, используемых военными и гражданскими медицинскими службами, военным и гражданским духовным персоналом противника, гуманитарными организациями, гражданской обороной, персоналом охраны объектов, находящихся под защитой. они не будут использоваться противником в военных целях;
- проведение комплекса организационных и технических мероприятий по радиоэлектронной защите систем и средств своих аналогичных служб (объектов) и организаций, определенных международным гуманитарным правом.

Распознавание радиоэлектронных средств, принадлежащих службам (организациям), указанным выше, производится по опознавательным радиосигналам в соответствии с требованиями Регламента Радиосвязи Международного союза электросвязи ISBN 92-61-04144-2.

Список сигналов и рабочих частот доводится до командиров (начальников) воинских частей и подразделений радиоэлектронной борьбы и хранится на соответствующих командных пунктах (пунктах управления) как в

мирное, так и в военное время.

Особенности распознавания медицинских формирований и санитарно- транспортных средств

Для распознавания медицинских формирований и санитарно транспортных средств могут использоваться опознавательный световой сигнал и радиосигнал, а также электронное распознавание.

Световой сигнал подается в виде вспышек голубого цвета (частота – от 60 до 100 вспышек в мин) и используется для распознавания санитарных летательных аппаратов. Никакой другой летательный аппарат не должен использовать этот сигнал. Использование указанного светового сигнала для распознавания наземных санитарно-транспортных средств и санитарных судов **не запрещается .**

Радиосигнал представляет собой радиотелефонное или радиотелеграфное сообщение, перед которым передается опознавательный сигнал приоритета (срочности), переданное на частотах и в порядке, установленных Регламентом радиосвязи.

Для оповещения и распознавания медицинского транспорта после передачи сигнала срочности передается слово MEDICAL в узкополосной литературопечатной телеграфии, а в радиотелеграфии – слово MAY-DEE-CAL, которое в украинской транскрипции произносится как «ме-ди-каль».

Использование сигнала приоритета (срочности) разрешается исключительно медицинским формированием и санитарно транспортными средствами.

Радиотелефонное или радиотелеграфное сообщение передается на английском языке и должно содержать следующие данные:

- позывное или иное признанное средство распознавания медицинского транспорта;
- местонахождение медицинского транспорта;
- количество и типы средств медицинского транспорта;
- намеченный маршрут;
- ожидаемое время пребывания в пути и время отправления и прибытия в зависимости от обстоятельств;
- любые другие сведения, такие, как высота полета, защищенные радиочастоты, используемые языки, режим работы и коды вторичного обзорного радара.

Перед вызовом следует передавать сигнал срочности, состоящий из группы слов «PAN PAN PAN». Каждое слово группы произносится в украинской транскрипции как «господин».

Сигнал срочности и следующее сообщение должны передаваться:

- на одной или нескольких международных частотах бедствия – 500 кГц, 2182 кГц и 156,8 МГц;
- на дополнительных частотах бедствия – 4125 кГц и 6215 кГц;
- на воздушной аварийной частоте 121,5 МГц;
- на частоте 243 МГц или любой другой частоте, которая может

использоваться в случаях бедствия.

Электронное распознавание обеспечивается применением Системы повторного распознавания радиолокаций, описание которой и процедуры введения ее в действие установлены международными договорами о Международной организации гражданской авиации. Данная система может применяться для распознавания санитарного летательного аппарата и наблюдения за его курсом.

Указанная система электронного распознавания с согласия сторон, находящихся в вооруженном конфликте, может использоваться для распознавания наземных санитарно-транспортных средств и санитарных судов.