ЗМІСТ

Радиоэлектронная борьба в Вооруженных силах США. Книга ворога, ворожою мовою

Анотація

В работе на основе открытых источников отражены взгляды военного руководства США на ведение радиоэлектронной борьбы.

Проведен анализ соответствующих руководящих документов, приведены сценарии применения систем РЭБ в вооруженных конфликтах. Рассмотрены способы подавления систем связи, управления и навигации. Подробно разобраны силы и средства РЭБ ВВС, авиации ВМС и Сухопутных войск ВС США.

Затронуты вопросы функционального поражения объектов. Показаны перспективы развития средств РЭБ. Материал адресован специалистам, ведущим прикладные исследования в области радиоэлектронной борьбы.

РАДИОЭЛЕКТРОННАЯ БОРЬБА В ВООРУЖЕННЫХ СИЛАХ США

КНИГА ВОРОГА
ВОРОЖОЮ МОВОЮ

Издательский дом
«С В А Р О Г»
Киев – 2023

УДК 621.396.663
Р 15

Радиоэлектронная борьба в Вооруженных силах США. Книга ворога, ворожою мовою. — Киев: Изд. дом «СВАРОГ», 2023. — 131с.

Р 15

ISBN 978-611-01-2980-0

В работе на основе открытых источников отражены взгляды военного руководства США на ведение радиоэлектронной борьбы. Проведен анализ соответствующих руководящих документов, приведены сценарии применения систем РЭБ в вооруженных конфликтах. Рассмотрены способы подавления систем связи, управления и навигации. Подробно разобраны силы и средства РЭБ ВВС, авиации ВМС и Сухопутных войск ВС США. Затронуты вопросы функционального поражения объектов. Показаны перспективы развития средств РЭБ.

Материал адресован специалистам, ведущим прикладные исследования в области радиоэлектронной борьбы.

ISBN 978-611-01-2980-0 УДК 621.396.663

Список используемых сокращений

AARGM – Advanced Anti–Radiation Guided Missile – перспективная управляемая противорадиолокационная ракета;
AEA – Airborne Electronic Atack – программа по применению авиационных групповых средств РЭБ в рамках единого комплекса;
ABL – Airbome Laser – проект "воздушный лазер";
AMMP – AEA Mission Management Processing – подсистема обработки и управления комплексом РЭБ АЕА;
AWACS – Airborne Warning and Control System – система дальнего радиолокационного обнаружения и управления авицией;
AEA – Airborne Electronic Atack – программа по применению авиационных групповых средств РЭБ в рамках единого комплекса;
C^3CM – Command, Control and Communication Counter Measures – борьба с системами боевого управления (концепция);
CCJ – Core Component Jammer – ядро (компонент для) создания нового комплекса радиоэлектронной борьбы;
CEASAR – Communications Electronic Attack with Surveillance and Reconnaissance – комплекс РЭБ и радиоэлектронной разведки;
CHAMP – Counter–electronic High Power Microwave Advanced Missile Project – проект демонстрационного образца нелетального СВЧ-оружия на воздушной платформе;
CIWS – Close–In Weapon System – орудийная система ближнего боя;
COIL – Chemical Oxygen Iodine Laser – химический лазер;
DARPA – Defense Advanced Research Projects Agency – Управление перспективных исследовательских проектов Министерства обороны США;
DEA – Defensive Electronic Attack – комплекс радиоэлектронной защиты;
DRFM – Digital Radio Frequency Memory – цифровое устройство запоминания радиочастот;
EFVS – Electronic Fight Vehicle System – мобильная система радиоэлектронной борьбы;
EWPMT – Electronic Warfare Planning and Management Tools – комплекс планирования и управления радиоэлектронной борьбой;
FCS – Future Combat Systems – Боевые системы будущего (программа);
FEL – Free Electron Laser – лазер на свободных электронах;
HARM – High–speed Anti–Radar Missile – высокоскоростная противорадиолокационная ракета;
HEL MD – High Energy Laser Mobile Demonstrator – опытный высокоэнергетический мобильный лазер;
HIRAT – High–power Ram Air Turbine – высокомощные генераторные турбины набегающего потока;
HMMWV – High Mobility Multipurpose Wheeled Vehicle – высокоподвижное многоцелевое колесное транспортное средство;
HPM – High Power Microwave – СВЧ или микроволновое оружие;
IDECM – (Integrated Defensive Electronic Countermeasures – интегрированная система РЭБ индивидуальной защиты самолетов;
IEWCS – Intelligence and Electronic Warfare Common Sensor – единые средства разведки и электронной войны (программа);
IEWS – Integrated Electronic Warfare System – интегрированная система радиоэлектронной борьбы;
INCANS – INterference CANcellation System – устройство исключения собственных помех;
INSCOM – Intelligence and Security Command – Командование разведки и безопасности;

JTIDS – Joint Tactical Information Distribution System – объединенная распределенная боевая информационная система;
LaWS – Laser Weapon System – лазерная система вооружения;
MALD – Miniature Air–Launched Decoy – миниатюрная воздушная ложная цель;
MFEW – Multi–Function Electronic Warfare – многофункциональный комплекс радиоэлектронной борьбы;
MLD – Maritime Laser Demonstrator – опытный морской лазер;
NCW – Network–Centric Warfare – сетецентрическая война;
NERO – Networked Electronic Warfare, Remotely Operated – сетевой комплекс радиоэлектронной войны с дистанционным управлением;
NGJ – Next Generation Jammer – система радиоэлектронного подавления следующего поколения;
RAT – Ram Air Turnbine – генераторная турбина набегающего потока;
RFW – Radio Frequency Weapon – радиочастотное оружие;
SINCGARS – Single Channel Ground and Airborne Radio System – система связи тактического звена управления;
TLS – Tactical Laser System – тактическая лазерная система;
TRACS – Tactical Radio Acquisition and Countermeasures Subsystem – тактическая система радиоразведки и радиоэлектронного подавления;
TTD – True Time Delay – задержка сигнала в реальном масштабе времени;
АЛВЦ – автономная ложная воздушная цель;
АМ – амплитудная модуляция (сигнала);
АСУ – автоматизированная система управления;
АФАР – активная фазированная антенная решетка;
ббр – боевая бригада;
БПЛА – беспилотный летательный аппарат;
БРЭО – бортовое радиоэлектронное оборудование;
ВВС – Военно-воздушные силы;
ВВТ – вооружение и военная техника;
ВМГ – взрывомагнитный генератор;
ВМС – Военно-морские силы;
ВС – Вооруженные силы;
ВТО – высокоточное оружие;
ВЧ – высокие частоты (диапазон радиосвязи);
ГСН – головка самонаведения;
ДКМ – декаметровый (диапазон радиосвязи);
КНШ – Комитет начальников штабов ВС США;
КПД – коэффициент полезного действия;
КРВБ – крылатая ракета воздушного базирования;
ЛА – летательный аппарат;
ЛВЦ – ложная воздушная цель;
ЛРС – линия радиосвязи;
ЛЦ – ложная цель;
ЛЧМ – линейная частотная модуляция (вид радиосигнала);
МВ – метровые волны (диапазон радиосвязи);
ММВ – миллиметровые волны (диапазон электромагнитных волн);
МО – Министерство обороны;
МП – морская пехота;
МППУ – малогабаритное приемопередающее устройство;
МСВЧ – монолитные сверхвысокочастотные (интегральные схемы);
НАТО – Организация Североатлантического договора;

НИОКР – научно-исследовательские и опытно-конструкторские работы;
ОВС – объединенные вооруженные силы;
ОВЧ – очень высокие частоты (диапазон радиосвязи);
ОСШП – отношение сигнал/(шум + помеха);
ПВО – противовоздушная оборона;
ПЛИС – программируемая логическая интегральная схема;
ПО – программное обеспечение;
ПОИ – передатчики одноразового использования;
ППРЧ – псевдослучайная перестройка рабочей частоты;
ПРО – противоракетная оборона;
ПУ – пункт управления;
ПЭ – программный элемент;
РЛС – радиолокационная станция;
РРЛ – радиорелейная линия (радиосвязи);
РРТР – радио- и радиотехническая разведка;
РСП – разведывательно-сигнализационный прибор;
РФ – Российская Федерация;
РЭА – радиоэлектронная аппаратура;
РЭБ – радиоэлектронная борьба;
РЭО – радиоэлектронное оборудование;
РЭП – радиоэлектронное подавление;
РЭР – радиоэлектронная разведка;
РЭС – радиоэлектронное средство;
СБА – стратегическая бомбардировочная авиация;
СВ – Сухопутные войска;
СВЧ – сверхвысокая частота (диапазон радиосвязи);
СРНС – спутниковая радионавигационная система;
ССС – система спутниковой связи;
США – Соединенные Штаты Америки;
ТВД – театр военных действий;
ТРЛ – тропосферная радиолиния (радиосвязи);
ТТХ – тактико-технические характеристики;
УКВ – ультракороткие волны (диапазон радиосвязи);
УФ – ультрафиолетовый (диапазон электромагнитных волн);
ФАР – фазированная антенная решетка;
ФКМ – фазово-кодовая модуляция (сигнала);
ФМ – фазовая модуляция (сигнала);
ЧМ – частотная модуляция (сигнала);
ЭВМ – электронно-вычислительная машина;
ЭДС – электродвижущая сила;
ЭМВ – электромагнитная волна;
ЭМИ – электромагнитное излучение;
ЭМО – электромагнитное оружие;
ЭМП – электромагнитное поле;
ЭПР – эффективная площадь рассеивания.

Введение

Борьба с системами управления противника за счет использования средств радиоэлектронной борьбы (РЭБ) является важным и исторически наиболее развитым направлением информационного противоборства.

Именно средства РЭБ традиционно использовались для решения тех задач, которые сейчас ставятся перед средствами информационного противоборства. Эволюция средств РЭБ и стремительное развитие информационных и телекоммуникационных технологий потребовали изменения роли радиоэлектронной борьбы, рассмотрения ее в качестве составной части информационного противоборства в технической сфере. Вместе с тем, это не привело к утрате радиоэлектронной борьбой своей актуальнейшей роли. Несмотря на широкое внедрение в системы военного управления телекоммуникационных и компьютерных систем, по-прежнему основой систем управления оружием являются средства радиолокации, а основой систем управления – средства связи. При этом средства РЭБ исторически ориентированы на нарушение функционирования именно этих средств. Опыт локальных конфликтов начала XXI века показал, что именно операции РЭБ являются основой дестабилизирующего воздействия на подсистемы связи систем военного управления противника. Системы РЭБ решают задачи подавления радиолокационных средств противовоздушной обороны (ПВО) и прикрытия боевых порядков авиации в первые часы войны. От эффективности операции РЭБ, проводимой накануне и в период первого удара, напрямую зависит эффективность подавления боевого потенциала противника, а также результативность применения высокоточного оружия (ВТО) и авиации.

В работе представлена терминология радиоэлектронной борьбы, принятая в Вооруженных силах (ВС) США, проведен анализ организационно-штатных структур подразделений, ведущих радиоэлектронную борьбу, а также соответствующих средств различных видов ВС США, ориентированных на борьбу как с системами управления оружием, так и с системами связи.

Автор выражает искреннюю признательность своему учителю – замечательному ученому, кандидату технических наук доценту Макаренко Сергею Ивановичу за помощь в подготовке материала и полезные советы, позволившие уточнить его предметную область. Общий методический подход к изложению материала, использованный в монографии [1], лег в основу настоящей работы.

Автор благодарит кандидата технических наук доцента Уткина Владимира Владимировича за кропотливый труд по поиску ошибок и неточностей при рецензировании работы.

1. РОЛЬ И СПОСОБЫ ПРИМЕНЕНИЯ СИСТЕМ И СРЕДСТВ РЭБ

1.1. Основные термины, определения и классификация систем РЭБ, принятые в ВС США

Анализ оперативных учений, локальных войн и вооруженных конфликтов последних лет позволяет сделать вывод о том, что радиоэлектронная борьба (Electronic Warefare – радиоэлектронная война согласно американской терминологии) в ВС США прочно утвердилась как одно из важных средств информационного противоборства. Она стала неотъемлемой частью вооруженной борьбы и информационных операций [2].

Согласно положению наставления JP 3–13 РЭБ определяется как "*... любые действия войск (сил), включающие в себя использование электромагнитной энергии и средств направленной энергии для непосредственного воздействия на противника и используемые им излучения электромагнитного спектра частот*". В этом же документе указывается, что РЭБ является одним из основных элементов информационных операций. Полевой устав FM 3–36 трактует термин РЭБ как "*... действия войск (сил) по использованию электромагнитной энергии и средств направленной энергии в целях осуществления управления (контроля) излучениями электромагнитного спектра частот (в том числе и использования самого спектра частот) или воздействия (атаки) на личный состав, радиоэлектронные системы и средства, объекты, вооружение и военную технику противника*" [3].

Опыт проведения учений и участия ВС США в вооруженных конфликтах показал, что даже подавляющее превосходство в области средств ВТО не гарантирует благоприятного исхода операции в том случае, если системы управления различного уровня оставались неподавленными [2, 4].

Объектами первоочередного воздействия систем РЭБ в ходе операции являлись [2]:

- элементы систем управления войсками (силами) и оружием;
- средства разведки и системы хранения, обработки и распределения информации;
- радиоэлектронные средства (РЭС);
- информационные и автоматизированные системы, базы данных и сети ЭВМ;
- системы поддержки принятия решений для командного состава.

Аналитики Пентагона полагают, что основными причинами повышения роли радиоэлектронной борьбы в современных сетецентрических войнах являются [2, 4]:

- возрастание факторов своевременности и устойчивости управления войсками и оружием в ходе боевых действий;
- рост масштабов использования РЭС различных типов для передачи информации на значительные расстояния в целях оперативного, непрерывного и гибкого управления войсками и оружием;
- возможность практически мгновенно дезорганизовать средствами радиоэлектронного подавления (РЭП) процессы боевого управления противника и тем самым обеспечить коренное изменение соотношений сил в свою пользу;
- повышение маневренности ВС, увеличение масштаба глубины проведения операций, автоматизация всех процессов управления (войсками, боевой техникой и оружием);
- создание функциональных интегрированных систем управления, разведывательного обеспечения, систем РЭБ и ВТО привело к количественному перераспределению в операции ударных и обеспечивающих сил. Так, по заключению экспертов, в операциях начала XXI века около 60 % войск, принимающих участие в боевых действиях, решают задачи обеспечения ударных сил (разведка, маскировка, управление и связь, автоматизация, наведение оружия и др.), что в еще большей степени повышает значение РЭБ в информационной и вооруженной борьбе;
- за вековой путь эволюционного развития РЭБ существенно изменились ее содержание, составные элементы, характер, используемые средства, объекты разведки, воздействия и защиты;

− повышение универсальности сил и средств РЭБ по отношению к средствам системы боевого управления противника. Они могут действовать на всю глубину театра войны в целом, позволяют осуществлять разведывательно-информационное обеспечение операции, использовать нелетальные и летальные (поражающие) средства, воздействовать в любое время суток на объекты, боевую технику и оружие, а также обеспечивать защиту своих сил и средств.

Средства РЭБ могут применяться скрытно и открыто, входить в состав различных многоцелевых функциональных и автоматизированных интегрированных систем многосферного базирования, боевого управления, связи, компьютерного обеспечения разведки, огневого поражения, борьбы с системами управления противника и защиты своих систем, использовать в своих интересах сети ЭВМ противоборствующей стороны и воздействовать на них [2].

Постоянное повышение требований к системам разведки и РЭБ, а также появление новых стратегических концепций сетецентрической войны стало основой революционного развития РЭБ в конце XX – начале XXI века. Это привело к изменению характера РЭБ, ее содержания, состава сил и средств, роли, места, цели и задач в операциях. Эти факторы предопределили создание новых средств РЭБ, в том числе для осуществления скрытного радиоэлектронного подавления, летального и нелетального оружия, средств подавления и поражения, действующих на новых физических принципах, а также информационно-технических воздействий, предназначенных для атаки на компьютерные сети противника [2, 5].

Развитие сил и средств РЭБ и преобразование их в одну из основных составляющих сил "борьбы с системами боевого управления" вызвало появление новых понятий в стратегии и терминологии информационной войны, таких как "война в сетях" или "сетевая война" (Net War), "кибервойна" (Cyber War), "ведение боевых действий и управление вооруженными силами в едином информационно-коммуникационном пространстве". Все эти термины предполагают организацию управления ВС в условиях ведения операций с использованием сил и средств борьбы с системами боевого управления для воздействия на многочисленные локальные, объединенные региональные и глобальные сети ЭВМ противника и защиты своих компьютерных сетей [2].

В настоящее время аналитиками Пентагона отмечается, что в современных условиях именно РЭБ является основой информационного противоборства [2].

Анализ эволюции и развития РЭБ в ВС США и объединенных вооруженных сил (ОВС) НАТО позволил выявить возникшие в последние годы различия между характером, содержанием мероприятий и ролью РЭБ, которые сводятся к следующему [4]:

− радиоэлектронная борьба в ВС США и в ОВС НАТО имеет различные объекты воздействия и защиты. Если мероприятия РЭБ в ВС ряда государств связаны только с воздействием на РЭС противника, то в ВС США, а в перспективе – и в ОВС НАТО они направлены как на воздействие, так и на защиту РЭС, а также распространяются на боевую технику, объекты ВС и системы оружия. В рамках проведения мероприятий РЭБ в ВС США уже сегодня кроме использования источников излучения электромагнитной энергии и противорадиолокационных ракет предусматривается задействование других видов летального и нелетального оружия, базирующегося на излучении направленной энергии. При этом в качестве основной цели радиоэлектронной атаки средств РЭБ в ВС США рассматривается система ПВО противника;

− в мероприятиях РЭБ в ВС США имеется такой самостоятельный элемент, как "радиоэлектронное обеспечение операции" (боевых действий), который отсутствует в подобных мероприятиях ВС ряда других государств НАТО;

− мероприятия РЭБ в ВС США и в ОВС НАТО являются основой противодействия системам боевого управления, то есть радиоэлектронная борьба стала наиболее важным составным элементом информационного противоборства. В других же странах это лишь один из элементов мероприятий оперативного обеспечения, проводимых при дезорганизации управления войсками противника в операции.

Как отмечается в программе создания сухопутных войск США нового типа, "радиоэлектронное поле боя" (Electromagnetic Field of Battle) претерпит значительные изменения с учетом

расширения спектра используемых рабочих радиочастот РЭС, который станет более насыщенным и менее доступным для противника. Возрастут возможности, и станут более гибкими силы и средства РЭБ. Последние будут способны функционировать во всех частотных диапазонах, причем планируется применять различные средства летального и нелетального воздействия не только на РЭС противника, но и на его боевую технику и системы вооружения [2].

Анализ эволюции характера, содержания и роли РЭБ в операциях конца XX – начала XXI в. дает возможность вскрыть и сформулировать основные тенденции развития РЭБ в ВС США и в ОВС НАТО до 2025 г., которые наметились в ходе интеграции сил и средств разведки, РЭБ и борьбы с системами боевого управления. К таким тенденциям развития следует отнести следующие [4].

− частичная утрата самостоятельной роли РЭБ, которая становится одним из основных элементов информационного противоборства, в основном для борьбы с системами боевого управления при проведении информационных операций;

− коренное поэтапное изменение характера, содержания и роли РЭБ в операции (бое). Так, на первом этапе она являлась одним из видов поддержки ударных сил в ходе боевых действий, на втором – составной частью ведения боевых действий каждого вида ВС со всеми специфическими особенностями. На третьем этапе РЭБ стала компонентом синергетической системы информационного противоборства – одной из составляющих военного потенциала;

− использование для ведения РЭБ новых видов направленной энергии, а также создание летального и нелетального оружия, действующего на новых физических принципах;

− переход от подавляющего воздействия и защиты РЭС к комплексному поражающему и подавляющему информационно-техническому воздействию и защите не только РЭС, но и боевой техники, объектов ВС, систем оружия, а также личного состава и органов государственного управления;

− смещение акцента противоборства в информационно-интеллектуальную область, сферу подготовки и принятия решений, планирования и руководства операцией (боем). Становление РЭБ в качестве основы информационного противоборства;

− обеспечение полной информатизации и автоматизации процесса радиоэлектронной борьбы.

В настоящее время в ВС США радиоэлектронная борьба рассматривается, с одной стороны, как составная часть вооруженного противоборства и военного потенциала, а с другой – как одна из форм вооруженной борьбы и новый, относительно самостоятельный и специфический вид боевых действий. Отличительной особенностью современных взглядов на ведение РЭБ является признание ее комплексности и тесной связи с другими видами боевой деятельности войск [4].

Мероприятия РЭБ составляют основу новой активно внедряемой в ВС США концепции "Борьбы с системами боевого управления" (CCCCM или C^3CM – Command, Control and Communication Countermeasures). Суть концепции состоит в том, чтобы *"...путем интегрированного проведения специальных операций по военной дезинформации, радиоэлектронного подавления, физического уничтожения, базирующегося на основе детальных разведданных, лишить противника информации и способности управлять вверенными ему силами, а также защитить свои системы боевого управления от аналогичных действий с его стороны*" [2].

Целями РЭБ в операциях нового типа наряду с дезорганизацией систем боевого управления противника станут лишение его возможности использовать информацию о своих войсках и действиях противостоящей стороны, обеспечение упреждения противника в принятии оперативных (боевых) решений и повышение эффективности ведения боевых действий ВС США, снижение людских и материальных потерь и успешное завершение операции в кратчайшие сроки. В ходе проведения информационных операций силы РЭБ будут применяться в сочетании с силами информационных операций других видов ВС [4].

Практическая реализация упомянутой концепции "радиоэлектронного поля боя" в информационной операции с участием сил и средств РЭБ предполагает последовательное выполнение четырех основных задач [2]:

− анализ системы боевого управления противостоящей группировки;
− выбор наиболее важных объектов и целей;
− распределение имеющегося ресурса средств по выбранным целям;
− непосредственное воздействие на выбранные цели.

Инструментом для проведения положений новой концепции в практику войск военное руководство США считает крупные многоуровневые иерархические структурно-упорядоченные системы РЭБ, тесно интегрируемые с другими боевыми и обеспечивающими системами войск [2].

Основными принципами ведения РЭБ в информационных операциях, по взглядам руководства США, являются [2]:

− жесткое согласование мероприятий РЭБ с общим планом информационной операции по месту, времени и задачам;
− массированное комплексное применение сил и средств РЭБ по всем радиоканалам между подавляемыми объектами;
− внезапность применения сил и средств РЭБ, нестандартная тактика их использования.

Способами воздействия на объекты подавляемой системы боевого управления противника являются массированное воздействие средствами поражения, захват командных пунктов и узлов связи, введение противника в заблуждение через его же средства разведки, РЭП, организация утечки ложной информации [2].

В информационных операциях воздействие на противника осуществляется силами и средствами борьбы с системами государственного и военного управления, в состав которых входят силы и средства РЭБ [2].

В интересах достижения решающего военно-технического превосходства средств РЭБ в США проводятся следующие мероприятия [2]:

− создание качественно новых средств "силового" радиоэлектронного подавления, предназначенных для кратковременного и необратимого вывода из строя информационных систем и РЭС противника;
− заблаговременная разработка аппаратуры, ориентированной на противодействие перспективным РЭС и системам противника и превосходящей их по временным и энергетическим параметрам работы;
− разработка средств РЭБ с высокой степенью адаптации, способных автоматически в реальном масштабе времени оценивать радиоэлектронную обстановку и осуществлять выбор оптимального воздействия на РЭС помехами;
− совершенствование технических характеристик средств радио- и радиотехнической разведки (РРТР) в направлении повышения чувствительности приемников, увеличения пропускной способности и быстродействия аппаратуры, а также точности определения частоты подавляемой РЭС;
− совершенствование технических характеристик средств РЭП.

Доктринальными документами ВС США определены следующие основные задачи РЭБ в информационной операции [2]:

− дезорганизация системы управления противника, лишение его возможности использовать информацию о своих войсках и действиях противника;
− разрушение, искажение или создание в неадекватной реальной обстановке информации, провоцирующей противника на неверные действия;
− повышение эффективности ведения боевых действий ВС США и их союзников;
− снижение людских и материальных потерь и завершение информационной операции в кратчайшие сроки.

В перечне задач выделяется воздействие не только на РЭС, но и на боевую технику, системы оружия и личный состав органов управления и обслуживания противника [2].

Радиоэлектронная борьба в ВС США подразделяется на следующие мероприятия (рис. 1.1) [1, 2, 4, 6, 7, 8]:

− радиоэлектронная атака (EA – Electronic Attack);

− радиоэлектронная защита (EP – Electronic Protect);
− радиоэлектронное обеспечение (EWS – Electronic Warfare Support).

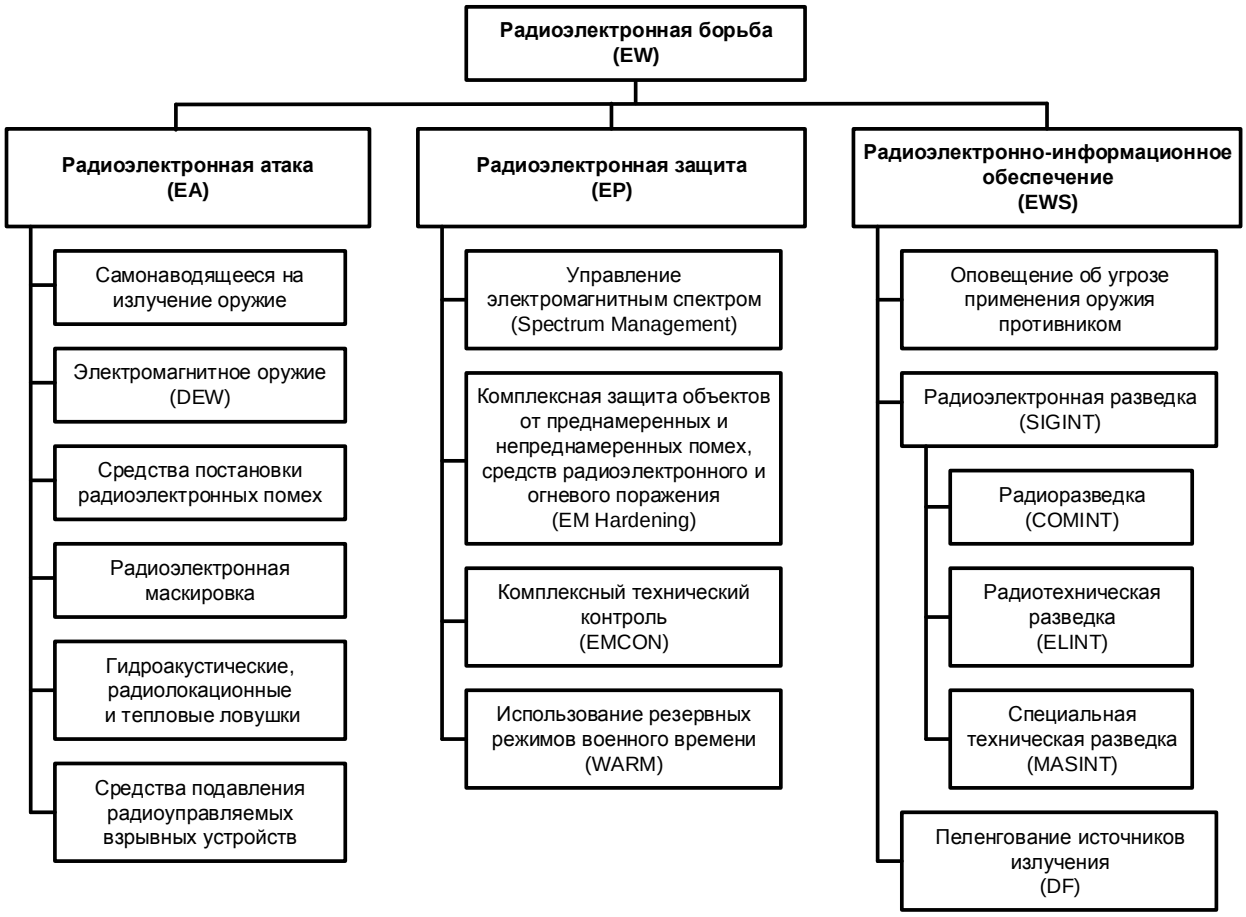


Рис. 1.1. Классификация РЭБ в ВС США

Радиоэлектронная атака – действия наступательного характера, предусматривающие использование электромагнитной и других видов направленной энергии и (или) самонаводящегося на электромагнитное излучение оружия для целенаправленного воздействия на системы управления, личный состав, объекты и боевую технику с целью дезорганизовать, нейтрализовать или снизить возможности противника по эффективному использованию им радиоэлектронных систем в различных звеньях управления ВС [2, 8].

Радиоэлектронная атака проводится с использованием [2]:

− средств РЭП и радиоэлектронной дезинформации;

− огневых средств, самонаводящихся на излучение различных радиоэлектронных устройств (например, излучение РЭС, систем пуска автомобилей, бронетранспортеров, танков, электропривода орудий и др.);

− управления режимами излучения электромагнитной и направленной энергии;

− управления ложной работой РЭС, имитацией их работы и обеспечения демонстративных действий;

− управляемого оружия с радио- и радиолокационными, инфракрасными, лазерными, гидроакустическими и другими головками самонаведения (ГСН);

− инфразвукового, радиочастотного, лазерного, пучкового и других типов оружия направленной энергии.

Для воздействия на информационные ресурсы противника в мероприятиях РЭБ в ВС США помимо использования источников излучения электромагнитной энергии и иных средств предусматривается применение ложных целей, летального и нелетального оружия,

базирующегося на излучении других видов направленной энергии, в том числе действующих на новых физических принципах (инфразвуковое, лазерное, пучковое и др.) [2].

К объектам (целям) радиоэлектронных атак командование ВС США относит [9]:

− личный состав, боевую технику и системы оружия, а также различную радиоэлектронную аппаратуру;

− пункты управления, узлы связи и радиотехнического обеспечения;

− системы и средства боевого управления, связи, разведки, радиолокации, радионавигации.

Согласно наставлениям и уставам ВС США выбор конкретных способов и средств радиоэлектронной атаки, также как и электронной защиты, а также обеспечения ведения электронной войны, зависит от задач проводимой операции, возможностей противника и, собственно, имеющихся на вооружении или уже задействованных в операции соответствующих сил и средств. Кроме того, учитываются видовая принадлежность этих сил и средств, платформы размещения, тактико-технические характеристики и т. п. [9].

Разновидностями форм проведения радиоэлектронной атаки, по взглядам военных аналитиков США, являются [2]:

− радиоэлектронный удар;
− поражающий радиоэлектронный удар;
− радиоэлектронно-огневой удар;
− радиоэлектронная блокада;
− удар средствами нелетального и летального оружия.

Таким образом, мероприятия радиоэлектронной атаки в зависимости от применяемых средств подразделяются [2]:

− на непоражающие;
− поражающие.

К непоражающим (нелетальным) средствам воздействия относятся [2]:

− средства радиоэлектронных помех;
− средства радиоэлектронной дезинформации.

Поражающими средствами воздействия являются [2]:

− средства излучения направленной энергии;
− ВТО и боеприпасы с элементами радиоэлектронного самонаведения.

При этом средства излучения направленной энергии на больших площадях могут действовать как средства помех, не оказывая поражающего воздействия.

Задачами непоражающих средств при проведении радиоэлектронной атаки являются [2, 4]:

− срыв, подавление или вывод из строя радиоэлектронных и оптико-электронных систем, а также средств разведки, наблюдения, наведения, связи, навигации, управления войсками и оружием;

− изменение режима излучения РЭС;
− имитация и ложная работа РЭС, объектов и оружия своих войск и войск противника;
− имитация демонстративных действий войск;
− дезорганизация систем связи и управления противника;
− введение противника в заблуждение относительно намерений своих войск;

− воздействие на личный состав противника, обслуживающий РЭС, системы разведки, наблюдения, средства связи, навигации и управления войсками и оружием, а также участвующий в анализе добытой разведкой информации, подготовке и принятии решений, планировании операции или боя.

Задачами поражающих средств при радиоэлектронной атаке могут быть следующие [2, 4]:

− наведение на цель средств ВТО и оружия направленной энергии;
− уничтожение, разрушение и вывод из строя средств разведки, навигации и наблюдения;

− уничтожение, разрушение и вывод из строя средств, узлов, центров и органов связи, управления войсками и оружием противника, а также его объектов, боевой техники и систем оружия;

− поражение и вывод из строя личного состава противника, участвующего в подготовке, принятии оперативных (боевых) решений и планировании операции (боя).

Опыт локальных войн показал, что применение средств РЭБ ведется одновременно с применением средств ВТО и оказывается для противника кратковременным и неожиданным. В связи с этим было бы логично выделить отдельную форму радиоэлектронной атаки – "радиоэлектронный удар" [2].

При этом в зависимости от состава привлекаемых сил и средств, "радиоэлектронные удары" могут быть [2]:

− одиночными;

− массированными.

С учетом пространственного размаха "радиоэлектронные удары" могут быть [2]:

− сосредоточенными;

− рассредоточенными.

Комбинированное применение средств РЭП и огневого воздействия в целях нарушения функционирования РЭС противника можно определить как "радиоэлектронно-огневой удар". В подобных ударах огневые средства поражения могут использовать как обычные боеприпасы, так и боеприпасы с радиолокационными ГСН. Учитывая широкомасштабные научно-исследовательские и опытно-конструкторские работы в области создания военной робототехники, его разновидностью может быть "роботизированный радиоэлектронно-огневой удар". Ответные радиоэлектронные и радиоэлектронно-огневые удары, возможно, приведут к новому виду формы боя – "радиоэлектронно-огневому бою" [2].

Радиоэлектронная защита включает в себя разносторонние пассивные и активные мероприятия и специальные средства, обеспечивающие защиту от любого воздействия противника и его средств РЭБ своих группировок войск, личного состава, боевой техники, систем оружия, объектов и отдельных радиоэлектронных средств. Кроме того, этот вид защиты предусматривает необходимые мероприятия и способы противодействия техническим средствам разведки противника, контроль за излучением своих РЭС, обеспечение управления их режимами и электромагнитной совместимости [4].

Радиоэлектронная защита согласно положениям наставления Комитета начальников штабов (КНШ) JP 3–13 и полевого устава FM 3–36 предусматривает [3]:

− управление задействованием электромагнитным спектром частот, обеспечивающее свободное использование в нем своих РЭС, в том числе и перепрограммирование сил, средств, задач и способов РЭБ;

− усиление защитных свойств объектов (целей), в частности создание специальных схем, экранов, укрытий, технических средств защиты (в первую очередь речь идет о физических и технических средствах защиты от воздействия электромагнитных излучений РЭС своих войск или войск противника);

− контроль за любыми излучениями электромагнитного спектра частот.

Управление задействованием электромагнитным спектром частот предполагает планирование, координацию, распределение и руководство совместным использованием электромагнитного спектра частот объединенными силами ВС США при решении всех боевых (оперативных), инженерных, тыловых и административных задач [3].

К обеспечению управления задействованием электромагнитного спектра частот относится также и обеспечение электромагнитной совместимости РЭС – способности систем, вооружения и военной техники, аппаратуры, которые используют излучения электромагнитного спектра частот, работать в реальных условиях эксплуатации и предполагаемой оперативной обстановке с требуемым качеством при воздействии на них непреднамеренных помех или от предпринимаемых противником ответных действий, то есть способность одновременной работы РЭС и осуществления обмена информацией без взаимного недопустимого влияния [3].

Одним из важных мероприятий по управлению задействованием электромагнитного спектра частот является перепрограммирование сил, средств, задач и способов РЭБ, которое включает в себя заранее спланированные изменения в порядке применения сил и средств РЭБ, а также способов и тактики обнаружения и подавления цели, в ответ на действия противника и с целью обоснованного и эффективного изменения сил, средств и задач РЭБ, тактики действий или радиоэлектронной обстановки. Эти изменения могут быть результатом преднамеренных действий, в части касающейся своих ВС, ВС противника или третьей стороны, либо могут быть вызваны возникновением взаимных радиоэлектронных помех или другого непреднамеренного воздействия и изменений обстановки [3].

Важным элементом радиоэлектронной защиты является контроль излучений, который заключается в избирательном и контролируемом использовании электромагнитной, акустической и других видов энергии с целью оптимизации боевых возможностей управления, связи, разведки и действий сил информационных операций, снижения эффективности разведки противника, устранения взаимных радиоэлектронных помех, обеспечения электромагнитной совместимости РЭС, успешной реализации планов военной дезинформации и психологических операций.

Средства и методы радиоэлектронной защиты можно условно разделить на три типа [4]:

− непосредственной защиты РЭС;

− обеспечения электромагнитной совместимости РЭС на пунктах управления и в боевых порядках войск;

− радиоэлектронной защиты при проведении информационных операций.

Задачами средств и методов непосредственной защиты РЭС в операции могут быть [4]:

− защита РЭС своих войск от преднамеренных радиоэлектронных и оптико-электронных помех противника;

− защита РЭС своих войск от случайных атмосферных, промышленных помех, непреднамеренных помех от РЭС гражданских ведомств и союзных войск;

− защита РЭС, боевой техники, систем оружия и личного состава своих войск от радиоэлектронной дезинформации противника;

− защита боевой техники, объектов, пунктов управления (ПУ), РЭС, систем оружия, боеприпасов от самонаводящегося на радиоэлектронные излучения оружия противника;

− защита объектов, ПУ, РЭС и войск от летальных и нелетальных средств излучения направленной энергии.

Средства и методы обеспечения электромагнитной совместимости РЭС на ПУ и в боевых порядках войск призваны обеспечить защиту РЭС своих войск от взаимных помех при подготовке и в ходе операции частей и подразделений ВС США и союзных войск, в том числе от помех средств радиоэлектронных атак, используемых для подавления РЭС противника.

Задачами средств обеспечения электромагнитной совместимости РЭС на пунктах управления и в боевых порядках войск являются [4]:

− отслеживание и выдача рекомендаций на использование радиочастот и режимов работы различных РЭС в интересах исключения их взаимных помех;

− оценка нанесенного ущерба используемому спектру радиочастот и текущей радиоэлектронной обстановки;

− ведение радиоэлектронной разведки (РЭР).

К задачам сил и средств радиоэлектронной защиты при проведении информационных операций следует отнести [4]:

− информационную и радиоэлектронную защиту средств разведки, средств РЭП;

− радиоэлектронную защиту подразделений и средств РЭБ;

− информационную защиту сил и средств психологических операций;

− информационную защиту сил и средств, ведущих сбор, передачу и обработку собственной информации.

Радиоэлектронное обеспечение информационной операции включает в себя мероприятия и средства, своевременно обеспечивающие разведывательные потребности штабов войск по выявлению и оповещению об угрозах, их немедленному распознаванию, оценке

оперативной и радиоэлектронной обстановки, своевременному принятию оперативных решений, планированию операций, а также выработку данных, необходимых для целеуказания средствам поражения и воздействия в интересах радиоэлектронной атаки и защиты [2].

Фактически радиоэлектронное обеспечение представляет собой действия, направленные на обнаружение, идентификацию и определение местоположения РЭС противника, которые могут являться как источниками получения разведданных, так и источниками информационных угроз [8, 10].

Контроль радиоизлучений, радиоэлектронная маскировка и программирование средств РЭБ, хотя формально и не являются составными элементами радиоэлектронной борьбы, однако обеспечивают эффективность ее ведения.

Контроль за излучениями различных видов электромагнитной энергии предполагает круглосуточное обеспечение строгого выполнения установленных нормативов электромагнитного излучения войсками и техническими средствами в местах их постоянной дислокации, на учениях, а также при подготовке и в ходе проведения операций. При этом обычно контролируются мощность, характер, направленность и виды излучений, а также соблюдение установленных правил радиообмена и скрытного управления войсками (силами) [4].

Целями радиоэлектронной маскировки являются [4]:

− маскировка излучений объектов, боевой техники и РЭС в местах их постоянной дислокации, на учениях, при подготовке операций;

− введение противника в заблуждение относительно истинных режимов излучений электромагнитной энергии;

− выявление демаскирующих радиоэлектронных признаков объектов, боевой техники и войск в местах их постоянной дислокации, на учениях, при подготовке и в ходе проведения операций;

− принятие мер по минимизации и (или) исключению нарушений радиоэлектронной маскировки;

− обучение личного состава ВС методам радиоэлектронной маскировки в местах постоянной дислокации, на учениях, при подготовке и в ходе ведения боевых действий ВС и их союзников.

Задачами перепрограммирования средств РЭБ являются [4]:

− обеспечение своевременной нацеленности средств РЭБ, организации способов радиоэлектронных атак и защиты согласно установленной командованием приоритетности целей и объектов;

− реализация своевременной перестройки указанных средств в соответствии с изменением оперативной (боевой, радиоэлектронной) обстановки;

− достижение максимальной эффективности (по мощности, направлению, виду, типу радиоэлектронного обеспечения) радиоэлектронных атак и радиоэлектронной защиты при изменении формы, вида и характера электромагнитного излучения цели (объекта) и совершении целью (объектом) маневра;

− своевременное резервирование, замена излучающих средств и дублирование их при выходе из строя или уменьшении эффективности средств РЭБ, радиоэлектронных атак и защиты.

Планирование РЭБ, которое подразделяется на долгосрочное и краткосрочное, носит централизованный характер, а ее ведение – децентрализованный [2].

В ходе планирования радиоэлектронных атак, радиоэлектронной защиты и радиоэлектронного обеспечения определяются [2]:

− порядок обеспечения электромагнитной совместимости РЭС и защиты от радиоэлектронных излучений личного состава, объектов и боевой техники;

− способы разрешения конфликтных ситуаций по: устранению случайных и непреднамеренных помех, маскировки и РЭР, радиоэлектронной безопасности, РЭП и перепрограммирования средств РЭБ в ходе операции;

− способы контроля излучения РЭС, применения летального и нелетального оружия, разведывательного обеспечения сил и средств РЭБ и их сопряжения со средствами разведки.

В решении на применение сил и средств РЭБ учитываются вопросы, связанные с возможностью использования группировками войск (многонациональными силами) гражданских средств связи, навигации и опознавания.

Составными элементами сил радиоэлектронного обеспечения ведения РЭБ ВС США являются средства [3]:

− радиоразведки (сбора, обработки, анализа и оценки разведывательных данных);

− РТР, то есть разведки электромагнитных излучений, не относящихся к средствам связи (сбора, обработки, анализа и оценки);

− обеспечения радиоэлектронной безопасности и скрытности использования радиоэлектронных систем, средств и информации.

Средства РРТР, обеспечивающие ведение РЭБ, могут быть использованы и для сбора данных, необходимых для дополнения добытых РЭР национального уровня информации.

В ВС США их силами решается более широкий спектр задач, в том числе [3]:

− распознавание угрозы и оповещение войск и штабов о применении сил и средств РЭБ противника;

− пеленгование целей и объектов РЭБ;

− сбор, обработка, анализ, подготовка и распределение разведданных, необходимых для немедленного принятия определенного (боевого) решения, в том числе уклонение от угрозы, выдача целеуказаний и целенаведение.

Вместе с тем органы ведения РЭБ и разведывательные органы применяют одни и те же средства РРТР. Различие в их использовании заключается в первоочередности применения добытой информации, степени ее анализа и детализации, а также в продолжительности времени ее проведения. Их сходство (подобие) – в добывании данных, необходимых командиру для определения первоочередных потребностей и принятия решения [3].

1.2. Совершенствование структуры подразделений сил РЭБ ВС США в условиях перехода к концепции сетецентрических войн

Постоянное повышение требований к системам разведки и РЭБ, а также появление новой концепции сетецентрической войны стало основой революционного развития РЭБ в конце XX – начале XXI века. Это привело к изменению характера радиоэлектронной борьбы, ее содержания, состава сил и средств, роли, места, цели и задач в операциях. Эти факторы предопределили создание новых средств РЭБ, в том числе скрытного радиоэлектронного подавления, летального и нелетального оружия и средств борьбы с другими видами излучения направленной энергии, средств подавления и поражения, действующих на новых физических принципах, а также информационно-технических воздействий, предназначенных для атаки на компьютерные сети [2].

К настоящему времени аналитиками Пентагона отмечается, что в современных условиях именно радиоэлектронная борьба является основой информационной войны на военном уровне, а развитие теории "информационных операций" является базой для ведения такой войны [2].

Ключевые концепции строительства сухопутных войск (СВ) США XXI века нового типа и задачи РЭБ по подавлению систем боевого управления противника определены рядом документов КНШ и командования армией США [2]:

− меморандум Joint Vision 2020 (2000);

− стратегия – The Army Transformation Strategy (2001);

− уставы КНШ: JP 3–13.1, JP 3–51;

− уставы сухопутных войск: FM 2–0, FM 3–0, FM 2–19.301/ST, FM 2–19.401/ST, PM2–40.1/8T и др.

В настоящее время одним из основных руководящих документов в области РЭБ является наставление КНШ JP 3–13.1 Electronic Warfare ("Радиоэлектронная война") 2007 года. Кроме то-

ОГЛАВЛЕНИЕ

УЧЕБНОЕ ИЗДАНИЕ

РАДИОЭЛЕКТРОННАЯ БОРЬБА В ВООРУЖЕННЫХ СИЛАХ США

Підписано до друку 27.11.2023 р. Формат 60x84 1/8.
Друк цифровий. Папір офсетний. Гарнітура Newton.
Ум. друк. арк. 16,5. Тираж 100 прим.

Видавничий дім « С В А Р О Г »
вулиця Гната Юри, 9
м. Київ 02105

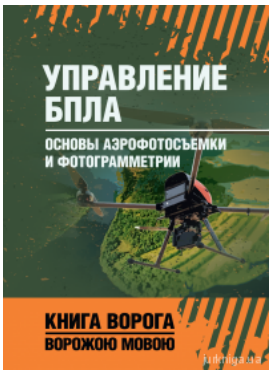
Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру
видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2581 від 10.08.2006 р.

Книги, які можуть вас зацікавити

Организация противодействия малым БПЛА. Книга ворога ворожою мовою

Забезпечення особистої кібербезпеки військовослужбовця

Обеспечение защиты от FPV дронов автомобильной техники, БТРов и танков. Книга ворога ворожою мовою



Управление БПЛА. Основы аэрофотосъемки и фотограмметрии. Книга ворога ворожою мовою

Аналитика БПЛА ВСУ. Книга ворога ворожою мовою

Засоби спостереження та ведення розвідки

Перейти до галузі права
Військове право