Радиоэлектронная борьба в сложной электромагнитной обстановке

Горбачев
Юрий Емельянович,
ведущий научный сотрудник НИИ МО,
к.в.н., доцент, полковник в отставке,
участник ВОВ

Введение

В конце XX и начале XXI веков в военной терминологии США и НАТО появилось несколько новых терминов, связанных с дальнейшим развитием перспективных информационных технологий, которые нашли свое отражение в основных документах и уставах. К таким терминам можно отнести следующие: «Информационные операции» (Information Operations); «Информационная обстановка» (Information Environment); «Стратегия действий в информационной обстановке» (Strategy Operations in the Information Environment); «Информационное поле боя» (Information Battlefield); «Информационно-сопряженные боевые возможности» (Information-Related Capabilities); «Операции в компьютерных сетях» (Computer Network Operations); «Электромагнитная обстановка» (Electromagnetic Environment) и некоторые другие термины, развивающие стратегию и доктринальные положения ВС США и ОВС НАТО. Так, например, в июне 2016 года министр обороны США Э. Картер в предисловии к одному из официальных документов МО США отметил, что, хотя термин «информационная обстановка» (Information Environment) и является относительно новым термином, он не заменяет понятие «Информационное поле боя» (Information Battlefield), а оценка информационной обстановки является важной частью военного планирования организации и ведения боевых действий. Далее он отметил, что в истории войн командование ВС всегда изыскивало возможность достижения преимущества над противником путем оказания влияния на восприятие им информационной обстановки, на ее оценку и на принимаемые противником на этой основе решения. Он также отметил, что сегодня информация является мощным инструментом влияния на противника, поэтому ВС США должны быть хорошо подготовлены к синхронизации и интеграции различных информационных программ и планов ее применения как составной части усилий ВС и правительства США.

Возникновение сети Интернет, увеличение возможностей радиосвязи, обширное влияние социальных медиасредств на информационную обстановку сегодня представляет новый комплексный вклад, который изменяет характер и создает новые сложные проблемы при подготовке и осуществлении военных действий.

1. Информационная обстановка. Содержание. Влияние на боевые действия. Электромагнитная обстановка как важнейшая составная часть информационной обстановки

Уставы ВС США определяют информационную обстановку как «… Состояние информационной сферы в районе боевых действий, которая является совокупностью деятельности людей, организаций, систем и средств, которые собирают, обрабатывают, распространяют и излучают электромагнитную энергию или используют в тех или иных целях информацию. Сама информационная сфера является глобальной, недоступной сферой, в которой люди и автоматизированные системы ориентируются, осуществляют слежение (наблюдение за излучениями и информацией), фиксируют информационную обстановку, принимают на ее основе решения, а также осуществляют свою деятельность на основе добытой информации, своих интеллектуальных способностей и имеющихся научных знаний».

В XXI веке создалась возможность использовать информационную обстановку различными способами: искажать или видоизменять ее, разрушая тем самым или нарушая работу систем разведки и управления; вести пропаганду и распространять дезинформацию, способствуя тем самым организации действующей оппозиции и созданию внутригосударственного инакомыслия; оказывать серьезное влияние на устойчивость и качество работы информационных систем и компьютерных сетей, вызывая дополнительные финансовые расходы государства; способствовать созданию видимости и законности этих действий, одновременно дискредитируя законность действий вероятного противника. Возможность информационного воздействия противника на информационную инфраструктуру США, как отмечал Э. Картер, в том числе имея в виду и структуру государственных и негосударственных субъектов, потребовала от ВС США разработки стратегии действий в информационной обстановке и стратегии проведения информационных операций с целью обеспечения консолидации и сбалансированности информационной деятельности ВС, достижения эффективной интеграции усилий МО в динамической информационной обстановке, адаптации к новым технологиям и социологическим изменениям, обеспечения достижения и удержания информационного превосходства над любым противником с акцентом на успешное решение задач в области подготовки личного состава ВС США, а также решения политических задач и обеспечении партнерства с союзниками.

Таким образом, подводя итог, можно сказать, что информационная обстановка — это как бы совокупный результат деятельности электромагнитных устройств, автоматизированных систем управления,

информационных и компьютерных сетей, людей и потоков информации в определенном районе военных действий в физической, информационной и когнитивной областях.

Оценка информационной обстановки, заключает министр обороны США, как бы является путепроводом, оказывающим влияние на принимаемые оперативные решения, являясь при этом основным компонентом оценки оперативной обстановки, весьма необходимым для принятия решений командиром. Она также позволяет решать проблемы, взаимосвязанные между собой, в физической, информационной и когнитивной областях, эффективно использовать в военных действиях информационно-сопряженные боевые возможности видов ВС; минимизировать аналогичное воздействие на свои ВС, включая различные информационные формы и способы как самого воздействия, так и его познавательной части, состоящей из отношений людей, их верований, восприятия ими информации, с учетом того, кто передает, получает информацию, отвечает или реагирует на изменения информационной и оперативной обстановки. Все это связано с тем, что деятельность личного состава ВС взаимосвязана во всех областях и оказывает взаимное влияние на конечные результаты обстановки и в целом на успешность военных действий. В физической области информационной обстановки это сказывается на устойчивости систем и объектов управления и разведки и их адекватности реальной обстановке, возможности эффективной организации и использования информационно-сопряженных боевых возможностей ВС. При этом, подчеркивает министр, необходимо учитывать, что киберсфера также является составной частью глобальной информационной сферы и также состоит из взаимосвязанных систем и средств, созданных на базе информационных технологий, инфраструктур и обеспечивающих их информационными данными, включая компьютерные сети, встроенные в них процессоры и управляющие устройства. При этом операции в киберсфере также воздействуют на физическую, информационную и когнитивную области.

Когнитивная часть информационной обстановки определяется восприятием ее состояния и работоспособностью, а также способностью людей адекватно оценивать и принимать правильные решения, рационально использовать информационно-сопряженные боевые возможности ВС, правильно реагировать на изменения обстановки.

Значение истинного (реального по времени и месту) состояния информационной обстановки необходимо для своевременного и эффективного проведения информационных операций и использования ее сил. Это прежде всего действия по обеспечению: безопасности действий войск (OPSEC), военной дезинформации (MILDEC), операций военного информационного обеспечения (MISO), электромагнитной войны (EW), кибероперациий (КО), операций в компьютерных сетях (CNO) и специально-технических операций (STO), а также усилий интеграции и синхронизации всех сил в информационной операции (IO). Информационные операции являются интегрированной составной частью военных действий, в которых используются информационно-сопряженные возможности видов ВС, как для оказания влияния на противника, так и для защиты своих ВС, в том числе для обеспечения эффективной киберэлектромагнитной деятельности ВС США.

Возникновение новой (закрепленной уставами и наставлениями ВС США), пятой по счету, информационной сферы, равнозначной другим сферам деятельности ВС (космической, воздушной, наземной и морской), оказало значительное влияние на дальнейшее усложнение информационной обстановки. Ее часто в документах США именуют «электромагнитной обстановкой» (Electromagnetic Environment), а все связанное с использованием электромагнитной энергии, в той или иной ее форме, именуют «Киберэлектромагнитной деятельностью» (Cyber Electromagnetic Activity).

Вышеперечисленные новые термины свидетельствуют о дальнейшем развитии военной теории, связанной с использованием излучений электромагнитной энергии в современных операциях, с интеграцией и синхронизацией всей киберэлектромагнитной деятельности ВС США и ОВС НАТО, что ведет к дальнейшему значительному усложнению электромагнитной обстановки, которая является составной частью информационной обстановки. Это объясняется тем, что все информационные системы и средства, киберсети и киберустройства имеют элементы, использующие излучения или прием электромагнитной энергии, а действия в информационной сфере оказывают влияние не только на эффективность мероприятий в этой сфере, но и на характер обстановки в других сферах военной деятельности.

Уставы и наставления ВС США 2014 года издания определяют киберэлектромагнитную деятельность ВС США как «…..Деятельность по интеграции и синхронизации действий ВС по захвату, обеспечению превосходства, удержанию, сохранению преимущества и использованию выгодных условий над любым противником в информационной, киберсферах и в электромагнитном спектре при одновременном лишении возможностей противника эффективно использовать информационную и киберсферу, а также электромагнитный спектр, в условиях обеспечения аналогичной защиты своих ВС.

Согласно уставам ВС США, киберэлектромагнитная деятельность обеспечивает решение следующих основных задач:

- проведение кибероперациий и операций в информационных сетях;
- ведение электронной войны;
- управление электромагнитным спектром (планирование; распределение; координация; эксплуатация; устранение конфликтных ситуаций; управление информационными органами, силами и средствами; контроль излучений);
- интеграция и координация всей киберэлектромагнитной деятельности ВС.

Другие конкретные факторы, влияющие на повышение сложности электромагнитной обстановки, будут рассмотрены ниже.

2. Изменение форм и способов вооруженной борьбы и их влияние на электромагнитную обстановку

Большое внимание на характер и способы ведения боевых действий в операциях XXI века в условиях сложной электромагнитной и оперативной обстановки уделяется и за рубежом, особенно в США[19, 22, 24, 26]. Так, например, начальник центра ИО ВС США Д. Борк на страницах военного журнала изложил новую концепцию «Ведения войны в электромагнитном спек-

тре», которая в 2009 году была разработана Объединенным стратегическим командованием ВС США. По мнению Д. Борка, эта концепция должна заменить концепцию «Электронной войны (ЭВ)». Суть ее — связать в единое целое роль и функции ЭВ с использованием электромагнитного спектра (ЭМС), обеспечив свободный доступ для США в ЭМС и эффективное ведение ЭВ в интересах достижения информационного преимущества ВС США над любым противником. Еще в 2010 г. руководство МО США вплотную приступило к изучению и исследованию этой новой проблемы с целью создания новой организационной структуры войск, обучения и оснащения ВС, интеграции усилий ЭВ и управления ЭМС в операциях XXI в. [24].

В июне 2013 г. этот же журнал15 опубликовал статью Д. Борка, которая констатировала факт, что стратегия ЭВ ВС США требует совершенствования и укрепления в связи с новой концепцией развития ВС США, предусматривающей создание маневренных командований СВ США и требующей интеграции средств ЭВ и «Операций в компьютерных сетях» (Computer Network Operation), а также интеграции всех других элементов информационных операций, проводимых под руководством единого центра обеспечения информационного превосходства ВС США.

3. Анализ уроков локальных войн в сложной электромагнитной обстановке

23 апреля 2015 г. председатель научного комитета МО США (Defense Science Board –DSB) Крейг Филдс12 доложил заместителю министра обороны США о результатах исследований опыта локальных войн по ведению военных операций в XXI веке в сложной электромагнитной обстановке. Исследования были проведены группой экспертов и специалистов аппарата МО и всех видов ВС под руководством комитета с участием приватных консультантов и представителей аппарата заместителя министра обороны США по приобретениям, технологиям и логистике (AT&L).

Исследования проводились в течение двух лет (в 2013 и 2014 годах). В докладе отмечается, что способность ВС США создавать и удерживать информационное превосходство в операциях XXI века (в целях обеспечения военно-политического успеха США) подвергнуто опасности в связи с возникновением серьезных недостатков, снижающих возможность эффективного решения задач ведения электронной войны, и, в связи с успехом, достигнутым вероятным противником в области ведения информационной войны (ссылка сделана на изучение опыта боевых действий в конфликтах 2002, 2004, 2006 годов в Ираке, Афганистане и в 2008 году в Грузии).

В докладе отмечается, что взгляд в будущее говорит о беспрецедентной скорости глобального размаха развития ультра-современных информационных технологий, увеличивающих значимость влияния ЭВ на успех операций.

К. Филдс доложил, что на основании выполненных исследований выработан ряд рекомендаций: организовано изучение имеющихся и создаваемых новых сил, средств и систем ЭВ, проводятся экспертизы их возможностей и оценка технической и оперативной эффективности на ближайший период в течение 20 лет. Так, в ходе исследований были выявлены и оценены путь и методы, позволяющие снизить или исключить некоторые из самых серьезных недостатков существующих систем и органов ЭВ ВС США, с учетом потребностей и возможностей действия ВС в сложной электромагнитной обстановке в операциях XXI века. При этом была также учтена необходимость динамичного управления войсками, ведения разведки, электронной войны и управления ЭМС в реальном или близком к реальному масштабу времени, при проведении сетецентрических операций, на основе создания единого информационного пространства, в условиях ведения боевых действий в воздушной, наземной, морской, космической и информационных сферах.

В докладе научного комитета МО США [12] предлагается создать систему, продолжить изучение, проверку и оценку эффективности ЭВ на основе осуществления, проверки и оценки оперативно-технических циклов ведения боевых действий на различных уровнях управления (стратегическом, оперативном и тактическом), с оценкой эффективности реализации различных мер, контрмер и с учетом возможных ответных действий вероятного противника. В докладе отмечается, что исследования этих циклов должны обеспечить выявление и учет важности и значимости взаимосвязей в операциях XXI века, оценку влияния ЭВ на ход и исход боевых действий во всех пяти боевых сферах, а также установление: взаимосвязи и взаимного влияния применения сил ЭВ на ведение разведки, наблюдение, целеуказание, управление ВС; мер совершенствования организации связи и информационного обеспечения, управления оружием, определения точного положения войск, навигационного обеспечения и согласования действий единых сил США с учетом места и времени их применения.

В докладе комитета также отмечается, что несмотря на то, что исследование создаваемых на ЭВМ и учениях войск циклов не может охватить все возможные способы ведения боевых действий в операциях XXI века, а также точно определить порядок их обеспечения и поддержки, в любом случае глубокое изучение результатов отработки этих циклов позволяет раскрыть и оценить возможную эффективность ЭВ, определить необходимый потенциал ЭВ, вскрыть существенные недостатки, риски и определить наиболее благоприятные условия ее ведения (как на индивидуальном техническом, так и на оперативном уровне), уточнить эффективность влияния ЭВ на ход и исход операции при ведении боевых действий типа «сила против силы» («force-on-force»). Анализ циклов дает также возможность определить эффективность ЭВ в условиях динамического управления ЭМС и необходимую организацию войск для обеспечения преимущества над вероятным противником. Все это позволяет определить способы снижения или исключения непреднамеренных (случайных) комплексных влияний электронных многофункциональных систем (в том числе и систем ЭВ) на оперативную и электромагнитные обстановки; выявить степень влияния ЭВ в сложной оперативной и электромагнитной обстановке операций XXI века на возможность достижения и удержания всестороннего (в том числе и информационного) превосходства над противником.

В этой связи научный комитет МО выработал несколько рекомендаций по следующим вопросам [12]:

1. Разработка и использование новых средств и систем ЭВ в наступатель-

ных и оборонительных операциях, в возможных потенциальных конфликтах XXI века (рекомендации касаются всех имеющихся и перспективных средств ЭВ во всем ЭМС).

2. Разработка и использование методов моделирования и имитации, необходимых для оценки возможного взаимного влияния сил и средств ЭВ своих ВС и ВС противника на успешность операции единых сил США.
3. Создание и совершенствование необходимой структуры сил и органов ЭВ и выделение достаточных ресурсов техники и личного состава, обучение и подготовка как специалистов, так и всего личного состава ВС.
4. Проведение специальных специфических испытаний и экспертная оценка эффективности применения сил ЭВ; оценка ее потенциально возможного влияния (преднамеренного и не преднамеренного) на электромагнитную и оперативную обстановку; определение необходимой ответной реакции на изменение обстановки (своих войск и войск вероятного противника) в операциях XXI века.
5. Формирование программ, учитывающих весь перечень разработанных рекомендаций на всех уровнях управлений МО, командований ВС, во всех звеньях управления, которые определены директивой МО США и другими документами1,16,22.

Как оценивает научный комитет МО, стоимость реализации предлагаемых рекомендаций составляют сумму в 2,3 миллиарда долларов (реализуемых по крайней мере в течении пяти лет до 2020 г.). Комитет указывает, что он понимает, что такие инвестиции будет трудно выделить в эру бюджетной сдержанности, однако их невыделение будет провалом в повышении боевых возможностей ВС США. Кроме того, невыделение финансов, нужных ВС, создает серьезные риски в обеспечении ВС США информационно-электромагнитного превосходства в операциях XXI века [12].

Научный комитет МО также отмечает, что в ходе исследования были вскрыты серьезные проблемы во всех пяти сферах ведения боевых действий и что они характерны для большинства видов и способов военных действий в операциях XXI века; превосходство США в области информационно-электронной технологии постепенно утрачивается, и необходим существенный набор инициатив, чтобы восстановить это преимущество ВС США.

Утрате превосходства, по мнению комитета, способствовали три фактора.

Во-первых, 25 лет пренебрежительного отношения к ЭВ на фоне завершения холодной войны. В результате США утратили свое подавляющее лидерство в перспективных технологиях.

Во-вторых, в XX веке произошла широкая международная миграция перспективных технологий и появилась возможность создания новой матчасти электроники, ее программного обеспечения, управляемой архитектуры построения электронных систем, а также организована подготовка и обучение специалистов ЭВ не только в странах с высоким уровнем развития науки и техники, но и в отдельных акторских коллективах и террористических группах.

В-третьих, стало ясно, что потенциальные противники, которые ранее могли только наблюдать наличие американского господства электроники на поле боя, получили возможность ее создания и предприняли тщательно организованные и хорошо обеспеченные финансами шаги по преодолению преимущества США в области информационно-электронной технологии.

В связи с этим научный комитет МО США предлагает:

- восстановить преимущество ВС США в возможных конфликтах XXI века, научиться динамично управлять ЭМС, исключить имеющиеся сегодня ситуативное осознание недостатков переполненного ЭМС и неумение динамично и эффективно его использовать; расширить диапазон использования ЭМС в сторону как высоких, так и низких частот;
- совершенствовать навыки специалистов по использованию и управлению ЭМС при ведении ЭВ в ходе операции в масштабе времени, близком к реальному; научиться эффективно применять программное обеспечение систем ЭВ в условиях динамичного управления ЭМС в операции;
- перейти к более широкому использованию сил и средств электронной атаки с целью увеличения конкурентоспособности США и эффективности ЭВ.

Можно предположить, что командование ВС США на основе рекомендаций Научного комитета МО продолжает работу по дальнейшему совершенствованию сил, средств и систем ЭВ, по выработке методов динамичного управления ЭМС в операциях единых сил США. Об этом свидетельствуют уточнение и издание в 2012–2014 гг. ряда новых, единых уставов КНШ ВС США и уставов видов ВС, которые не только упорядочивают и совершенствуют формы, способы, задачи ЭВ, но и уточняют ответственность должностных лиц в области ведения информационных операций, электронной войны, обеспечения безопасности и динамичного управления ЭМС в операциях единых сил США, а также интегрируют всю киберэлектромагнитную деятельность ВС США в мирное время, в чрезвычайной обстановке и в операциях XXI века [1,3–11].

О принятых мерах также свидетельствует изменение механизма и порядка формирования организационной структуры, интеграция руководства киберэлектромагнитной деятельностью ВС США. Так, на страницах военного журнала Д. Хайстед сообщает, что с 01.12.2013 г. в составе оперативного управления штаба Объединенного Стратегического Командования ВС США начал действовать новый орган управления J3-E, который обеспечивает: координацию всей киберэлектромагнитной деятельности (КЭМД) командования; динамичное управление ЭМС; анализ и планирование ЭВ в кризисной обстановке и операциях. По мнению специалистов США, деятельность этого нового органа (J3-E) не только будет охватывать подразделения штаба ОСК ВС США, но и обеспечит всестороннюю обработку информации; проведение экспертных оценок, а также разработку предложений командованию ОСК по своевременной организации КЭМД в боевой и повседневной деятельности ВС США, в том числе и в период возникновения кризисных ситуаций. В то же время на орган J3-E КНШ возложена координация киберэлектромагнитной деятельности всех единых сил США. Руководить органом J3-E будет бригадный генерал Р. Эванс. Являясь заместителем начальника отдела глобальных операций оперативного управления ОШ КНШ (J3MA), он будет помогать обеспечивать ситуационную боеготовность (стратегическую осведомленность), осуще-

ствление боевого управления, интегрированное планирование космических, ядерных и кибернетических операций, а также обеспечивать организацию ведения ЭВ и объединенное использование ЭМС в повседневной деятельности и в операциях ВС США [17, 18, 20, 22].

4. Факторы, повлиявшие на повышение сложности электромагнитной и общей информационной обстановки

К факторам, повысившим сложность электромагнитной и общей информационной обстановки, можно отнести:

- развитие систем и средств радио, радиорелейной, тропосферной, ионосферной и космической связи; радиолокации и радионавигации;
- расширение ЭМС в сторону низких и высоких частот;
- возникновение и развитие перспективной электронной (информационной) технологии и появление на этой основе информационно-сопряженных боевых возможностей ВС, в том числе развитие самонаводящихся на излучение ЭМЭ средств поражения;
- одновременное использование аналоговых и цифровых методов передачи информации;
- появление высокопроизводительных АСУ войсками, разведкой, оружием и боевой техникой;
- дальнейшее развитие и внедрение в ВС многих стран сил и средств ЭВ (РЭБ);
- расширение использования ЭМС различными силовыми структурами и гражданскими ведомствами, в том числе средствами массовой информации;
- возникновение информационных операций, интегрирующих использование сил, систем, средств и личного состава для обеспечения информационного превосходства своим ВС и затруднения использования ЭМС вероятным противником;
- возникновение новой сферы ведения боевых действий — информационной;
- отсутствие у информационной сферы четких границ в операциях по территории, по времени, по пространству — в отличие от других сфер;
- информационная сфера может одновременно охватывать не только сами районы боевых действий (своих ВС и ВС противника), но и важнейшие жизненно важные объекты и системы государственного значения, причем обеих противоборствующих сторон;
- военные действия в информационной сфере планируются, организуются и ведутся путем осуществления информатизации интеграции основных сил, в том числе и сил электронной войны;
- для ведения военных действий в информационной сфере не существует государственных границ и закрытых территорий;
- боевые действия в информационной сфере могут одновременно носить как локальный, так и глобальный характер;
- боевые действия в информационной сфере характеризуются потенциально высокой анонимностью и скрытностью действий, трудностью выявления агрессора, его принадлежности, используемого им информационного оружия и программно-математического обеспечения;
- ведение военных действий в информационной сфере может осуществляться с территории невоюющих, нейтральных, в том числе дружественных государств;
- подготовка к ведению боевых действий в информационной сфере может осуществляться заблаговременно, в том числе и в мирное время, не проявлять себя до особого сигнала;
- боевые действия в информационной сфере оказывают влияние, иногда решающее, на характер и способы действий, их эффективность, успешность ведения боевых действий в других четырех сферах (воздушной, наземной, морской, космической), на успешность операции в целом;
- боевые действия в информационной сфере могут предшествовать или сопровождать боевые действия в других сферах, а также являться способом побуждения начала или продолжения силовых военных действий, или вестись с целью заставить противника отказаться от ведения силовых военных действий, а также с целью устрашения противника и отказа его от своих намерений;
- боевые действия в информационной сфере могут обеспечить достижение и удержание информационного превосходства над противником, сократить потери и сроки проведения операции, обеспечить достижение поставленных военно-политическим руководством целей, сократить временной цикл подготовки и принятия решений и обеспечить упреждение действий и намерений противника;
- боевые действия в информационной сфере создают благоприятные условия для принятия и осуществления военных и политических целей государства, иногда даже без необходимости использования физической силы;
- действия в информационной сфере не имеют аналогий с опытом ведения боевых действий в других сферах, так как они оказывают комплексное когнитивное, информационное и физическое воздействие на ВС, участвующие в подготовке и ведении боевых действий во всех пяти сферах.

По взглядам ряда военных специалистов США и других стран НАТО, лишение возможности использования 50% и более своих информационно-управляющих сетей войсками, боевой техникой, оружием и разведкой является побуждением к отказу от начала и продолжения боевых действий в других сферах и операции в целом.

Таким образом, в операциях XXI века возникли не только новые технические и природные факторы, повлиявшие на сложность восприятия и оценки электромагнитной обстановки, но и новые оперативные факторы, связанные с тем, что бóльшая часть боевой техники и систем оружия передовых развитых стран имеют в своей структуре элементы, использующие излучение или прием электромагнитной энергии. Это, с одной стороны, значительно увеличило их дальность действия и точность нанесения ударов, а с другой — значительно повысило загруженность ЭМС. При этом устойчивость применения информационно-сопряженной боевой техники и систем оружия зависит от возможности свободного доступа к ЭМС и от степени его защищенности от воздействия противника. «Цифровизация вооруженных сил», создание единого информационного пространства в режиме времени, близком к реальному, осуществление «сетецентрических операций» — все это привело к к дальнейшему расширению и применению сущности информационной (и электромагнитной в частности) обстановки, затруднило ее восприятие, выдвинуло новые

требования и критерии ее оценки, ограничило время на оценку и принятие решений, а также возможность своевременной реакции на изменения обстановки.

Можно сказать, кроме того, что в XXI веке произошло смещение центра тяжести из физической в информационную и когнитивную области, повысилась еще значимость влияния электромагнитной обстановки на ход и исход военных действий. Своевременность и достоверность оценки состояния и изменения электромагнитной, информационной и оперативной обстановки в огромной степени оказывает влияние на возможность принятия адекватных и своевременных решений, что и будет определять возможность выполнения поставленных задач и достижения желаемой цели.

Рассмотрим теперь имеющиеся элементы схожести и различия терминологических понятий «Электронная война» и «Радиоэлектронная борьба», которые в военной литературе России зачастую не указывают и считают равнозначными несмотря на то, что ЭВ и РЭБ имеют разный состав, а их составные элементы имеют разные возможности, разные задачи и разные объекты воздействия и защиты. Да и их оперативно-стратегические и доктринальные положения различны.

Рассмотрим более детально определение ЭВ уставами ВС США, ее доктринальные основы и структуру, взаимосвязи ЭВ с другими доктринальными основами ВС США, задачи и состав каждого из составных элементов ЭВ, их объекты воздействия и защиты. Такой разбор сущности ЭВ позволит офицерам ВС России, знающим доктринальные основы, состав, задачи, объекты воздействия и защиты РЭБ, понять, в чем ЭВ и РЭБ имеют схожесть, а в чем они кардинально различаются.

Согласно уставам ВС США, ЭВ состоит из трех взаимосвязанных элементов: электронной атаки (Electronic Attack), электронной защиты (Electronic Protection) и электронного обеспечения (Electronic Support) [3, 8, 9, 10, 25, 26].

Электронная атака включает в себя использование следующих сил и средств: электромагнитных помех (активных и пассивных), в том числе средств и систем индивидуальной, коллективной и групповой защиты боевой техники и систем оружия; средств нарушения работы систем позиционирования, навигации и временных параметров; средств электромагнитной дезинформации; средств разового использования (ИК, активных и пассивных ложных целей и ловушек электромагнитного спектра); самонаводящегося на излучение оружия; средств и оружия направленной энергии. Под средством направленной энергии понимаются технические устройства нелетального воздействия, а под оружием направленной энергии — средства и системы, оказывающие летальное воздействие. Электронная атака включает в себя действия, направленные на предотвращение, снижение эффективности или ликвидацию возможности использования противником электромагнитного спектра; на снижение эффективности управления войсками, боевой техникой и оружием, путем применения средств систем и оружия, использующего электромагнитную или другие виды направленной энергии. Например — для создания помех с целью срыва, ухудшения или блокирования работы или уничтожения электронных средств и систем противника информационно-сопряженной боевой техники и оружия или для введения противника в заблуждение. Применение излучений электромагнитной или другой направленной энергии называется активной электронной атакой, а применение пассивных помех, ложных целей, дипольных отражателей и ловушек — пассивной электронной атакой. Силы и средства электронной атаки используются как в наступательных, так и в оборонительных целях, оказывая воздействие на электронные средства и системы, боевую технику, системы оружия, управления и разведки, объекты, а также на личный состав ВС противника[3, 8, 9, 10, 25].

Электронная защита включает в себя: управление электромагнитным спектром, обеспечение электромагнитной защиты; усиление защитных свойств объектов, РЭС и личного состава, различных систем и другого электронного оборудования, боевой техники и систем оружия против любых способов использования излучения электромагнитной энергии. При этом базируется ЭЗ на использовании атрибутов систем и процессов. Защита обеспечивается как от воздействия противника, так и от излучения электронных средств своих войск, нейтральных войск, естественных природных явлений и окружающей среды. Кроме того, составной частью электронной защиты является осуществление контроля за электромагнитными и другими излучениями, оказывающими влияние на успешность боевых действий. Электронная защита имеет также задачу обеспечения электромагнитной совместимости электронных средств и осуществления защиты, целераспределения, наведения, целеуказания и приведения в действие боевой техники и оружия [3, 8, 9, 10, 26].

Электронное обеспечение (Electronic warfare support или Electronic support) организуется и осуществляется под непосредственным руководством командира и имеет задачу поиска, наблюдения, перехвата, выявления наиболее важных целей, засечки координат или определения зон нахождения источников преднамеренных или непреднамеренных излучений электромагнитной энергии с целью немедленного распознавания угрозы, целераспределения и целеуказания, определения наиболее важных целей и объектов воздействия, оценки электромагнитной обстановки, подготовки предложений командованию для принятия решений, планирования и ведения электронной войны в предстоящих или будущих операциях. Электронное обеспечение позволяет адекватно оценить информационную и оперативную обстановки и эффективно выполнять оперативные задачи. Оно обеспечивает синхронизацию и интеграцию планирования ЭВ и адекватное оперативное использование разведывательных средств, процессов в рамках конкретной оперативной обстановки в целях снижения неопределенности: в намерениях и действиях противника; в оценке обстановки, в оценке временных параметров действий войск и использования местности. Данные, добытые силами и средствами электронного обеспечения ВС (ES) совместно с данными, полученными от органов АНБ (добывающего стратегические данные радио, радиотехнической и радиоэлектронной разведки), используются для целераспределения и целеуказания средствам ЭВ и огневого поражения, для выработки задач электронной и физической атаки, данных для инструментальной разведки (MASINT) [3, 7, 8, 10, 11, 22, 24, 26].

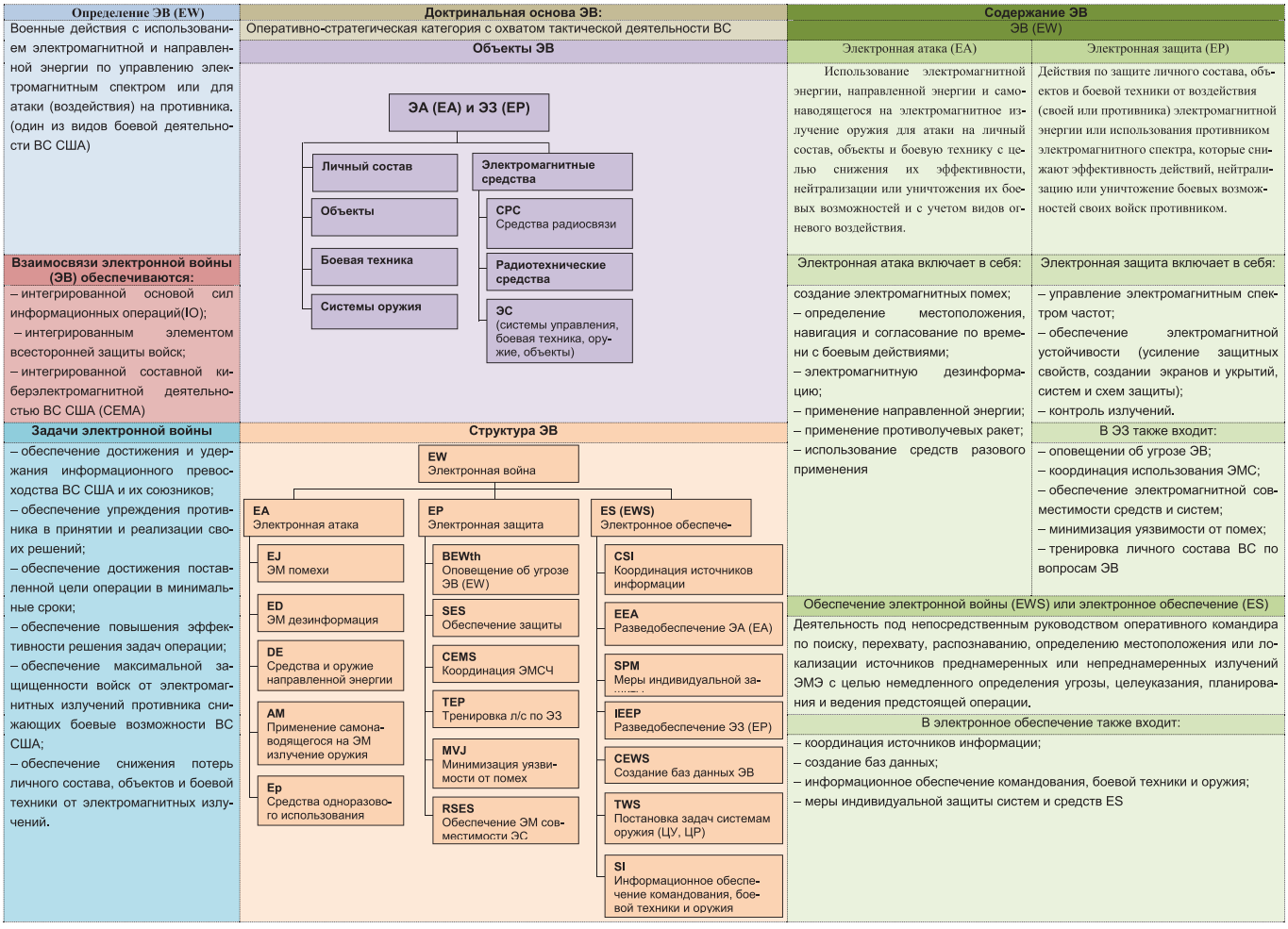

Рис. 1

Содержание, структура, задачи, объекты и взаимосвязи ЭВ ВС США приведены на рис. 1, из которого видно, что ЭВ является интегрированной составной частью информационных операций, элементом всесторонней защиты войск и киберэлектромагнитной деятельности ВС.

5. Развитие теории информационного противоборства

Этапы развития теории оперативного искусства, формы и способы оперативного и боевого обеспечения вооруженных сил, в том числе и РЭБ, определяются степенью развития теории военного искусства. Радиоэлектронная борьба образует теорию и практику обеспечения ведения боевых действий оперативно-стратегического и оперативного масштабов и объединениями видов ВС, в то время как электронная война в ВС США определяется как вид военных действий с использованием электромагнитной и направленной энергии.

Рассматривая этапы развития теории оперативного искусства (ОИ) в ВС РФ, военный энциклопедический словарь выделяет шесть этапов развития [32]:

- возникновение отдельных элементов ОИ — конец XIX — начало XX века;
- обобщение объекта ОИ и разработка теоретических основ — 1904–1924 гг.;
- развитие теории и практики ОИ — 1925–1940 гг.;
- дальнейшее развитие теории и практики ОИ с учетом событий второй мировой войны — 1941–1953 гг.;
- развитие теории и практики ОИ с учетом изменения ЯО и возможности достижения паритета в военной области — 1954–1989 гг.;
- развитие теории и практики ОИ под влиянием мировых военно-политических реформ в мире и в России — 1990–2007 гг.

Можно с достаточной степенью вероятности предположить, что во многом возникновение отдельных элементов РЭБ, обобщение опыта, разработка теоретических основ и их совершенствование до некоторой степени аналогично пятому и шестому этапам развития ОИ, но при этом РЭБ имеет и свои специфические особенности развития. Отдельные элементы РЭБ как вида боевого обеспечения возникли в 1904 г. и со сдвигом в несколько лет сформировались в единое целое. РЭБ прошла те же этапы развития теории и практики, что и ОИ. Основное отличие состоит в том, что первое практическое применение сил и средств радиоэлектронного подавления (РЭП) в интересах оперативно-стратегического и оперативного обеспечения относится к 1942–1945 гг., а развитие теории и практики, с учетом событий второй мировой войны и развития ВС СССР, относится к 1954–1989 гг. и последующим годам развития теории и практики развития ВС РФ.

На последнем этапе развития, в связи с развитием перспективных технологий (информационной, электронной, высокоточного оружия), с возникновением пятой равнозначной сферы ведения боевых действий — информационной сфе-

ры — РЭБ становится составной частью информационного противоборства, но остается видом оперативного обеспечения, и по-прежнему ее объектами воздействия и защиты остаются только радиоэлектронные средства и системы управления войсками, оружием и разведкой.

Если на первых этапах развития теории и практики ОИ и РЭБ, как ее составного элемента, развивались только когнитивная и физическая области, то начиная с четвертого этапа развития ОИ (когда в 1942 году были сформированы орган руководства РЭБ и четыре радиодивизиона «Спецназ») возникла новая сфера развития теории и практики ОИ — информационная.

РЭБ в ряде случаев стала принимать форму радиоэлектронно-информационную, носить в себе в какой-то мере элемент психологического противоборства.

Однако проблема соотношений категорий РЭБ, ИПБ, ОИ, решаемая средствами силового противоборства, возникла еще ранее. Так, возникший в 1954 г. термин «радиоэлектронное противодействие», измененный двумя годами позже на термин «радиоэлектронное подавление», был заменен в 1963 году на термин БРЭСП (борьба с радиоэлектронными средствами противника). Элементами БРЭСП являлись: РЭП, РЭЗ, применение самонаводящегося на излучение электромагнитной энергии оружия, нанесение ударов РВ и А по радиоэлектронным объектам и пунктам управления войсками и оружием, их захват, вывод их из строя или уничтожение силами десантных войск. В 1968 г. термин БРЭСП был уже заменен на современный термин РЭБ и в ВС РФ, и продолжилось создание теории, практики и войск РЭБ. Радиодивизионы «Спецназ», сформированные в 1942–1943 гг., были расформированы в 1945 г. Первый послевоенный батальон РЭБ был сформирован в г. Калуге в 1953–1954 гг.

Опыт локальных войн конца XIX и начала XX веков [14, 17, 18, 26] стал определяющим в области развития теории и практики ОИ, а вместе с ним и РЭБ. Бурное развитие информационных технологий и радиоэлектроники, резкое увеличение в вооруженных силах наиболее развитых государств информационно-сопряженной боевой техники и, прежде всего, высокоточного оружия, продолжающаяся милитаризация космического пространства, возникновение информационного оружия и элементов кибервойны, создание в ВС ряда стран кибервойск (киберкомандований) все это привело к возникновению пятой сферы ведения боевых действий — информационной сферы. Возникновение пятой сферы боевых действий стало возможным в связи с беспрецедентно быстрой миграцией по всему миру информационно-электронных технологий и технологий высокоточного оружия. С созданием единого информационного пространства, в масштабе времени, близком к реальному, с цифровизацией процессов управления ВС и с появлением сетецентрических операций ВС, ведение боевых действий в информационном пространстве приняло новую форму.

Все эти новые тенденции развития теории и практики ОИ изменили возможности ВС, формы и способы ведения боевых действий и РЭБ, изменили роль, задачи, значимость и субъекты вооруженного противоборства — со значительным сдвигом усилий в информационную сферу противоборства. Опыт локальных войн конца XX и начала XXI веков свидетельствует о том, что информационная сфера ведения боевых действий может не только являться самостоятельной сферой ведения боевых действий, но и оказывать влияние на ведение боевых действий в других сферах (воздушной, наземной, морской и космической).

В настоящее время в ВС ведущих зарубежных стран переизданы основные документы, определяющие стратегию и концепции информационной и электронной войны; введена новая оперативно-стратегическая категория «информационная операция», определены ее задачи и используемые силы и средства.

Так, в ВС США в 2000 г. был издан документ, определивший перспективы строительства, развития и использования в операциях XXI века ВС США на перспективу до 2020 г. В нем поставлена задача достижения и удержания превосходства над любым противником, в том числе и информационного превосходства [29].

В 2012–2014 гг. в ВС США были обновлены уставы «Информационные операции», «Электронная война», «Управление электромагнитным спектром», «Операции обеспечения безопасности единых сил на театре войны», «Обеспечение безопасности боевых действий», которые уточнили категории, задачи, формы и способы, состав сил информационных операций, в том числе и электронной войны, ведения боевых действий в условиях электронной войны и оперативного управления электромагнитным спектром.[3,11,13] Наметилась централизация руководством всей киберэлектромагнитной деятельностью. В этой связи были разработаны уставные документы, определяющие порядок руководства киберэлектромагнитной деятельностью. К таким уставам, например, можно отнести устав Армии ВС США «Киберэлектромагнитная деятельность», изданный и утвержденный 12.02.2014 г. [10]. Необходимо учитывать при этом, что киберэлектромагнитная деятельность осуществляется в трех областях — физической, информационной и когнитивной — и является совокупной деятельностью людей, систем, организаций и техники; предусмотрено ее перепрограм-мирование в операции [10, 13].

Устав определяет, что киберэлектромагнитная деятельность — это деятельность, направленная на захват, использование и удержание превосходства над вероятным или действующим противником в информационно-телекоммуникационном пространстве, информационном пространстве и в использовании электромагнитного спектра при одновременном снижении или лишении возможности противника совершать аналогичные действия [10].

В 2013 г. в объединенном стратегическом командовании ВС США были объединены органы ведения электронной войны и управления электромагнитным спектром, а для единого руководства ими учрежден в оперативном управлении штаба ОСК орган единого руководства киберэлектромагнитной деятельностью в операциях — под руководством заместителя начальника оперативного управления штаба ОСК (J3E) [16].

Под руководством председателя КНШ США В. Гётней (W. Gortney) была разработана обновленная доктрина электронной войны для операций единых сил [2, 8].

Доктрина определила такие стратегические категории, как: «операции в электромагнитном спектре»; «руководство боевыми действиями в электромагнитном спектре»; «управление операциями в электромагнитном спектре»; «взаимосвязь электронной войны с ведением кос-

мических, кибернетических и навигационных операций, борьбы с системами управления, определения местоположения, времени и параметров действий единых сил США».

В развитие положений этой доктрины в марте 2014 г. была издана директива МО США 3224.4, определившая основные направления стратегии электронной войны и обязанности основных должностных лиц единых сил США в этой области.[1]

Обновление доктрины электронной войны было связано с изменением характера боевых действий в операциях (локальных войнах) начала XXI века, с возникновением пятой, равнозначной другим сферам ведения боевых действий, закрепленной впоследствии уставами ВС США, с влиянием характера и способов ведения боевых действий в этой новой, информационной, сфере на ведение боевых действий в других сферах, с возможностью ведения боевых действий только в информационной сфере и со сложностью электромагнитной обстановки, ставшей важнейшей частью информационной и оперативной обстановок и во многом их определяющей [17].

6. Коренные отличия сущностей Электронной войны и РЭБ

Кроме Российских, Американо-натовских взглядов в мире существует еще одна теория ведения информационного противоборства и, как составная часть его, теория радиоэлектронной борьбы в операциях XXI века — Китайская.

Следует отметить, что теоретические основы Китая сформировались на основе его исторической стратегии, а также за счет знаний, приобретенных китайскими специалистами в ходе обучения их в военных учебных заведениях СССР. Много взято им и из опыта использования сил и средств ЭВ США и НАТО в локальных войнах конца XX и начала XXI веков. Именно поэтому китайская теория ИВ и РЭБ, в частности, имеет некоторые совпадения с теориями США и России. Однако у нее имеются и свои характерные отличия.

Китайские специалисты свою теорию ИВ образно сравнивают с увеличением силы тигра за счет придания ему крыльев (…«она подобна добавлению крыльев тигру»). Есть в Китае и другое образное сравнение и определение ИВ: «…ИВ своего рода война научных знаний».[27,28]

В конце XX и начале XXI века в Китае было опубликовано большое количество научных трудов, охватывающих как историческое прошлое, так и события XX века и начала XXI-го, которые связаны в той или иной мере с ведением информационного противоборства, радиоэлектронной борьбы и электронной войны на различных театрах военных действий. Эти труды отражают несколько важных обстоятельств.

Во-первых, в Китае были завершены исследования в области специфической (особой) китайской теории информационной войны, которые соответствовали культурным, военным и экономическим особенностям ведения боевых действий и развития теории ИВ.

Во-вторых, китайские военные специалисты изучили и использовали опыт, накопившийся ВС США и ВС СССР (РФ), в создании и развитии своей теории и практики ведения ИВ (информационного противоборства). Были использованы также знания, приобретенные в области теории, создания и использования средств радиопомех (радиопротиводействия) в военных вузах СССР.

В-третьих, военная доктрина и стратегия Китая оказала сильное влияние на содержание китайской теории ИПБ и РЭБ. Китай быстро интегрировал положения теории ИПБ и РЭБ ВС РФ, теории ИВ и ЭВ США в свою теорию ИВ, с учетом теории «Народной войны» Мао Дзедуна, а также с учетом независимости и разветвленности «сетевых сил» (войск связи) видов ВС НОАК (СВ, ВВС и сил обеспечивающих ВМС), и с учетом, 36 китайских «хитрых» способов ведения войны, превратив ее в своеобразную теорию Китая по построению и использования сил ИВ, и РЭБ в частности.

Китайская военная наука определяет сегодня содержание «информационной войны», в том числе и радиоэлектронной борьбы, исходя из условий своего исторического развития, а также влияния, оказываемого на развитие этой теории и практики в США и России. В этой связи, китайская теория ИВ и РЭБ, хотя и отличается от теории ИВ, ИПБ, ЭВ и РЭБ (США и России), все-таки имеет тождественность по некоторым позициям, особенно в практике их осуществления в мирное и военное время. Основные отличия теории Китая касаются форм, способов и сущности реализации основных положений стратегии и тактики, характерных черт и принципов ведения ИВ и РЭБ.

Необходимо отметить, что различия и некоторые характерные особенности указанных трех теорий, в определенной степени схожих по своей сущности, целям и практики реализации, были отмечены специалистами США. Так, начальник отдела анализа перспективных боевых возможностей (аппарата Директора национальной разведки США Роберт Броз (Robert Brose)[18], на основе исследований, проведенных в 2013 и 2014 годах, подготовил в 2015 году доклад аппарата директора национальной разведки США Конгрессу с оценкой взглядов трех государств в сфере сущности теории информационной войны. Основной целью документа является изучение и разъяснение существующих различий в доктринальных подходах США, России и Китая по организации и ведению информационной войны (информационного противоборства), в том числе электронной войны и радиоэлектронной борьбы. Документ содержит анализ сущности и возможностей информационно-телекоммуникационного пространства и всей информационной сферы для решения различных задач информационных операций, в том числе сущностей и возможностей электронного, психологического (когнитивного) и силового воздействия, осуществляемого в интересах достижения политических, экономических и военных целей государства.

Кроме того в докладе приводится сравнительная оценка доктринальных подходов военно-политического руководства различных стран, имеющих развитый электронный и кибер-потенциалы, обеспечивающие национальную информационную безопасность. При этом в докладе уделяется большое внимание изучению взглядов ВПР государств, связанных с использованием вооруженных сил государства, его информационным обеспечением, наличием нетрадиционных (гибридных) форм и способов организации и ведения вооруженного противоборства и применения так называемой «мягкой силы». В докладе дан анализ отдельных подходов России и Китая к правовым аспектам информационного противоборства с применением сил радиоэлектронной борьбы и электронной войны в операциях XXI века.

Доклад дает рекомендации, как выделить социально трансформируемое информационное и кибервоздействие из общей теории и перспективных технологий, которое значительно увеличивает важность всех видов и форм использования вооруженных сил в этой области; как трансформировать информационные и киберконцепции в существующие стратегические и оперативные концепции в операциях XXI века; как они реализуются в новых теориях Китая («United Front Theory», «Legal Warfare») и информационного противоборства России.

Рассматривая современную теорию ВС США «сетевой войны» (NETWAR) [18], являющуюся составной частью электронной войны (Electronic Warfare), Роберт Броз предлагает рабочее определение этой теории для операций XXI века, выделяя в нем термин «сетевая война». Сетевая война, по его определению, состоит из преднамеренных действий с целью оказания влияния на область человеческого восприятия (когнитивную область). В данном случае «сетевая война» не подразумевает использование физической силы. Применение силовых методов воздействия на противника обеспечивает использование других составных элементов «электронной войны», а также других сил информационных операций, при этом в информационных операциях осуществляется интеграция когнитивных, информационных и силовых методов ведения информационной войны.

Далее Роберт Броз детально анализирует китайскую и другие теории и делает заключение, что теория ведения информационной и кибервойны становятся все более переплетенными и взаимосвязанными в операциях XXI века.

Данная статья не имеет цели раскрывать и оценивать все перечисленные теории. Она сосредоточена на изучении влияния сложной электромагнитной обстановки на характер оперативной обстановки и ведения РЭБ в операциях XXI века, которое определяется бурным развитием перспективных технологий, их безмерно высокой миграцией по всему миру, особенностями информационной сферы, насыщением вооруженных сил электронно-сопряженной боевой техникой и оружием, а также исследованием использования отличительных особенностей электронной войны ВС США и радиоэлектронной борьбы ВС РФ. Острая необходимость показала важность определения схожести и различия сущности содержания, составных элементов, задач и объектов ЭВ и РЭБ. Это связанно с тем, что в военной и гражданской литературе РФ, зачастую и в научных трудах, не делают различия между терминами ЭВ и РЭБ, произвольно употребляют без всяких ограничений и замечаний один термин вместо другого. Такая произвольная, неадекватная замена терминов приводит к тому, что значительная часть личного состава ВС РФ, не имеющая прямого отношения к теории РЭБ, может быть введена в заблуждение, неправильно и неадекватно оценивать обстановку, как информационную, так и оперативную, что в итоге приведет к тому, что эти специалисты не смогут правильно определять имеющиеся боевые возможности, условия ведения операции, возможность выполнения задач операции, сроки ее проведения и возможные потери, а также возможность правильной организации радиоэлектронной защиты и радиоэлектронной маскировки. Все это может сказываться не только на оценке обстановки, но и на замысле операции, решении, принимаемом командующим, на планировании и ведении самой операции, на боеготовности ВС, организации обучения и подготовки личного состава ВС РФ.

В связи с этим необходимо более четко определить и широко обсудить на страницах военной печати схожесть и различия РЭБ и ЭВ, чтобы исключить неправильное употребление того или иного термина. Это определяется рядом факторов.

Во-первых, РЭБ и ЭВ являются доктринальными стратегическими и оперативными понятиями. РЭБ, согласно основным документам ВС РФ, является одним из видов оперативного (боевого) обеспечения.

Электронная война, согласно единым уставам ОШ КНШ ВС США, определяется как: «…Военные действия с использованием электромагнитной и направленной энергии для управления электромагнитным спектром и для атаки противника» [3–11].

То, что уставы ВС США определяют электронную войну, как один из видов военных действий, имеет сегодня особо важное значение. Так, современная военная доктрина ВС США рассматривает не четыре, как в наших уставах, а пять равнозначных сфер ведения боевых действий (воздушную, наземную, морскую, космическую и информационную). Это положение уже закреплено уставами ВС США.

Во-вторых, одним из составных элементов электронной войны ВС США является «обеспечение электронной войны» (Electronic Warfare Support — EWS, ES), которое выполняет задачи оперативной и тактической разведки. Задачи стратегической разведки выполняет Агентство Национальной безопасности МО США. Между органами ЭВ и АНБ существует тесное взаимодействие и осуществляется обмен данными разведки в масштабе времени, близком к реальному. Кроме того, одной из задач электронного обеспечения является оценка электромагнитной обстановки, разработка и доклад предложений по ведению ЭВ командующему (командиру) для принятия им решений. В составе органов РЭБ ВС РФ имеются лишь силы и средства обнаружения, опознавания объектов, подавления и наведения на них средств РЭБ. Основные данные о противнике в ВС РФ добывает стратегическая, оперативная, тактическая разведка, которая ведется силами видов ВС и силами центрального подчинения, а между органами разведки и РЭБ организован обмен данными.

В-третьих, такие составные элементы РЭБ и ЭВ, как «радиоэлектронное подавление» (радиоэлектронное поражение) ВС РФ и «электронная атака» ВС США, имеют разный состав, разные силы и средства, разные задачи, разные объекты воздействия и защиты, разные формы, средства и способы ведения. В состав «электронной атаки» ВС США входят силы, средства электромагнитного воздействия и средства и оружие направленной энергии, а в состав радиоэлектронного подавления ВС РФ средства и оружие направленной энергии не входят, а входят только средства функционального поражения РЭС и радиоэлектронных объектов. В ВС США имеются и комбинированные системы направленной энергии, которые на малых дальностях наносят летальный ущерб, а на больших дальностях — нелетальный.

Объектами воздействия «радиоэлектронного подавления» (радиоэлектронного поражения) ВС РФ являются только радиоэлектронные средства и радиоэлектронные объек-

ты. Этим положением определяются и задачи РЭБ в операции.

Объектами воздействия «электронной атаки» ВС США являются: электронные средства, электронно-сопряженная боевая техника и системы оружия, электронные объекты, узлы связи и пункты управления, а также личный состав ВС, независимо от того, обслуживает он или не обслуживает радиоэлектронные средства и объекты. Особым объектом считается личный состав, участвующий в оценке обстановки, принятии решений, планировании и руководстве ведением операции.

Необходимо также учитывать то, что в ВС США происходит интеграция всей киберэлектромагнитной деятельности, создаются единые органы планирования и руководства всей этой деятельностью в операциях, а также то, что «ЭВ», «операции в компьютерных сетях», «информационное обеспечение военных действий», «военная дезинформация», «обеспечение безопасности действий ВС» являются основными элементами информационных операций (которые, в свою очередь, являются формой ведения информационной войны). Потому употребление без оговорок и замечаний термина РЭБ вместо термина ЭВ и наоборот означает преднамеренное введение в заблуждение командующих (командиров) и личного состава, принимающего участие в оценке обстановки, в подготовке предложений для принятия решений, в планировании и руководстве ведением операций. В операциях XXI века, ведущихся в сложной электромагнитной обстановке, такая неадекватная замена терминов может привести к увеличению потерь техники и личного состава, к увеличению сроков осуществления операций, к невыполнению задач или их неуспешному решению, а в целом — к обострению обстановки и необходимости принятия новых оперативных решений.

Выводы

Какие можно сделать выводы о характерных особенностях ведения РЭБ в боевых действиях в сложной электромагнитной обстановке?

Во-первых, возникновение новой, пятой по счету, но равнозначной другим сферам сферы ведения боевых действий (правда, закрепленной пока доктринальными положениями уставов только в ВС США). С появлением пятой сферы боевых действий возникла необходимость оценивать электромагнитную и информационную обстановки не только в каждой из пяти сфер, но и общую для всех сфер обстановку с учетом возможного влияния на общую эффективность операции действий в пятой сфере.

Во-вторых, в ВС наиболее развитых стран осталось очень мало боевой техники и оружия, которые не имеют электронных устройств или средств, связанных с использованием для своего функционирования электромагнитной энергии. С одной стороны, увеличилась эффективность этих средств и систем, а с другой — увеличилась и их уязвимость от электромагнитного и кибервоздействия, усложнилась в связи с этим и электромагнитная, общая информационная и оперативная обстановки.

В-третьих, возникновение единого информационного пространства в реальном, или близком к реальному, масштабе времени, цифровизация ВС промышленно-развитых государств и формирование в них киберкомандований, появление сетецентрических операций — все это не только расширило информационную сферу ведения боевых действий, но и значительно осложнило сам процесс и оперативность ее оценки, принятия решения, планирования, постановки задач подчиненным войскам, а также осуществления контроля их деятельности, составной частью которой является оценка возможностей РЭБ в сложной электромагнитной обстановке.

В-четвертых, появление в ВС информационного оружия, организация и проведение кибероперации, интеграция в ВС США всей киберэлектромагнитной деятельности (появление органов управления киберэлектромагнитной деятельностью в оперативном управлении штаба объединенного стратегического командования ВС США), включающей в себя: ведение информационных и кибероперации; управление всем процессом в масштабе времени, близком к реальному, в том числе оценку обстановки; применение сил и средств электронной войны и кибертехнологий; динамическое управление электромагнитным спектром — все эти действия и мероприятия могут оказывать существенное влияние на организацию, планирование и ведение РЭБ и в целом операций в XXI веке.

В-пятых, существующая у нас тенденция произвольного толкования терминологических понятий ВС других стран, которым нет соответствующего перевода на русский язык, а также замена иностранных терминов своими терминами без пояснений и замечаний, может усложнить, а иногда и исказить как истинную картину информационной, электромагнитной, кибернетической обстановки, так и в целом картину общей оперативной обстановки, создать неопределенность в оценке состояния, намерений и боевых возможностей противника, а также в определенной степени определения истинного влияния средств электронной войны и РЭБ на боеспособность ВС в операции.

Так, например, хочется еще раз подчеркнуть, что употребление нашего термина «РЭБ» вместо американо-натовского термина «электронная война» может привести к тому, что личный состав, участвующий в оценке обстановки и подготовке предложений для принятия решений, может не знать, что в составе сил «электронной атаки» ВС США имеются средства и оружие направленной энергии, а также, что объектами воздействия и защиты для сил ЭВ будут не только радиоэлектронные средства, но и личный состав, боевая техника, системы оружия, объекты и пункты управления войсками, разведкой, боевой техникой и оружием. Учитывая также то, что оценку обстановки надо отслеживать и оценивать в масштабе времени, близком к реальному, последствия такой путаницы в терминологии может привести к серьезным последствиям.

В-шестых, отсутствие четких границ информационной сферы, динамичность ее изменения, наличие, зачастую одновременно, локального и глобального характеров информационной сферы, анонимность и сложность выявления акторов, использующих информационную сферу в своих целях, а также то, что боевые действия в информационной и киберсфере могут вестись до начала боевых действий в операции, в угрожаемый период и в мирное время, что они могут явиться побуждающим фактором для начала операции, ее продолжения или прекращения — все это является существенной особенностью, усложняющей оценку электромагнитной, информационной и оперативной обста-

новки, и может оказать значительное влияние на сущность и характер ведения операций в XXI веке, привести, как уже указывалось выше, к срыву или невыполнению задач операции, к увеличению потерь личного состава и боевой техники.

Чтобы обеспечить успешное решение задач РЭБ в операциях XXI в. в сложной электромагнитной обстановке, на наш взгляд, необходимо:

- продолжать исследования, связанные с новыми достижениями в области перспективных информационных технологий, влияющих на повышение сложности оценки электромагнитной обстановки в операциях в XXI в., с учетом тенденций в развитии в высокоразвитых странах сил и средств кибер и информационных операций, в том числе сил и средств электронной войны, а также с учетом ведения сетецентрических операций в едином информационном пространстве в масштабе времени, близком к реальному;
- детально проанализировать опыт ведения информационной войны в локальных войнах ВС США и ОВС НАТО в конце XX и начале XXI в., способы осуществления ВС США кибероперации, изучить и проанализировать задачи, которые они ставят перед своими киберкомандованиями.

Использованная литература

1. Директива МО США (USD-AT&L) 3222.04, «EW Policy» от 26.03.2014 г.
2. Директива Министра ВВС США, «AF Network Operations»,13.3, от 11.01.2008 г.
3. JP 1–02 «Department of Defense Dictionary of Military and Associated Terms», 2010 (As Amended trough 15.10.2015 г.)
4. JP 3–10 «Joint Security Operations in Theaters», 13.11.2014 г.
5. JP 6–01 «Joint Electromagnetic Spectrum Management Operating»,

20.03.2012 г.

6. JP 3–12 «Cyber Operations», 05.02.2013 г.
7. JP 3–13 «Information Operations», 27.11.2012 г., Incorporating Change 1, 20.11.14 г.
8. JP 3–13.1 «Electronic Warfare», 08.02.2012 г.
9. FM 3–36 «Electronic Warfare «, 09.11.2012 г.
10. FM 3–38 «Cyber Electromagnetic Activities», 12.02.2014 г.
11. ADP 3–0 «Unified Land Operations CEMA», 2012 г.
12. «Memorandum for Chairman, Defense Board», R. Stein, W. Delaney, 18.09.2013 г. «21-st Century Military Operations in a Complex Electromagnetic Environment».
13. «Army Regulation 525 – 15, «Software Reprogramming for CEMA»,

19.02.2016 г. штаб армий США.

14. CSBA «Восстановление американского превосходства в электромагнитном спектре», Б. Кларк, М. Гунцингер, 2015 г.
15. «The EMS is a maneuver space, and that maneuver space is our Ahilles hell», JED, 01.06.2013 г., J. Borque
16. «The Department of Defense of Strategy for Implementing the Joint Information Environment», National Defense Authorization Act, 18.09.2013 г.
17. IO Sphere, Summer 2013, Fall 2013 «Information Operating — 2020», R. Gabel, J. Drummond, R. McKinstry.
18. «Cyberwar, Netwar, and the Future of Cyberdefense», R. Brose. Office of the director of National Intelligence USA, summer 2013.
19. «Structure View of Electromagnetic Spectrum Warfare», JED, 01.10.2012, D. Borque, J. Noul (начальник центра информационных операций ВС США и редактор JED). 01.10.2012 г.
20. «Stratcom shifts gears on its joint EMS Support organizational structure», J. Haysted, JED, 01.12.2012 г. pp 15, 16.
21. «Cyber Electromagnetic Activities (CEMA)» a key to success in Unified Land Operations, Army, June 2012, pp 43–46, Grigsey, J. Howard, T. McWeel, G. Burheer.
22. «Joint EMS Operations in the Electromagnetic Operational Environment», CJCSM 3320.01c, 14.12.2012 г., N. Tyson RADM, USN, Vice Director J. S.
23. «USA Computer Network Operations — EW Proponent (USA CEWD)»,

US Army Combined Arms Center — Intellectual Center of the Army, 2011 г.

24. «Information Operations, Cyber Spectrum Operations, Conference (CPAWR)», 30.11–02.12.2010 г., JED, 01.10.2011 г., pp 84–90.
25. «Directed Energy- View in future», Air&Space Power Journal (ASPJ) №4, 2009 г., J. Skotty, J. Roby, ВВС США.
26. «Ведение электронной войны в информационной сфере в XXI в.» (EW in IS). J. Elder, стратегическая конференция ВВС США, июнь 2008 г. Обзор тезисов конференции.
27. «Chinese Military Studies IW», JED, 2003 г., № 280 at 1, p. 6.
28. MI, VII–IX, 2003, pp 22–26, Wang Jinghuai Lin Dong, T. Thomas «Китайский взгляд на информационную войну».
29. Меморандум ВС США «Joint Vision 2020», 2000 г.
30. ВПК № 10, 13–19 марта 2013 г., Материалы практической конференции «Военная безопасность России: XXI век».
31. ВПК № 9, 9–15 марта 2016 г., «Гибридная война требует высокотехнологичного оружия и научного обоснования», начальник ГШ ВС РФ В. Герасимов.
32. Военный энциклопедический словарь, Воениздат, 2007 г., МО РФ.