Макаренко С.И., Иванов М.С.

СЕТЕЦЕНТРИЧЕСКАЯ ВОЙНА
принципы, технологии, примеры и перспективы

Монография

С.И. Макаренко, М.С. Иванов

СЕТЕЦЕНТРИЧЕСКАЯ ВОЙНА –
принципы, технологии, примеры и перспективы

Санкт-Петербург
Наукоемкие технологии
2018

УДК 355.4
ББК 68.4
М15

Рецензенты:

Президент Российской академии ракетных и артиллерийских наук, действительный член Академии военных наук, Заслуженный деятель науки РФ, доктор технических наук, профессор ***Василий Михайлович Буренок;***

Генеральный директор Центра стратегических оценок и прогнозов, доктор технических наук, старший научный сотрудник ***Сергей Николаевич Гриняев;***

Руководитель Центра военного прогнозирования, член-корреспондент Академии военных наук, член экспертного совета Председателя Военно-промышленной комиссии при Правительстве РФ, кандидат военных наук, доцент ***Анатолий Дмитриевич Цыганок.***

М15 Макаренко С.И., Иванов М.С.
Сетецентрическая война – принципы, технологии, примеры и перспективы. Монография. – СПб.: Наукоемкие технологии, 2018. – 898 с.

ISBN 978-5-6040965-3-6

УДК 355.4
ББК 68.4

Монография является результатом работы авторов по обобщению исследований в области ведения боевых действий и управления войсками в условиях произошедшей в начале XXI века информационно-технической революции. Результатом внедрения достижений информационно-технической революции в практику военного дела стало резкое синергетическое наращивание боевой эффективности вооружений, коренной пересмотр стратегии и тактики ведения военных действий, а также подходов к строительству вооруженных сил. Эти революционные изменения были обобщены в рамках концепции сетецентрической войны, сформированной в США в конце XX века. В монографии проведен анализ основ концепции сетецентрической войны, выявлены фундаментальные взаимосвязи этой концепции с информационно-технической революцией, тенденциями развития нового оружия, перестройкой организационной структуры вооруженных сил, а также способов и форм ведения боевых действий. В работе представлены перспективы развития вооружения и военной техники, получившей широкое применение в сетецентрических войнах. На примерах вооруженных конфликтов конца XX – начала XXI веков выявлены ключевые особенности сетецентрической войны. Материал монографии адресован специалистам, ведущим прикладные исследования в области военного строительства, управления войсками, и разработчикам новых вооружений.

ISBN 978-5-6040965-3-6

Научное издание.
Напечатано с оригинал-макета, подготовленного авторами.

Оглавление

Предисловие

Читателю представлена монография, содержание которой явно, и в значительной степени, выходит за рамки рассмотрения непосредственно «сетецентрической войны». В данной работе сосредоточены аналитические и информационные материалы, которые характеризуют практически все появившиеся в последние годы и ожидаемые в недалеком будущем инновации в военном деле. Причем не только технические инновации, но и новые способы военных действий (именно военных, а не только боевых).

Авторы поставили перед собой в определенном смысле трудно выполнимую задачу. Однако, можно сказать, что задача глубокого анализ технических и технологических инноваций ими в целом выполнена (во всяком случае, мне неизвестны не учтенные авторами новые аспекты развития вооружения, военной и специальной техники). Другое дело, что детальность изложения этих аспектов различна, но вряд ли в одном труде одинаково подробно можно было их изложить. Что касается новых способов военных действий, то здесь успех значительно скромнее, но, наверное, это и невозможно было сделать. Такую задачу должны поставить перед собой именно военные специалисты на основе ознакомления с изложенными в труде возможностями перспективных систем и средств силового противоборства.

В результате огромной работы, проведенной авторами, ими создан фактически справочник по новым, перспективным направлениям развития систем вооружения вооруженных сил передовых стран мира, в определенной (однако, по понятным причинам, не в полной) мере проведена оценка их места и роли в силовом противоборстве будущего.

Очевидно, давая себе отчет, что невозможно быть квалифицированным специалистом во всех анализируемых областях, авторы повели себя весьма корректно, давая подробные ссылки на первоисточники, в которых та или иная частная проблема изложена. Причем часто, хотя и не всегда, сопоставляются оценки, изложенные в разных источниках, что особенно ценно. Эта осторожность в оценках также дает право рассматривать данный труд как своеобразный справочник.

В целом можно оценить данный труд как весьма полезный и необходимый в современных условиях. Он позволит специалистам не только еще раз рассмотреть известную им проблему, но и оценить ее во взаимосвязи с другими аспектами и тенденциями, понять важ-

ность и нужность приложения усилий в том или ином направлении, соотнести собственные проблемы с возможностью их комплексирования со смежными областями военной науки и техники, провести поиск синергетических эффектов.

По широте и глубине изложенного в труде материала данную монографию можно оценить как уникальное, наиболее обширное (из всех мне известных), системное издание, которое дает представление обо всех заметных тенденциях в развитии технических средств и технологий силового противоборства. Это, пожалуй, наиболее ценное качество данного труда. В этом смысле можно согласиться с авторами, которые адресуют его «специалистам, ведущим прикладные исследования в области военного строительства, управления войсками и разработчиков новых вооружений». Можно только продолжить, что к числу адресатов обязательно необходимо добавить слушателей высших военно-учебных заведений, сотрудников научно-исследовательских организаций Минобороны России.

Президент Российской академии ракетных и артиллерийских наук,
Вице-президент Академии военных наук,
Заслуженный деятель науки Российской Федерации,
доктор технических наук, профессор,
Лауреат Государственной премии им. Г.К.Жукова
и премии Правительства Российской Федерации

В.М. Буренок

Введение

«Эксперты часто характеризуют современные им методы ведения войны как революционный прорыв в военном деле. То обстоятельство, что они приурочивают время этого прорыва к собственной эпохе, должно насторожить аудиторию…

Полагать, что эволюция методов ведения боевых действий не была непрерывной и, по большей части, равномерной, – ошибка, вызванная незнанием истории развития военной техники и тактики».

Сирил Фоллс «Сто лет войны: 1850 – 1950»

Конец XX века ознаменовался информационно-технической революцией, которая не только позволила вывести на принципиально новый уровень системы сбора, передачи и обработки информации, но и открыла новую эру геополитики. Она характеризуется факторами всемирного доступа к глобальному информационному пространству, широкого распространения электронных средств обработки информации, а также мировым экономическим кризисом и очередным витком передела сфер влияния в мире. Анализ результатов информационно-технической революции показывает, что в настоящее время США утрачивают позиции мирового экономического и технологического лидера из-за высокого темпа развития стран Азиатско-Тихоакеанского региона, а также из-за экономического кризиса капитализма, центром которого является США и Евросоюз. Сейчас Китай, Япония, Индия являются лидерами современной радиоэлектронной и микропроцессорной промышленности, а также индустрии производства программного обеспечения, однако не обладают высоким уровнем политического влияния в мире. В результате геополитические тенденции, порождаемые информационно-технической революцией, могут спровоцировать появление новых точек напряженности и конфликты в мировой внешнеполитической сфере, направленные на передел сфер влияния в мире. И, прежде всего, это конфликты между США и Китаем.

Достижения информационно-технической революции были использованы для создания высокоточного оружия, информационных систем и средств военного назначения, прорывных исследований в военной радиоэлектронике. Именно ее достижения являются той основой, на которой строится вся система вооружения современной ар-

мии. Это в свою очередь обусловило и изменение подходов к ведению войны и основам строительства вооруженных сил. Анализ военно-прикладных эффектов от использования достижений информационно-технической революции свидетельствует о том, что развитие средств сбора, передачи и обработки информации определяет прорывной скачок в характеристиках средств вооруженной борьбы. При этом именно развитие средств борьбы неизбежно обусловливает изменение способов ведения военных действий.

Отличительная особенность развития средств вооруженной борьбы в современных условиях состоит в появлении качественно новых видов оружия, такого как высокоточное оружие, оружие на новых физических принципах, информационное оружие, оружие на основе робототехнических средств. При этом информатизация средств вооруженной борьбы позволила создать не только глобальные системы разведки, связи и навигации, но и взаимоувязать различные средства вооружения, разведки и пункты управления в единую информационно-сетевую среду, что позволило резко увеличить боевые возможности новых видов оружия. В условиях такого объединения вооружений в единое информационное пространство была выдвинута концепция сетецентрической войны как стратегического взгляда на ведение войны в новых военно-технических условиях. Эта концепция не ограничивается разработкой новых способов применения вооружений, а предусматривает коренную ломку организационных форм вооруженных сил и способов ведения военных действий всех масштабов

Целью монографии является анализ основ концепции сетецентрической войны, выявления фундаментальной взаимосвязи этой концепции с информационно-технической революцией, с тенденциями развития нового оружия, перестройкой организационной структуры вооруженных сил, а также способов и форм ведения боевых действий.

Исследования в области развития методов ведения боевых действий и управления войсками с учетом использования новых информационных технологий велись такими учеными как: Н.В. Огарков, М.А. Гареев [1], С.Н. Гриняев [2, 3], В.С. Пирумов [4, 5], Н.А. Костин [6, 7, 8], С.А. Комов [9, 30, 31, 55, 56, 57], В.И. Цымбал [10], А.А. Прохожев, Н.И. Турко [12], С.А. Модестов [9, 10, 11], Т.В. Гуржеянц, Е.А. Дербин, Г.О. Крылов, А.Н. Кубанков [15], А.В. Бедрицкий [16], В.И. Слипченко [17], Ю.Я. Бобков, Н.Н. Тютюнников [29], В.М. Буренок [38, 39, 40, 41, 42], А.Е. Кондратьев [43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54], С.В. Коротков, И.Н. Дылевский, А.Н. Петрунин [31, 55, 56, 57], А.А. Рахманов [58, 59, 60], Г.А. Налетов [61], Ю.И. Старо-

дубцев [62-68], С.С. Семенов, В.В. Бухарин [62-63], Е.В. Гречишников [64-68], М.П. Фархадов, Д.Н. Душкин [69], С.В. Кругликов, А.А. Липатов [70], А.В. Копылов [82], Р.В. Арзуманян [84], А.Н. Сидорин, В.М. Прищепов, В.П. Акуленко [95], И.М. Капитанец [173], Л.В. Савин [239], А.А. Ивлев [290]. И.М. Попов, М.М. Хамзатов [461]. В основу данной монографии положены анализ, развитие и обобщение вышеуказанных работ в области развития методов вооруженной борьбы и управления войсками в условиях информационно-технической революции. Также авторы широко использовали материал открытых работ американских экспертов: A.K. Cebrowski, J.J. Garstka, P.J. Dombrowski, D.S. Alberts, F.P. Stein, E.A. Smith [329, 330, 331, 332, 333], которые легли в основу создания и развития концепции сетецентрических войн в США. Кроме того, в монографии нашли отражения предварительные исследования авторов по рассматриваемой тематике, ранее опубликованные в работах – С.И. Макаренко [120, 145, 191, 216, 220, 270, 374, 458, 459, 460, 462, 463] и М.С. Иванова [47, 120, 121, 122, 123, 124, 125, 126, 127, 129, 130].

В первой главе монографии проведен анализ основных трендов развития геополитической обстановки в мире и влияния на них информационно-технической революции. Рассмотрена текущая геополитическая обстановка в мире. Выявлены основные факторы, определяющие геополитику на глобальном и региональном уровне. Представлен прогноз развития мировой геополитической ситуации с учетом возникновения точек напряженности, а также – локальных войн и конфликтов. Проведен анализ влияния информационно-технической революции на глобальные мировые тренды – информатизацию и глобализацию общества, а также на изменение геополитики с учетом развития информационных технологий. Сделаны выводы о том, что информационно-техническая революция конца XX века предопределила передел сфер влияния в мире, спровоцировала ряд точек геополитической напряженности, стала катализатором развития новых видов оружия, предопределила изменение способов военных действий и строительства вооруженных сил.

Во второй главе монографии показано, что концепция сетецентрической войны является отображением передовых взглядов на ведение войны и управление войсками в условиях информационно-технической революции. Проведен анализ основных направлений развития военного противоборства и управления войсками. Представлено развитие способов и форм ведения боевых действий в войнах доядерного и ядерного периода. Показано, что революция в военном деле в

конце XX века, предопределившая переход к бесконтактным войнам шестого поколения, является следствием произошедшей в 80-х гг. XX века информационно-технической революции. Выявлены основные особенности бесконтактных войн шестого поколения, а именно: существенное возрастание роли воздушно-космических, высокоточных и информационных средств при ведении войны. Выявлены факторы, предопределившие разработку концепции сетецентрической войны. Проведен анализ теорий, предшествующих концепции сетецентрической войны, теории декомпозиции стратегических целей на пять колец Дж. Вардена, теории циклов Дж. Бойда и концепции революции в военном деле Н.И. Огаркова. На основе отечественных и зарубежных открытых публикаций проведен фундаментальный анализ концепции сетецентрической войны. Указаны ее ключевые особенности, а также принципы ведения боевых действий в такой войне.

Проведен анализ сетецентрической среды как ключевого элемента концепции сетецентрической войны. Выявлены области среды, принципы ее построения и функционирования. Рассмотрены сетевые архитектуры, используемые для организации взаимодействия сил и средств в сетецентрической среде. Указаны основные эффекты для войск (сил), которые обеспечиваются за счет использования сетецентрической среды. Показано, что внедрение сетецентрической среды требует изменения подходов к строительству вооруженных сил и способам их применения. В заключении главы проведен анализ критических замечаний и недостатков концепции сетецентрической войны. Представлены основные уязвимости и противоречия этой концепции, а также возможности асимметричного противодействия высокотехнологическому противнику, ведущему сетецентрическую войну.

В третьей главе монографии проведен анализ изменения подходов к строительству вооруженных сил в условиях внедрения концепции сетецентрической войны. За основу взят анализ вооруженных сил США, Израиля, Китая, некоторых других государств, а также объединенных сил НАТО. При этом с наибольшей степенью детализации рассмотрены именно вооруженные силы США. Проведенный анализ военно-доктринальных документов, стратегических задач и основных тенденций строительства вооруженных сил показал, что в вооруженных силах практически всех зарубежных технологически развитых государств ведется переход к собственным версиям концепции сетецентрической войны. Вероятнее всего к 2020 г. их вооруженные силы полностью перейдут от централизованно-иерархического к сетецентрическому принципу управления. Переход к концепции сетецентри-

ческой войны требует кардинальной перестройки тактического и оперативно-тактического звена управления. Показано, что переход к мобильным, динамично комплектуемым подразделениям, ориентированность на проведение «операций, основанных на эффектах», позволяют даже подразделениям тактического уровня решать стратегические задачи. При этом существенно возрастает значимость сил специальных операций, сил разведки, авиационно-космических сил, сил радиоэлектронной борьбы. Существенное возрастание роли информации в контуре военного управления определило актуальность создания сил информационных операций (так называемых кибервойск), на которые возлагаеются задачи обеспечения безопасности собственной государственной и военной информационной инфраструктуры, а также проведение наступательных операций на информационную инфраструктуру противника.

В четвертой главе проведен анализ тенденций развития вооружения и военной техники в условиях перехода к концепции сетецентрической войны. За основу взят анализ вооружения и военной техники, разрабатываемой в США как наиболее милитаризованного и технологически развитого государства. Отметим, что при проведении анализа более глубоко рассмотрены вопросы совершенствования систем и средств РЭБ и средств информационного воздействия, что обусловлено научными интересами авторов монографии. Представлены общие тенденции развития вооружения и военной техники, а также тенденции развития военных технологий. Проведен анализ перспектив развития систем управления, связи и разведывательного обеспечения. На основе анализа таких военных систем связи, как DISN, GIG, NIPRNet, SIPRNet, JWICS, AEHF, WGS, MUOS, TacSat, SDS, WIN-T, обоснованы общие тенденции развития систем связи в условиях перехода к принципу сетецентрического управления. Анализ таких систем как DCGS, DCGS-A, DCGS-N, DCGS-AF, ASAS, а также космических, воздушных и наземных средств разведки позволил выявить общие тенденции развития разведывательного обеспечения. Анализ таких систем, как GCCS, GCCS-Army, GCCS-Maritime, TBMCS, ABCS, FBCB-2, A2C2S, а также программы FCS позволил выявить общие тенденции развития систем автоматизированного управления. Рассмотрены основные тенденции развития высокоточного оружия (ВТО). Показано, что главными трендами совершенствования ВТО является переход к гиперзвуковым средствам доставки и улучшение работы боевых частей. Рассмотрены примеры перспективных гиперзвуковых средств доставки, а также современные и перспективные бо-

евые части для ВТО. На примере систем GBMD, SBMD, THAAD, Patriot PAC-3 рассмотрены тенденции развития систем ПВО и ПРО. Проведен анализ тенденций использования космоса в военных целях. На основе анализа систем разведки KeyHole, Lacrosse, ORS, SSU и др., системы для обнаружения стартов МБР и ядерных взрывов IMEWS, космической навигационной системы NAVSTAR, спутниковых систем связи DSCS, WGS, MilStar, AEHF, UFO, MUOS, TDRS, SDS выявлены тенденции развития систем космического информационного обеспечения. На основе анализа перспективных средств ASAT, GBI, SM-3, Falcon и X-37 рассмотрены тенденции развития космического оружия, а также способы его применения. Проведен анализ перспектив развития робототехнических средств вооружений, основанных на беспилотных летательных аппаратах, наземных дистанционно-управляемых машинах и необитаемых надводных и подводных аппаратах. Подробно рассмотрены средства информационно-технического и психологического оружия. На основе большого числа средств и комплексов РЭБ подробно рассмотрены и проанализированы тенденции развития этого вида вооружений. Кратко рассмотрены основные тенденции развития базовых видов оружия массового поражения – ядерного, химического, биологического и генетического. А также оружие на новых физических принципах – лазерное, ускорительное (пучковое), акустическое, рельсотроны, радиочастотное и сверхвысокочастотное, геофизическое, а также оружие на основе нанотехнологий. В заключении главы рассмотрены перспективные исследования, проводимые агентством DARPA США, в интересах дальнейшего совершенствования вооружения и военной техники.

В пятой главе на основе военных конфликтов конца XX – начала XXI века выявлены основные особенности современных операций, проводимых в соответствии с концепцией сетецентрических войн: операция НАТО «Решительная сила» против Югославии в 1999 г.; операция США и их союзников «Иракская свобода» («Шок и трепет») в Ираке в 2003 г.; операции США и НАТО «Одиссея. Рассвет» и «Союзный защитник» в Ливии в 2011 г. На примере этих операций выявлены характерные особенности сетецентрической войны и их ретроспективное развитие. К этим особенностям относятся: проведение мощных информационно-психологических и экономических операций на начальном этапе конфликта; ралиазация концепции «обезоруживающего удара» в начале конфликта за счет массированного применения ВТО авиационного и морского базирования; массовое использование беспилотных и робототехнических средств для ведения

разведки и нанесения ударов; достижение информационного превосходства за счет использования космических средств связи, современных систем управления, разведывательного и навигационного обеспечения, а также за счет массированного применения средств РЭБ и информационно-технических воздействий; проведение психологических операций по формированию позитивного восприятия агрессоров в сознании мирового общественного мнения и гражданского населения страны, втянутой в конфликт; широкое использование сил специальных операций и наемников. В заключении главы сделаны выводы об общих тенденциях применения элементов сетецентрических войн в военных конфликтах начала XXI века и их дальнейшем развитии.

Материал работы ориентирован на неподготовленного читателя, интересующегося вопросами современной военной стратегии и развития средств вооружения. Кроме того, материал может быть полезен специалистам, научным работникам, соискателям ученой степени, ведущим исследования в области сетецентрических войн.

Специфика сложной и комплексной проблемы развития стратегии вооруженной борьбы и управления войсками в условиях информационно-технической революции такова, что далеко не все ее аспекты могут излагаться с одинаковой степенью подробности в открытой литературе. Разумеется, в настоящее время в силу изменений известных политических, экономических и социальных факторов многие проблемы, задачи и технические решения в области военной науки являются открытыми. Многое стало обсуждаться в кругах специалистов и публиковаться в открытых изданиях. Но, тем не менее, в целом предметная область перспективных путей развития военной науки содержит еще очень много деликатных тем, которые не могут рассматриваться с одинаковой степенью подробности в книге, адресованной широкому кругу читателей. В частности, в монографии при рассмотрении концепции сетецентрических войн, тенденций в изменении подходов к военному строительству, а также перспектив развития вооружения авторы сознательно ориентируются на вооруженные силы США и некоторых других технически развитых государств, избегая сравнительных оценок с отечественными исследованиями и разработками в этой области, как правило, носящими закрытый характер. Кроме того, не все затронутые в монографии темы рассмотрены с одинаковой степенью подробности, что обусловлено стремлением авторов глубже рассмотреть те вопросы, которые соответствуют области их научных интересов. Надеемся, что благосклонный читатель найдет эти обстоя-

тельства извинительным и не будет сурово осуждать представленную работу за некоторую неполноту и непоследовательность.

При подготовке книги авторы использовали только открытые материалы, на которые имеются соответствующие ссылки, а также собственный опыт службы в научных и учебных учреждениях. При этом авторы стремились к тому, чтобы книга по своему научно-методическому содержанию могла бы выступить своеобразным справочным пособием. Некоторые повторы и пояснения приведены для облегчения понимания материала неспециалистами, которые стремятся ознакомиться лишь с отдельными проблемами концепции сетецентрических войн. При этом авторы не претендуют на всеобъемлющее изложение всей проблематики сетецентризма в военной и технической области. Да это и невозможно, ведь концепция сетецентрической войны является молодой, многообразной и бурно развивающейся отраслью научного знания и использования технических возможностей.

Авторский вклад в написание материала монографии распределился следующим образом. Введение, разделы 1, 2.1-2.3, 2.4.1-2.4.3, 2.6, 4.1-4.9, 5, а также заключение написаны единолично С.И. Макаренко, редактирование материала этих разделов выполнено М.С. Ивановым. Разделы 2.4.4-2.4.5, 2.5, 4.10 написаны единолично М.С. Ивановым, редактирование материала этих разделов выполнено С.И. Макаренко. Разделы 2.7 и 3 написаны совместно С.И. Макаренко и М.С. Ивановым. В целом концепция и замысел настоящей монографии разработаны С.И. Макаренко, окончательное редактирование материалов выполнено М.С. Ивановым.

Авторы выражают благодарность рецензентам – заслуженному деятелю науки РФ, доктору технических наук профессору В.М. Буренку; доктору технических наук старшему научному сотруднику С.Н. Гриняеву; кандидату военных наук доценту А.Д. Цыганку за кропотливый труд по поиску ошибок и неточностей при рецензировании монографии. Кроме того, авторы благодарны кандидату технических наук Р.Л. Михайлову и С.И. Хорошилову за ценные замечания, которые помогли сделать материал монографии лучше и доступнее.

Данная работа стала возможной благодаря тем людям, которые помогали, поддерживали, направляли, критиковали и всячески способствовали авторам в их исследованиях. Авторы выражают глубокую признательность кандидату технических наук профессору А.В. Баженову, кандидату технических наук доценту В.Е. Федосееву, кандидату технических наук доценту А.В. Кихтенко, доктору технических наук

профессору А.Г. Ломако, доктору военных наук профессору Ю.И. Стародубцеву. Именно они способствовали становлению авторов как ученых, и мы гордимся, что имели возможность обучаться и работать рядом с такими людьми.

Особую признательность хочется выразить коллективам кафедры эксплуатации и ремонта бортового авиационного радиоэлектронного оборудования (радионавигации и радиосвязи), кафедры эксплуатации и ремонта бортового авиационного радиоэлектронного оборудования (оптико-электронных комплексов) в Ставропольском ВВАИУ, кафедры радионавигации и радиолокации, а также кафедры эксплуатации бортового авиационного радиоэлектронного оборудования в ВУНЦ ВВС «ВВА имени проф. Н.Е. Жуковского и Ю.А. Гагарина», кафедры сетей и систем связи космических комплексов ВКА имени А.Ф. Можайского. Именно на этих кафедрах авторам посчастливилось проходить службу, их творческая атмосфера всегда способствовала плодотворной деятельности и определила области научных интересов и направления исследований авторов.

Кроме того, авторы считают своим долгом поблагодарить всех тех специалистов, которые внесли свой научный вклад в исследование теории сетецентрической войны. Особенно хотелось бы отметить таких ученых как: В.М. Буренок, А.А. Ивлев, С.Н. Гриняев, О.Н. Остапенко, С.В. Баушев, И.В. Морозов, Т.В. Гуржеянц, Е.А. Дербин, Г.О. Крылов, А.Н. Кубанков, В.И. Слипченко, Ю.Я. Бобков, Н.Н. Тютюнников, А.Е. Кондратьев, А.В. Копылов, Р.В. Арзуманян, А.Н. Сидорин, В.М. Прищепов, В.П. Акуленко, И.М. Капитанц, А.Д. Цыганок. Работы именно этих авторов были положены в основу исследований концепции сетецентрической войны и составили ядро материалов монографии.

Авторы будут рады сотрудничеству в рассматриваемой области исследований, а также конструктивным замечаниям и предложениям по содержанию монографии. Замечания и предложения просим направлять по адресам: mak-serg@yandex.ru (С.И. Макаренко) и point_break@rambler.ru (М.С. Иванов).

1. Основные тренды развития геополитической обстановки в мире и влияние на них информационно-технической революции

1.1. Геополитическая обстановка в мире

Как показывает анализ материалов [18, 19, 20, 23, 36], по тенденциям развития геополитической, военной и экономической ситуации в мире современная политическая ситуация характеризуется возросшей турбулентностью событий, как на глобальном, так и на региональном уровнях.

1.1.1. Основные факторы, определяющие геополитику на глобальном уровне

Основные факторы, определяющие геополитику на глобальном уровне, в соответствии с работами С.В. Новоселова [18], Ю. Романенко [23], К.В. Сивкова [23], а также коллектива авторов Центра военно-политических исследований МГИМО [36], приведены ниже.

Завершение процесса глобализации, которое основано на экономическом базисе. Фактически, как показано в работе [21], основу современной мировой экономики составляет группа транснациональных корпораций (ТНК), включающая в себя 147 компаний, которым фактически подконтрольны приблизительно 40% мирового производства товаров и услуг и примерно 60% общемировых доходов (более 70% денежных ресурсов мира, драгоценных металлов, углеводородного сырья). Ими же контролируется до 80% ведущих мировых средств массовой информации (СМИ). Данная группа ТНК реализует стратегию финансового монополярного миропорядка, основой которого являются резервная система США, финансовые системы Великобритании и Ватикана, а также финансовые группы частных лиц (Rothschild, Rockefeller и др.). Следующей целью глобализации будет структурное оформление новой глобальной власти, придание ей законного статуса. При этом важнейшим вопросом становления геополитической структуры будущего мира является поведение отдельных субъектов глобального управления в процессе политического переустройства мира.

Ключевыми элементами такого переустройства будут являться [18]:

- создание мирового наднационального правительства;
- перемещение финансовой инфраструктуры в Восточную Азию;
- установление финансовой и экономической диктатуры.

При этом для маскировки расширения влияния мировых финансовых ТНК возможно проведение информационных операций по формированию в глазах мировой общественности образа врага. В прошлом таковым был СССР, сегодня – это исламский терроризм, Ливия, Сирия, Иран, а в ближайшей перспективе – Китай.

Нарушение нормального функционирования мировой финансовой системы. Анализ динамики цен на знаковые виды сырья (нефть, золото, пшеницу) показывает, что абсолютные значения цен на эти важнейшие виды сырья за очень короткое время выросли в 4-5 раз и продолжают расти. Таким образом, происходит резкое обесценивание мировых резервных валют, не обеспеченных в должной мере реальным содержанием, а также ценных бумаг [18]. Фактически мировая экономика по завершении ее глобализации оказалась перед фактом финансового кризиса, который был обусловлен множеством взаимоувязамно действующих факторов.

В работах В.П. Романова [20] и К.В. Сивкова [23] выделяются основные противоречия и диспропорции, которые вызвали глобальный системный политико-экономический кризис начала XXI века:

- кризис капитализма, связанный с исчерпанием возможностей роста и получения прибылей в рамках современной модели экономики;
- противоречие между ростом производства/потребления и имеющимися ресурсами, необходимыми для развития экосистемы Земли;
- диспропорции в распределении промышленных мощностей и сырья, породивших конфликт интересов между промышленно-развитыми странами и странами – поставщиками сырья;
- противоречия между «бедными» развивающимися странами и «богатыми» промышленно развитыми;
- противоречие между нациями, национальными элитами и транснациональной элитой;
- противоречие между объемом мирового «финансового пузыря» и масштабом реального сектора мировой экономики;

- противоречие между огромной мировой финансовой властью транснациональной финансовой элиты и отсутствием ее политической субъектности;
- противоречие между идеологией «свободного рынка», ставящего во главу власть денег, и духовными основами существования различных цивилизаций, формирующих цивилизационные различия, порождающих власть идей (в той или иной степени).

При этом в качестве вариантов изменения состояния глобальной экономической системы рассматривается [18]:

- величайшая глобальная депрессия с присущими ей застоем в производстве и науке, со значительным падением уровня жизни и культуры, с революциями и приходом к власти радикальных политических движений в отдельных регионах;
- попытка нарушить равновесие финансовой системы за счет войн и применения сценариев глобального хаоса, цели которых не столько в «переделе рынков», сколько в создании для победителей новых зон предпринимательской активности для вложения средств;
- кардинальное революционное изменение всей существующей социально-экономической системы.

При этом первый вариант является для представителей группы ТНК наихудшим выбором, а третий вариант – возможностью, допустимой, но требующий большей степени внутреннего единства во взглядах и делах. Таким образом, вариант с «большой войной» и «управляемым хаосом» представляет собой наиболее вероятное ближайшее будущее современного общества [22].

Формирование мировых геополитических центров силы и их стратегии. Мировые этнокультурные регионально-цивилизационные объединения Востока и Запада пока играют вторичную роль в формировании мировых процессов. Основными мировыми центрами регионально-цивилизационных объединений являются Северная Америка, Европа, Китай, и между ними идет острая борьба за лидерство. При этом Северная Америка, Япония и Европа служат основой существующей мировой финансовой системы, а Китай – основой мирового товаропроизводства, но и они на уровне государств ведут войну за независимость от финансовой олигархии группы ТНК. Индия, ЮАР, Россия и Бразилия динамично развиваются, но пока составляют страны «второго эшелона». Исламский мир разрознен и отстает в технологическом и экономическом развитии, а страны Латинской Америки

только вступили на путь цивилизационного строительства. Такая конфигурация мировых сил и разнонаправленность их действий создают конгломерат трудно разрешимых противоречий, которые выливаются в систему геополитического противоборства.

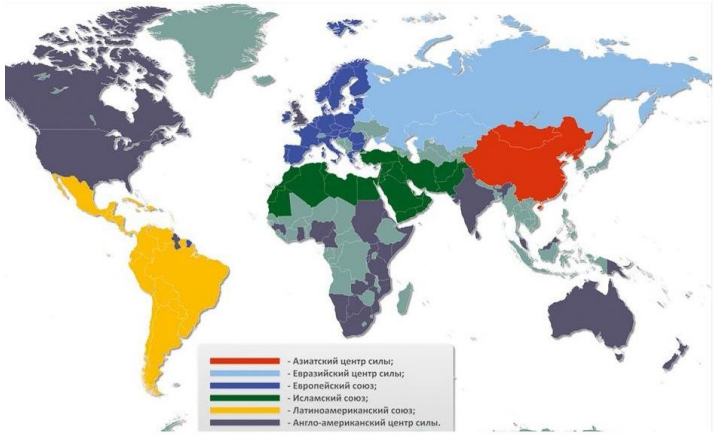


Рис. 1.1. Расстановка геополитических сил в начале XXI века

При этом главными объектами геополитического противоборства становятся [23]:

- стратегически важные районы мира;
- стратегические коммуникации (в том числе и информационные);
- глобальные ресурсы (в том числе и информационные).

Обладание этими объектами во многом будет определять геополитический статус цивилизаций и групп государств, динамику их развития, степень внешней и внутренней безопасности, уровень суверенности.

1.1.2. Основные факторы, определяющие геополитику на региональном уровне

К особенностям, определяющим геополитику на региональном уровне, в соответствии с работой С.В. Новоселова [18], можно отнести следующие.

1. Монопольное военно-политическое господство США в мире, а также их мировое экономическое лидерство подходит к

концу. США не выдержали испытания однополярностью, истощив себя в последнее десятилетие непрерывными войнами на Ближнем и Среднем Востоке. США остается сверхдержавой, которая, вместе с тем, с трудом справляется с выходящими из-под контроля глобальными изменениями, происходящими как на социально-экономической, так и на геополитической аренах.

В настоящее время у США недостаточно ресурсов, чтобы оставаться мировым лидером (рис. 1.2).

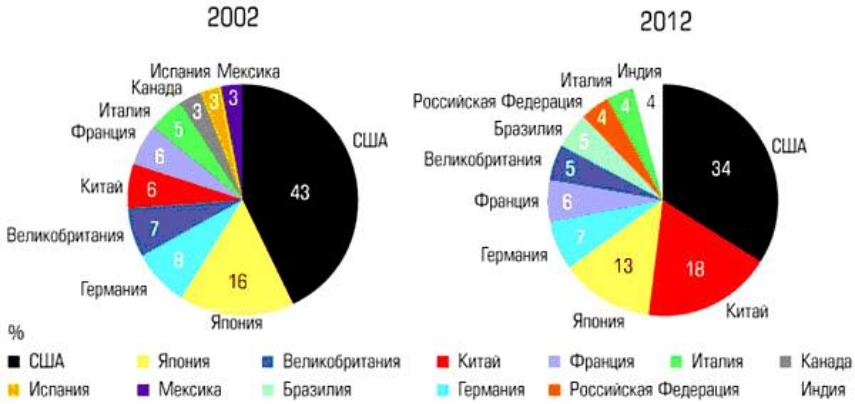


Рис. 1.2. Динамика изменения десятки стран с наибольшим вкладом в мировой ВВП с 2002 по 2012 гг. в процентах от мирового ВВП [34]

Как показывают данные МВФ [34], вклад Америки в мировую экономику упал на 10%. В списке 20 стран с самым высоким ВВП доля США упала с 43% в 2002 г. до 33% в 2012 г. В то же время экономическое влияние Китая выросло на 12% – с 6% до 18%, а Бразилия и Россия увеличили свой ВВП на 5,1 и 4,3%

2. Перемещение центра мирового экономического развития с Запада в Азию. Суммарный ВВП Индии и Китая по паритетной покупательной способности уже больше, чем у США, а ВВП государств группы БРИК (Бразилия, Россия, Индия и Китай) – превосходит совокупный ВВП Евросоюза (рис. 1.2). В обозримой исторической перспективе этот разрыв будет только возрастать. Совокупная доля Восточной Азии и Южной Америки в мировом ВВП уже к 2020 г. достигнет порядка 60%, из которых 45% будут приходиться на одну только Азию. Не стоит сомневаться в том, что экономический потен-

циал новых центров мирового роста будет неизбежно конвертироваться в политическое и военное влияние [34].

Серьезная конкурентная борьба развертывается между Китаем и Индией, между госкапитализмом и традиционной демократией. Именно Китай и Индия – два государства с самым многочисленным населением в мире определят основные направления и темпы будущего мирового экономического развития.

По итогам 2012 г. Китай стремительно догоняет США по уровню ВВП (Китай – 8 трлн долл., США – 16 трлн долл.) с темпом прироста ВВП 7,6%, что является максимальным в мире. При этом объемы внешней торговли Китая составили 3,87 трлн долл., превысив объемы внешней торговли Соединенных Штатов (3,82 трлн долл.) (рис. 1.3) [33].

Китай активно формирует вокруг себя зону военной и энергетической безопасности, активно переводя свой экономический потенциал в политическое влияние в Азиатско-Тихоокеанский регион (АТР). Так, общие объемы китайских инвестиций в экономику стран АТР составляют, по меньшей мере, 130 млрд долл. [33].

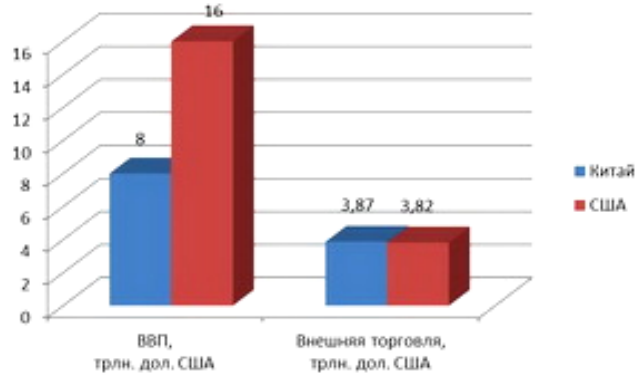


Рис. 1.3. Уровень ВВП и объем внешней торговли Китая и США [33]

Основные партнеры Китая в АТР – Индонезия, Филиппины, Вьетнам, Малайзия, Индия, Япония, Лаос, Южная Корея и Бруней. При этом главным партнером КНР в АТР является Индия. Невзирая на соперничество за влияние в регионе и наличие отдельных территориальных проблем, обе страны последовательно развивают свои связи в торгово-экономической отрасли. КНР является одним из самых круп-

ных торговых партнеров Индии. Например, объемы взаимной торговли составляют около 80 млрд долл., а в течение ближайших лет их товарооборот планируется довести до 100 млрд долл. в год [33]. Кроме того, между Китаем и Индией развивается сотрудничество сторон в военной сфере, получившей официальное начало в 2006 г. в рамках соответствующего меморандума между оборонными ведомствами обеих стран.

Одновременно Китай развивает сотрудничество с Россией и странами Юго-Восточной и Центральной Азии. Так, КНР реализуют на территории России крупные проекты по освоению природных ресурсов Дальнего Востока и Восточной Сибири. Также Китай является одним из крупнейших инвесторов российской промышленности, сельскохозяйственной и пищевой отраслей, транспорта и связи. При этом, со своей стороны, Китай обеспечивает Россию как товарами широкого потребления, так и высокотехнологичной продукцией, проявляя при этом неподдельный интерес к оборонной, космической и другим передовым российским отраслям [33].

В странах Центральной Азии (Казахстане, Киргизстане, Узбекистане, Туркменистане) Китай наращивает свое влияние за счет реализации совместных энергетических проектов, а также планов построения собственной модели «шелкового пути» – транспортного коридора из Азиатско-Тихоокеанского региона в Европу через Центральную Азию [33].

3. Борьба за мировое лидерство и доступ к ограниченным природным ресурсам между США и Китаем. Именно эта борьба определит социально-экономическую модель постиндустриального мира и доминирующий тип политической системы в XXI в. [18, 24].

Политическое руководство США рассматривает лидерство в мировой геополитической иерархии как необходимое условие развития страны. Один из фундаментальных принципов, лежащих в основе национальной стратегии США – принцип мирового лидерства. В XX в. США уже трижды воспользовались военным способом достижения геополитического лидерства, причем после мировых войн США всегда получали существенную геополитическую выгоду, повышая свой политико-экономический статус. Ожидается, что при существующих тенденциях геополитической динамики смена мирового лидера может произойти примерно к 2025 г.

Опираясь на доллар в качестве международной валюты, США проводят неограниченную эмиссию и занимаются экспортом необеспеченных долларов в обмен на реальные товары. В условиях экономи-

ческого кризиса США вынуждены регулярно тратить огромные суммы денег на стабилизацию своей экономики, а субсидирование таких трат требует все больших объемов заимствований, что, в свою очередь, ведет к росту дефицита наличных долларов, необходимых для выплаты процентов по займам. Выход из этой ситуации – это эмиссия долговых ценных бумаг казначейства США. Инвесторы, вкладывающие средства в векселя и облигации с гарантированной доходностью Казначейства США, ориентируются на потенциальное возрождение американской экономики и рейтинги ведущих экономических агентств (Standard & Poor's, Moody's, Fitch). Однако доходов от эмиссии долговых ценных бумаг абсолютно недостаточно для поддержания даже существующего уровня расходов государства. Парадокс ситуации состоит в том, что надежность и доходность этих бумаг обеспечиваются исключительно новыми, все более масштабными вложениями самих же инвесторов, стремящихся обеспечить сохранность и доходность своих средств в условиях экономического кризиса. Эта изначально деструктивная финансовая система обеспечивает США жизнь в долг, который на конец 2012 г. составлял 16,4 трлн долл. или 109% от ВВП страны [33].

В настоящее время появились признаки роста напряженности между Вашингтоном и Пекином, спровоцированные противоречиями в финансовой сфере. Одним из основных держателей внешнего долга США является Китай, который активно работает в направлении вытеснения доллара и, в частности, с 2008 г. активно снижает доли долларов и казначейских обязательств США в собственных золотовалютных резервах. В 2011 г. ЦБ КНР информировал о полном отказе от доллара в международных взаиморасчетах. В 2007 г. шесть стран-членов Совета сотрудничества арабских государств Персидского залива – Саудовская Аравия, Бахрейн, Кувейт, Катар, Оман и ОАЭ подписали соглашение о единой валюте «динаре залива» [28]. По концепции премьер-министра Малайзии, представленной в 2002-2003 гг., межгосударственные расчеты между мусульманскими странами должны осуществляться в золотых динарах с использованием клиринговых механизмов [28].

В результате, согласно докладу [20], за последние 20 лет доля американского доллара в мировых финансовых транзакциях снизилась с 80 до 60%. Это существенно подрывает финансовую гегемонию США, основанную, в том числе, на бесконтрольной долларовой эмиссии, и, как показано в работе [28], может служить для США поводом

искусственно поддержать мировую финансовую нестабильность, в том числе за счет развязывания военных конфликтов.

Как отмечается в докладе Американского национального совета по разведке «Глобальные тенденции 2025: изменившийся мир» [19], соперничество за природные ресурсы станет ведущим геополитическим фактором в ближайшие 20 лет и главной причиной нестабильности и все возрастающей вероятности возникновения конфликтов в мире. В ближайшем будущем мир столкнется с устойчиво высокими тратами потребителей на нефть в условиях, когда пик в добыче ископаемого топлива уже пройден (рис. 1.4, 1.5). Месторождения легкодоступной нефти в мире истощаются (рис. 1.6), а средняя себестоимость их разработки с 2005 г. по 2008 г. увеличилась почти в два раза (рис. 1.7) [18, 20, 28].

Рис. 1.4. Разведанные запасы и уровень добычи нефти (по состоянию на 2007 г. в %) [20]

Рис. 1.5. Мировые извлекаемые запасы нефти и газа (по состоянию на 2008 г., в млн баррелей) [20]

Рис. 1.6. Рост капиталовложений в добычу нефти [28]

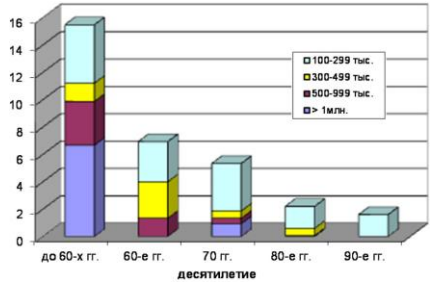


Рис. 1.7. Объемы добычи нефти на открытых месторождениях (барр./день) [28]

На этом фоне возникают новые сценарии, связанные с борьбой за Мировой океан или его отдельные важные участки, за доступ к ми-

ровой транспортной инфраструктуре и за владение морскими путями. В ближайшие годы чуть ли не главным фактором, который вызовет ряд серьезных вооруженных конфликтов и войн, станут водные ресурсы (от пресной воды и богатых рыбой и углеводородами участков Мирового океана до транспортных артерий) [18, 19].

В работах [18, 20, 26, 71] показано, что в США уже сформировался новый вектор внешней политики – тихоокеанский, направленный на сдерживание и противодействие растущей китайской мощи. Сужающиеся возможности США по военным расходам (сокращение на предстоящие 10 лет оборонного бюджета почти на 50%) диктуют:

- ускоренное снижение уровня военного присутствия в Азии (уход из Афганистана и Ирака) с оставлением ограниченного воинского контегента на Ближнем Востоке (прежде всего для проведения военных операций в Сирии);
- сохранение ограниченного военного присутствия в Европе, одна из функций которого – военное давление на западных границах России за счет реализации планов по строительству «ЕвроПРО» и создания ограниченных военных контингентов в странах бывшего СССР;
- наращивание сил в Тихом океане и в Восточной Азии.

Изменение вектора внешней политики ведет к переориентации на новых потенциальных внешних врагов. Хотя администрация США настаивает на том, что новый внешнеполитический курс не направлен на Китай, американская военная стратегия переориентируется от противодействия терроризму на сдерживание экономически бурно развивающегося Китая. При этом основной причиной столкновения двух держав будет борьба за доступ к мировым источникам природных ресурсов (прежде всего, углеводородных) и контроль над маршрутами их транспортировки.

США с населением в 5% от общемирового уровня на протяжении последних десятилетий потребляли порядка 40% всех природных ресурсов планеты. В условиях кризиса мировой экономии США не планируют снижать собственный уровень потребления, так как именно на него делается ставка по выходу американской экономики из кризиса. В то же время доступ к сырью, особенно к энергоносителям, как к основному обеспечивающему ресурсу экономики становится для стран Запада все более затруднительным. Традиционные месторождения нефти и газа истощаются, а потенциально новые сырьевые месторождения находятся либо в районах Сибири в вечной мерзлоте, либо на Арктическом шельфе, что в разы повышает стоимость их извлече-

ния. Западные ТНК теряют свои позиции в Африке и Латинской Америке, потому что страны, где сосредоточены основные энергоресурсы, проводят национализацию своих природных богатств, чтобы получить гарантированный источник поступления экспортной выручки в казну, в том числе и за счет сотрудничества с Китаем.

Сравнительный анализ динамики роста потребления углеводородов США и Китая, проведенный в работе [18], показывает неуклонный рост потребностей Китая в природных ресурсах для продолжения экономического роста.

В 2011 г. США потребляли до 19,6 млн баррелей нефти в день, из которых 9 млн производили сами, а остальное закупали за рубежом [18]. Для обеспечения безопасности транспортировки этого стратегического продукта США на протяжении десятилетий поддерживали монархии и авторитарные режимы на Ближнем Востоке. Всякий раз, когда ситуация выходила из-под контроля, США направляли сюда ограниченные воинские контингенты (Ливан, Сомали), а когда возникала угроза нефтяной блокады (вторжение Ирака в Кувейт в 1991 г.), то вели полномасштабные боевые действия. Такая стратегия до поры до времени себя оправдывала. Однако сейчас ситуация меняется.

В 2001 г. Китай потреблял 5 млн баррелей нефти в день (что в 4 раза меньше, чем США), причем ему требовалось импортировать всего 1,7 млн баррелей нефти в день. По итогам декабря 2012 г. Китай, обогнав США, вышел на первое место в мире по объемам нетто-импорта нефти с показателем 6,12 млн баррелей в день [32]. Это значительно усилило конкуренцию Китая с традиционными потребителями углеводородов и, прежде всего, с США. Несмотря на то, что часть нефти Китай может получать из Казахстана и России, ее значительная часть будет поступать с Ближнего Востока, из Африки и Латинской Америки. Помимо Китая, проблема получения и доставки углеводородов имеет исключительную важность также для Японии и Индии – двух других весомых региональных игроков.

Поскольку основные источники углеводородов находятся в Африке и в зоне Персидского залива, то всем азиатским потребителям они доставляются по маршрутам, пролегающим через Индийский океан и западную часть Тихого океана. Таким образом, оба эти водных бассейна в последнее время рассматриваются США как единое стратегическое целое. Данный регион является сферой противоборства интересов таких крупных игроков, как США и Китай. Необходимость обеспечения собственной энергетической безопасности ведет к наращиванию военного присутсвия (прежде всего ВМС) в данном регионе.

Для отстаивания своих интересов Китай активно наращивает свои вооруженные силы и их техническое оснащение. В 2012 г. Китай выделил на развитие безопасности страны значительные средства, достигшие суммы, по разным оценкам, от 100 до 180 млрд долл. [33] Как следствие, на сегодняшний день Народно-освободительная армия Китая (НОАК) владеет одним из самых больших в мире потенциалов, фактически уступающим лишь потенциалу ВС США. Так, численность НОАК на 2012 г. составляет 2 250 тыс. человек [33]. При этом НОАК прошла масштабную программу перевооружения и обладает современной боевой техникой, в т.ч. ракетно-ядерными системами дальнего действия наземного и морского базирования, космическими средствами разведки, управления и связи, атомными подводными лодками и надводными кораблями основных классов, ударной, истребительной и военно-транспортной авиацией, а также всем спектром вооружения сухопутных войск, включая системы ВТО. В рамках реализации национальной военной политики в АТР Китай прибегает к последовательному наращиванию сети военных баз в юго-восточных районах страны, а также увеличивает потенциал китайских ВМС, контролирующих прибрежные моря и выходы в Тихий и Индийский океаны. В этой связи особое внимание в НОАК уделяется созданию современного авианесущего флота, а также дальней авиации [33, 71].

Одновременно с этим пространство АТР является зоной ответственности Тихоокеанского командования ВС США, в котором в настоящее время проходит активное наращивание сил и средств (рис. 1.8). Обеспечив для себя вооруженное доминирование в данном регионе, США решат задачу неприкосновенности своих интересов и давление на страны АТР и, прежде всего, на Китай за счет угрозы военного перекрытия поставок углеводородного сырья странам-потребителям [18, 20, 26, 71].

На противостояние с Китаем направлен подрыв американцами стабильности стран Северной Африки и Ближнего Востока. Они рассчитывают на то, что уничтоженная инфраструктура этого региона потребует колоссальных финансовых вложений, способных оживить экономику США. В результате спровоцированной и управляемой американцами «арабской весны» созданы условия для объединения государств исламского мира в «новый халифат» в процессе замены их руководителей на американских ставленников. Кроме сохранения контроля над мировыми нефтегазовыми ресурсами, вооруженный Западом союз мусульманских государств призван защитить интересы США на азиатском Востоке и в Африке от растущей экономической и

военной мощи Китая. Следующим логичным шагом США будет усиление давления на государства, препятствующие сохранению американского доминирования на Ближнем Востоке, – Сирию и Иран.

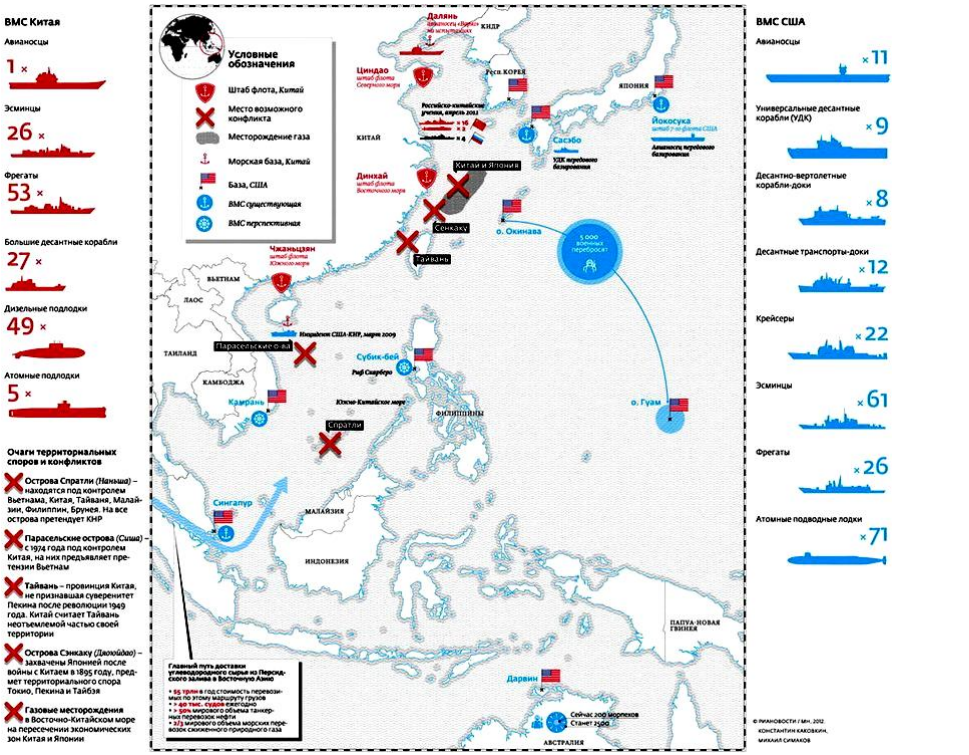


Рис. 1.8. Военные базы и соотношение сил ВМС США и Китая в АТР [33]

В результате предполагаемой победы США в «большой войне» намечена реализация проекта «Большой Ближний Восток» [18] с нанесением политического ущерба Китаю и России. В ходе него Россия и Китай теряют свое влияние в Средиземноморье и Среднем Востоке. Россия уходит из Южного Кавказа и Центральной Азии, а Китай лишается стратегического поставщика энергоносителей [20]. Проект «Большой Ближний Восток» полностью исключает для России перспективу мирного, относительно спокойного развития, поскольку нестабильный и находящийся под внешним управлением США Южный Кавказ станет зоной постоянной напряженности и детонатором дестабилизации ситуации не только на Северном Кавказе, но и в Россий-

ской Федерации. При этом главную дестабилизирующую роль будет играть исламский фундаментализм.

4. Ведение США информационной войны и использование стратегий управляемого хаоса для достижения собственных геополитических интересов. Как показано в работе В. Бурбаки [24], крупномасштабная война является способом для США быстро вернуть теряемое геополитическое лидерство. При этом ставка делается не только на ведение обычных боевых действий, но и на нелетальные способы войны на основе информационных операций и технологий «управляемого хаоса». Отладка форм и способов проведения таких операций ведется в рамках «арабской весны», однако данные операции пока не могут рассматриваться как универсальный способ воздействия, поскольку в силу цивилизационных и культурных особенностей они пока неприменимы к Китаю и ряду других стран [18, 47].

Желая закрепить за собой роль мирового лидера, США официально представили новую стратегическую доктрину американской дипломатии – концепцию «лидерства через гражданскую власть» [18]. В новой доктрине заявленный тезис «американское лидерство через гражданскую власть» связывает представление о «правильной» гражданской власти с требованием к единомыслию в «общегосударственном подходе» к международной политике. На первое место в дипломатии выносится претворение в жизнь «целей тысячелетия» и «глобального управления» [18]. Госдепартамент США в рамках новой доктрины должен обеспечивать американским транснациональным компаниям возможность участвовать в выбранных приоритетных областях глобальной экономики. К ним относится – реализация национальной продовольственной безопасности, лидерство в медицинской и фармацевтической отраслях, борьба с изменением климата, а также лидерство в гуманитарных акциях при чрезвычайных ситуациях [18, 25, 47].

Новая дипломатическая доктрина США претендует на большую эффективность вмешательства в глобальную экономику и мировую политику благодаря широкому привлечению частных инвестиций, использованию новейших информационных технологий и переформатированию идеи «народной дипломатии». Доктрина балансирует между прямым вмешательством администрации США в ситуацию в третьих странах в целях создания благоприятных предпосылок для американского бизнеса и смещением ответственности за процессы дестабилизации на внутреннее гражданское общество этих стран, к которому якобы переходит лидерство в процессе изменений.

Параллельно США активно продвигает идею создания глобального Альянса молодежных движений [18], через которые Госдепартамент США сможет участвовать в финансировании, технической и организационной поддержке, обучении и координации оппозиционных молодежных движений в мировом масштабе, прежде всего на Ближнем Востоке, в Северной Африке, в Латинской Америке, а также в странах бывшего СССР. Партнерами Госдепартамента в создании глобального Альянса молодежных движений стали компании-лидеры информационного пространства «Facebook», «Google», «YouTube», MTV, AT&T, «JetBlue» и др. Таким образом, на смену традиционным сценариям «цветных революций» пришла схема контроля над общественными движениями через использование новейших информационных технологий, внедрение схем управления молодежными движениями через глобальную информационную сеть Интернет. Применяя методы теории хаоса, информационных войн и новую концепцию «лидерства через гражданскую власть» политико-дипломатическое и военное руководство США предполагает, что дестабилизация ситуации в мире и последующее управление ею – оптимальный способ обеспечения интересов своей страны.

1.2. Прогноз развития мировой геополитической ситуации

Анализ текущих мировых тенденций в геополитике [18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 32, 33, 34, 35, 36, 54] позволяет спрогнозировать противостояние интересов стран, международных организаций, мировых и региональных центров силы во имя достижения своих геополитических целей.

1. Относительно ведущих стран мира и международных организаций [35].

- США будут отстаивать свою роль как ведущего центра силы, способного оказывать решающее влияние на основные политические, экономические процессы, а также процессы безопасности в мире.
- КНР последовательно будут укреплять свой экономический и военный потенциалы для обеспечения своего лидерства в Азиатско-Тихоокеанском регионе, а в последующем – в мире.
- Европейский Союз будет решать свои финансово-экономические проблемы, проблему выхода Великобритании из

ЕС, миграционные проблемы, а также возобновлять единство и динамическое развитие организации, включая составляющую своей безопасности.

2. Относительно региональных и сверхрегиональных стран [35].

- Россия будет восстанавливать свою роль как лидера на постсоветском пространстве и на Ближнем Востоке для укрепления своих региональных и глобальных позиций.
- Индия будет усиливать свои позиции в Юго-Восточной Азии, а также прилагать усилия для обеспечения регионального паритета с КНР.
- Бразилия и Аргентина будут укреплять свои региональные позиции в регионе Латинской Америки с перспективой выхода на мировой уровень.
- Турция – будет укреплять свои позиции регионального лидера в Ближневосточном регионе, а также на Черноморском и Кавказском направлениях.
- Иран будет предпринимать попытки возглавить шиитские страны и неформальные политические силы Ближневосточного региона.

С учетом вышеуказанного основные мировые процессы сфокусируются на трех основных регионах, а именно [35]:

- на Азиатско-Тихоокеанском регионе и Юго-Восточной Азии;
- на регионах Ближнего Востока и Северной Африки;
- на Европе и на постсоветском пространстве (включая, прежде всего, Украину и Кавказ, Каспийский регион и Центральную Азию).

При этом к дополнительным факторам, влияющим на положение дел в мире и отдельных регионах, следует отнести [35]:

- продолжающийся конфликт в Сирии и в целом на Ближнем Востоке, в который втянуты основные мировые геополитические игроки – Россия, США, Евросоюз;
- сосредоточение стран Евросоюза, прежде всего, на своих внутренних социально-политических проблемах, связанных с неконтролируемой миграцией мусульманских беженцев из ближневосточного региона;
- нарастание напряженности в политической и экономической сфере на Украине, переход в активную фазу вооруженного конфликта на востоке Украины, расширение сфер

экономического и политического давления на Россию в связи с восточно-украинским и крымским вопросом;
- активизацию усилий ведущих стран мира и, в частности, России в деле освоения Арктики с целью получения доступа к ее природным ресурсам;
- сохранение позитивной динамики в развитии стран Ближнего Востока, Латинской Америки и Южной Африки, в т.ч.: Саудовской Аравии, Объединенных Арабских Эмиратов, Катара и Турции, Бразилии и Аргентины, Южноафриканской Республики.

Вместе с тем сохранятся основные вызовы и угрозы мирового и регионального масштабов, к которым можно отнести [18, 19, 20, 35]:
- негативные последствия мирового финансово-экономического кризиса и возможность возникновения новых кризисных процессов в мировой экономике;
- возможность возникновения новых крупномасштабных вооруженных конфликтов в странах Африки, Ближнего Востока, Центральной Азии и АТР, спровоцированных борьбой за ресурсы, а также политическими, экономическими, межрелигиозными и межнациональными противоречиями;
- высокую вероятность эволюции до уровня глобальных геополитических игроков политически неформальных групп и объединений, построенных по надгосударственному сетевому принципу, таких как «Исламское государство» или «Аль-Каида»;
- активизацию процессов неконтролируемого распространения оружия массового поражения и средств его доставки;
- повышение угрозы масштабных стихийных бедствий и техногенных катастроф на фоне глобальных климатических изменений.

В среднесрочной перспективе до 2020 г. следует ожидать расширения спектра глобальных вызовов и угроз, вызванных результатами передала сфер влияния при формировании многополярной системы мироустройства, проходящего на фоне мирового экономического кризиса. Сегодня становится нормой практика применения ведущими геополитическими игроками стратегии односторонних действий. Это дискредитирует существующую систему обеспечения безопасности в мире и стимулирует нарастание конфликтного потенциала в ряде регионов. Разрастаются масштабы международной террористической деятельности. Все это способствует эскалации существующих и воз-

никновению новых вооруженных конфликтов. Большинство экспертов считают, что локальные конфликты будущего будут носить характер восстановления и поддержания мира. Практика показала, что активная фаза в них заканчивается очень быстро, а потом надо или уходить, или вести бесконечную партизанскую войну. Таким образом, ограниченные региональные войны, очевидно, останутся в обозримом будущем наиболее распространенной формой межгосударственных вооруженных конфликтов.

Основной точкой мировой напряженности является потенциальный конфликт Китая и США. Америка стремительно теряет статус единственной супердержавы, и ее место может занять Китай. На вершине господства миром всегда остается только одна сила, и когда ситуация достигнет критической точки, может начаться война, а поводом для этого послужит Тайвань, который Китай рано или поздно решит подчинить себе, а США вероятно постараются этому помешать. Вероятность возникновения большой войны невелика, но каждая крупная держава должна быть к ней готова.

Помимо этой гипотетической войны мирового масштаба, в настоящее время резко возросли угрозы локальных и региональных конфликтов. Многосторонние конфликты разной степени интенсивности сегодня имеют место на Ближнем и Среднем Востоке (Сирия, Ирак, Израиль, арабские страны Северной Африки, Мали, Иран, Афганистан), на Юге Европы (Югославия и постюгославские страны, Грузия, Армения, Азербайджан), непростая обстановка складывается и в Южной Азии (между Индией и Пакистаном).

Далее представлен анализ военно-политических и экономических процессов в основных регионах мира, а также основные направления развития геополитической обстановки в них.

1.2.1. Азиатско-Тихоокеанский регион и Юго-Восточная Азия

Учитывая рост экономических потенциалов Китая и Индии, Азиатско-Тихоокеанский регион и Юго-Восточная Азия в ближайшей и среднесрочной перспективе будут непрестанно превращаться в новый и все более масштабный центр деловой активности в мире. С одной стороны, это будет замедлять экономическое развитие АТР, а с другой – превращать его в объект для пересечения интересов, как ведущих мировых, так и региональных стран. Поэтому на фоне своего позитивного экономического развития Азия будет характеризоваться

как новый источник напряженности с потенциальными конфликтами и войнами, а также как арена международного противостояния глобального уровня. В первую очередь имеется в виду обострение борьбы между США и Китаем за влияние в АТР, а также возможное усиление региональных противоречий между Китаем и Индией, Индией и Пакистаном в Юго-Восточной Азии.

США, сдерживая амбиции Китая, и далее будут отстаивать свои интересы в АТР. В рамках такой стратегии будет наращиваться военное и военно-морское присутствие США в регионе путем развертывания американских военных баз в Австралии, а также направляться дополнительные военные контингенты в Японию и Южную Корею, разворачиваться системы ПРО в регионе. Кроме того, США будут наращивать свои экономические связи и политическое влияние с теми странами АТР, которые имеют проблемы в отношениях с КНР: Австралией, Японией, Южной Кореей, Вьетнамом, Филиппинами и Малайзией [35, 71].

В то же время на стратегическом уровне США будут принимать меры по созданию, развитию и принятию на вооружение военных космических систем, МБР в обычном снаряжении, нового поколения самолетов-истребителей F-35, систем высокоточного оружия, вооружения, основанного на новых физических принципах. Внимание будет уделено также экспедиционным силам.

Китай, отстаивая свои стратегические интересы в Азиатско-Тихоокеанском регионе и Юго-Восточной Азии, будет повышать свои военные возможности, а также наращивать финансово-экономическое сотрудничество со странами-партнерами. Китай продолжит реализацию программ по созданию своего авианесущего флота, строительству атомных подводных лодок, усилению Восточного и Южного флотов НОАК, наращиванию системы военно-морских баз в Восточно-Китайском и Южно-Китайском морях, а также в районе Малаккского пролива – основного пути транспортировки энергоносителей в КНР из региона Ближнего Востока и Персидского залива [35].

Однако США и КНР будут стараться найти взаимные точки соприкосновения в наиболее важных вопросах мировой и региональной безопасности, а также возможности углубления сотрудничества в экономической сфере. Это обусловлено сильной взаимозависимостью экономик двух мировых лидеров и недопустимостью для них ухудшения развития ситуации в условиях продолжающего экономического кризиса.

Новым источником напряженности в АТР, который может вылиться в вооруженные конфликты, послужит борьба стран региона за доступ к спорным месторождениям нефти и газа на шельфах Восточно-Китайского и Южно-Китайского морей. Это противоречия, возникшие, между КНР и Японией, Китаем и Вьетнамом, а также КНР, Вьетнамом, Филиппинами и Малайзией. Учитывая важность вопросов доступа к энергетическим ресурсам в условиях высокой вероятности дальнейшего осложнения ситуации в странах Северной Африки и Ближнего Востока (основных поставщиков энергоносителей в АТР), упомянутая борьба может перерасти в полномасштабный региональный военный конфликт. О развитии ситуации в данном направлении свидетельствует концентрация конкурирующими сторонами сил своих ВМС вблизи спорных островных территорий [35].

Роль отдельного игрока в Азиатско-Тихоокеанском регионе и в дальнейшем будет принадлежать Российской Федерации, развивающей свою стратегию сдерживания Китая, угроза которого на Дальнем Востоке в отношении России возрастает. В рамках этой стратегии РФ будет усиливать свой военный потенциал в Дальневосточном регионе, а также диверсифицировать экономические связи со странами АТР, наращивая сотрудничество с региональными соперниками КНР, в т. ч. в военной и военно-технической сферах. Одновременно Россия будет заинтересована в развитии финансово-экономического сотрудничества с Китаем.

1.2.2. Ближний Восток и Северная Африка

В 2017-2018 гг. главным событием на Ближнем Востоке может стать разрешение конфликта в Сирии и победа над террористами «Исламского государства» как вследствие успешных действий сирийских войск, так и внешнего силового вмешательства в ситуацию извне.

Сирийский конфликт имеет свои особенности. Так, представители Саудовской Аравии пытаются скоординировать вместе со своими союзниками, прежде всего США, размещение войск арабской коалиции на территории Сирии. При этом США это выгодно, так как они считают, что войска арабской коалиции на территории Сирии будут выполнять функции дополнительных региональных сил и помогут избежать втягивания американцев в конфликт. Турция также заинтересована в присутствии своих войск в коалиции, так как это поможет ей узаконить в глазах арабских соседей свое участие в сирийском конфликте. При этом Турция обеспокоена усилением присутствия в реги-

оне России и Ирана, и поэтому ищет дополнительной поддержки. Вместе с тем активизация участия арабских стран в сирийской гражданской войне может подорвать любые попытки создать единый фронт борьбы с «Исламским государством» в Сирии и в Ираке. А именно эти задачи провозглашаются в качестве основных в сирийском конфликте со стороны западных государств. Поддержка со стороны различных государств (финансами или оружием) противоборствующих сторон конфликта препятствует общим усилиям в борьбе с «Исламским государством». Военные действия между турками и курдскими отрядами народной самообороны у турецко-сирийской границы также мешают этому процессу. Кроме того, присутствие саудовских войск в Сирии нежелательно для Ирана, который оказывает значительную поддержку сирийскому правительству [54].

В случае смены сирийской власти возникнут предпосылки для реализации стратегических планов США по смене руководства Ирана, который лишится своего главного союзника на Ближнем Востоке. По оценкам американских экспертов, достичь в Иране этой цели можно как спровоцировав массовые социальные беспорядки (по сирийскому сценарию), так и возглавив силовую операцию против Ирана под предлогом не допустить для последнего возможности получения ядерного оружия.

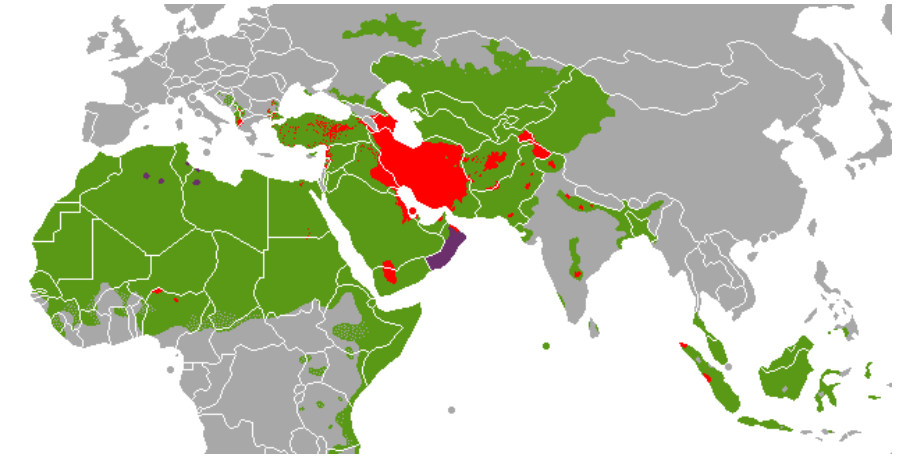


Рис. 1.9. Расселение суннитов и шиитов на Ближнем Востоке

Такое развитие событий может иметь геополитические последствия регионального и мирового уровней. Так, изменится расстановка политико-религиозных сил в регионе, когда лидерство перейдет от

шиитских к суннитским странам и режимам, а именно: от Ирана и Сирии к Турции, Саудовской Аравии, ОАЭ и Катару. Это усилит позиции США в регионе и существенно снизит влияние России на Ближнем Востоке.

Что касается отстранения от власти нынешнего руководства Ирана, занимающего агрессивные антизападные позиции, то оно будет способствовать усилению как военной, так и энергетической безопасности Европы. Ведь фактически ликвидируется иранская ракетная угроза, а Исламская Республика Иран получит возможность подключиться к европейским энергетическим проектам.

В настоящее время с Ираном заключена ядерная сделка, которая состоялась при активном участии России и которая позволяет рассчитывать на предотвращение возможности получения Ираном ядерного оружия. Это должно снизить потенциальную напряженность в регионе Ближнего и Среднего Востока, обусловленною иранской ядерной программой.

При этом США рассчитывают на преференции и надеются восстановить сотрудничество с Ираном в своих интересах. В частности, снятие международных санкций против Ирана расширит возможности выхода иранских нефти и газа на мировой и европейские рынки, что позволит использовать иранскую территорию для реализации планов по созданию «Южного энергетического коридора» (предполагает строительство новых транспортно-энергетических систем от Каспия и Центральной Азии к Европе в обход России).

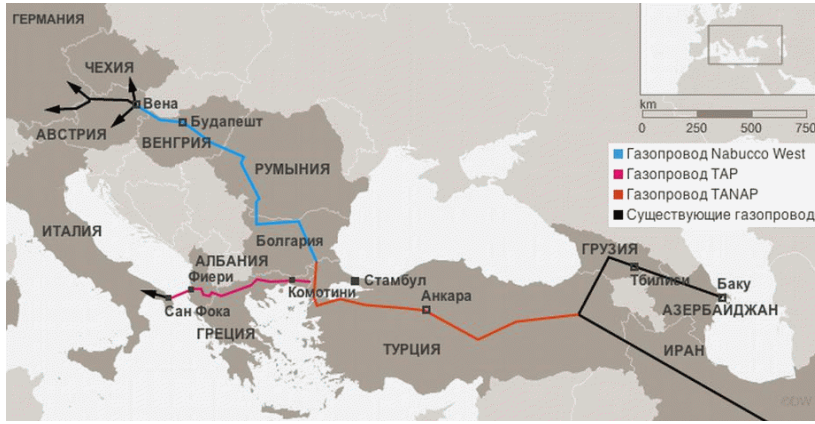


Рис. 1.10. Южный энергетический коридор

В целом вышеприведенные процессы положительно скажутся на развитии региона. Однако в случае затягивания сирийского кризиса или в случае иранского вооруженного конфликта ситуация на Ближнем Востоке резко ухудшится.

1.2.3. Европа и постсоветское пространство

Положение дел в Европе и на постсоветском пространстве будет характеризоваться усилением противоречий между западными странами и Российской Федерацией в ключевых сферах их отношений из-за политики по возрождению роли России как крупного мирового государства. Запад воспримет это как угрозу своей безопасности, особенно в условиях проведения российской стороной собственной национально-ориентированной политики на Ближнем Востоке и на постсоветском пространстве. В рамках такой политики Россия попытается возобновить свой политический и экономический контроль над постсоветским пространством, укрепить свои позиции в европейском энергетическом секторе, удержать военный паритет с НАТО, а также противостоять формированию антироссийских политических процессов в странах ближайшего окружения. В этом контексте Россия активно наращивает военное присутствие в зонах потенциальных конфликтов (в Крыму, на российско-украинской границе, на Северном Кавказе), а также активизирует действия, направленные на расширение Таможенного союза и укрепление Организации Договора о коллективной безопасности (ОДКБ) как составляющих стратегического плана по созданию Евразийского союза.

В рамках потенциального противостояния с вооруженными силами Украины, блоком НАТО в Европе и исламским экстремизмом на Северном Кавказе руководство России усилит внимание к вопросам повышения боевых возможностей Российских Вооруженных Сил на Северо-Западном, Западном, Юго-Западном и Южном направлениях, в том числе и за счет реализации масштабных программ перевооружения войск Южного, Западного оперативно-стратегических командований ВС России. Кроме того, поддерживая свой стратегический ракетно-ядерный потенциал, Россия продолжит разработку и постановку на вооружение новых ракетных систем стратегического назначения.

На европейском направлении Россия продолжит расширение возможностей выхода на европейские энергетические рынки, создавая новые транспортно-энергетические коридоры в обход Украины и Белоруссии, в т. ч. газопровод «Северный поток». При этом зачастую

политическое значение указанных проектов будет превалировать над их экономической целесообразностью.

Российская сторона попытается также использовать финансово-экономические и социально-политические противоречия стран – членов ЕС для достижения собственных интересов – формирование России как мирового политического игрока с правом геополитического контроля постсоветского пространства, признания факта присоединения Крыма к России, снятие экономических санкций с России, устранение социально-политических барьеров для российской политической и бизнес-элиты в Евросоюзе.

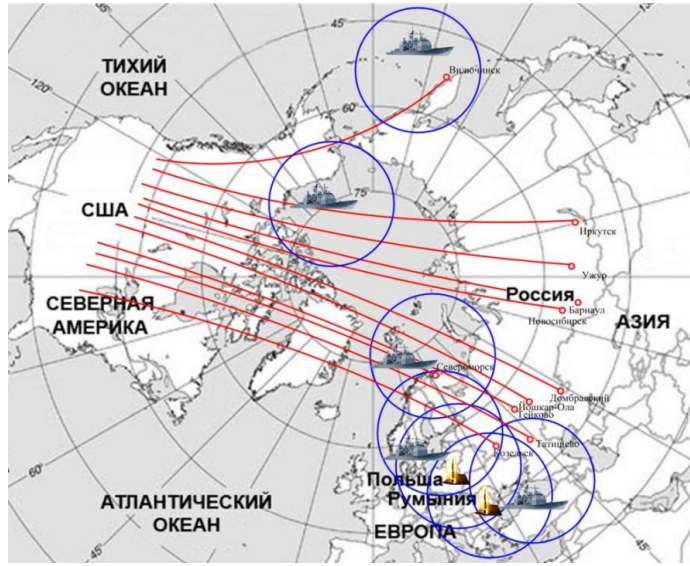


Рис. 1.11. Размещение противоракетных систем SM-3 в Европе

Европейский союз сосредоточится на мероприятиях по преодолению финансово-экономического кризиса, а также разрешении социально-политических проблем, обусловленных массовой миграцией мусульманского населения.

Как предполагают западные эксперты, благодаря мероприятиям финансового оздоровления, в ближайшее время возобновится позитивная динамика развития европейской экономики. Тогда же появятся благоприятные предпосылки и для решения политических проблем Европейского Союза, а именно: устранение противоречий между

странами – членами ЕС, возникшие в последнее время из-за разных подходов к проблеме преодоления финансово-экономического кризиса в еврозоне, а также в проблеме ассимиляции ближневосточных беженцев.

Оживление экономики европейских стран позволит им увеличить оборонные расходы, что будет способствовать укреплению НАТО и усилению европейской оборонной составляющей. Например, Североатлантический Союз во главе с США сможет реализовать планы развертывания полноценной системы ПРО в Европе.

Укрепляя свою оборону, страны ЕС во главе с ФРГ и Францией будут и в дальнейшем проводить общую внешнюю политику и политику безопасности, повышая эффективность и расширяя полномочия Европейского оборонного агентства, развивая оперативные возможности многонациональных боевых тактических групп в миротворческих зонах и в наблюдательных и тренировочных миссиях на территории других стран.

Отдельным важным для Европейского Союза останется вопрос снижения своей зависимости от российских энергоносителей. Считая это для себя стратегическим, ЕС приступит к практической реализации проекта «Nabucco» и других проектов в рамках «Южного энергетического коридора». Это позволит Европейскому Союзу интенсифицировать мероприятия по противодействию усилиям России по расширению своего влияния на постсоветском пространстве. Поэтому ЕС продолжит активное наращивание сотрудничества со странами бывшего СССР в рамках программы «Восточное партнерство», в первую очередь в плане подписания соглашений об ассоциации, создания зон свободной торговли и упрощения визовых режимов с Украиной, Молдовой, Грузией, Азербайджаном и Арменией. Среди важных направлений сотрудничества ЕС со странами Черноморско-Кавказского и Центрально-Азиатского регионов – активная реализация совместных энергетических проектов по выходу Азербайджана, Туркменистана, Казахстана и Узбекистана на мировые рынки энергоносителей, а также содействие урегулированию «вялотекущих» конфликтов на Украине, в Молдове, в Грузии и в Азербайджане.

Европейский вектор внешней политики США активизируется. Экономические связи США со странами ЕС будут углубляться, их энергетическая безопасность получит поддержку (в т. ч. за счет поставок американского сжиженного газа на европейский рынок). Активизируется также сотрудничество со странами СНГ. Так, США попыта-

ются сохранить свои европейские позиции в противовес растущему влиянию России в Европе и на постсоветском пространстве.

1.2.4. Россия

На сегодняшний день для России характерны два вида угроз – внешние и внутренние. Эти угрозы по времени наступления можно разделить на ближайшие, а также угрозы среднесрочной и долгосрочной перспективы.

1.2.4.1. Внешние угрозы масштабной войны

Из внешних угроз наиболее опасными можно считать:

- возникновение и эскалация военных конфликтов вблизи государственных границ России и внешних границ СНГ;
- резкая эскалация масштабов международного терроризма против России и ее союзников, в т. ч. с возможным использованием оружия массового поражения;
- увеличение военно-технического отрыва ведущих держав и наращивание их возможностей по созданию ВВСТ новых поколений, что ведет к качественно новому этапу гонки вооружений и существенному изменению содержания, форм и способов ведения военных действий;
- существование территориальных претензий к России со стороны сопредельных государств.

Наиболее полно и наглядно значимость этих угроз для РФ проявилась в ходе расширения НАТО на восток, а также в ходе событий на Северном Кавказе и на Украине.

Сейчас доминирует экспертное мнение, которое утверждает, что большие войны между государствами в будущем маловероятны. Тем не менее полностью исключать вероятность их возникновения нельзя. Разумеется, это не означает того, что мир стоит на пороге военного столкновения России и НАТО но поскольку после завершения «холодной войны» Альянс не был распушен, то Москва продолжает расценивать его в качестве потенциального противника. Таким образом, хотя вероятность войны России с Западом крайне мала, но она сохраняется.

Так, в решении вопросов межгосударственных отношений уже сейчас США делают и будут делать ставку на обеспечение своих национальных интересов в критически важных для себя и своих союзников районах мира. Вне всякого сомнения, превалирующее влияние

на определение повода для развязывания войн и вооруженных конфликтов оказывали американские экономические и политические интересы.

Четкое проявление контуров исчерпаемости мировых сырьевых ресурсов заставляет американцев учитывать это и объявлять зоной своих интересов регионы, имеющие значительные природные запасы и, прежде всего, нефти и газа. Именно поэтому все регионы и пространства, содержащие эти ресурсы, вовлечены в планы их стратегической экспансии, и именно отсюда проистекает «дружеское внимание» США к странам Ближнего Востока, Прикаспийского региона, Грузии, России и другим ресурсо-содержащим и транзито-пригодным странам и регионам мира. Достижение своих целей в этих регионах они будут пытаться осуществить любыми путями [19, 29].

При относительно небольшой удельной численности населения (порядка 2,5%) США потребляет до 40% добываемых в мире природных ископаемых, импортируя при этом около половины нефти, за счет которой на 40% удовлетворяет свои базовые потребности в энергии. Поэтому по мере возрастания зависимости своего экономического благополучия от доступа к мировым рынкам и запасам природных ресурсов военно-силовая компонента политики США будет систематически усиливаться, в т. ч. и по отношению к России в силу специфики ее геополитического положения. А это значит, что при возникновении военных действий со стороны США война для России будет оборонительной в силу национальной политики и существующей военной доктрины [3, 29].

В тоже время потенциально большая опасность угрожает России с Востока. Никто не знает, как в будущем поведет себя набирающий силу Китай. Ему понадобятся ресурсы и жизненное пространство, поэтому он может обратить внимание, прежде всего, на российские Сибирь и Дальний Восток, где мало жителей, много территорий и большие запасы природных ресурсов. Если военный потенциал Пекина будет расти теми же темпами, вероятность нападения Китая на Россию резко возрастет. При этом поводом может послужить, например, защита прав проживающих на Дальнем Востоке китайцев [20, 29].

Военная опасность со стороны Китая обусловлена следующими причинами. По многим макроэкономическим показателям Китай вышел, несмотря на кризис, на второе после США место в мировой экономике. А стремительный рост экономической и, как прямое следствие, военной мощи Поднебесной означает, что необходимые ей природные богатства и территории она не прочь брать силой, о чем в Пе-

кине заговорили уже практически открыто на достаточно высоком уровне [16, 29]. Виной тому – бурный рост экономики Поднебесной: дело не в какой-то особой агрессивности Китая, а в том, что экспансия для него – вопрос выживания его экстенсивной модели экономики. Что касается вектора экспансии Китая, то после потери своих позиций в Африке и на Среднем Востоке у Поднебесной остается одно направление – Север, то есть Сибирь и Дальний Восток [29]. Тем более что подобный сценарий развития событий уже прописан у Китая в его доктрине «Три севера, четыре моря», принятой Центральным военным советом Центрального комитета Коммунистической партии Китая еще в 1993 г.

Китаеведы отмечают, что по этой зашифрованной для понимания иностранцев доктрине занятый Китаем центр по закону перемен к 2019 г. одолеет «Три севера в пределах четырех морей» и тогда «XXI век станет веком Китая». А три севера – это «Североатлантический альянс, Россия как север Евразии и США в Новом Свете».

Оценивая возможность перехода «китайской опасности» в «китайскую угрозу», следует учитывать, что Китай имеет колоссальные людские ресурсы, активно ведет перевооружение своей армии на новые средства ведения крупномасштабной войны, вплоть до применения ядерного оружия. Осваивает китайская армия и новые формы и методы ведения войны – информационные и психологические операции, а также управление войсками на основе сетецентрической концепции. При этом основные предприятия оборонно-промышленного комплекса (ОПК) Китая находятся в глубине его территории и их поражение в случае войны возможно только с использованием стратегического оружия [29].

1.2.4.2. Внешние угрозы регионального военного конфликта

В среднесрочной перспективе в обозримом будущем наиболее распространенной формой межгосударственных вооруженных конфликтов для России окажутся ограниченные региональные войны. Такие войны могут быть спровоцированы такими основными угрозами как [29]:

- поддержка Россией Донецкой и Луганской народных республик в военном конфликте с Украиной, а также непризнание Украиной итогов референдума о присоединении Крыма к России;

- расширение конфронтации и втягивание России в долговременный конфликт на Ближнем Востоке по итогам ее военной операции против «Исламского государства» и сирийской оппозиции;
- военный конфликт в Южной Осетии, а также непризнание Грузией итогов конфликта 2008 г. в Южной Осетии;
- претензии Японии на Южно-Курильские острова.

При этом в настоящее время именно политический конфликт с Украиной, и военная операция в Сирии несут для России риск региональных войн в ближайшей перспективе.

«Украинский вопрос» как нарастающая угроза регионального конфликта с Украиной постепенно уходит в тень из-за потери к нему интереса как со стороны ЕС и НАТО, так и самих США. При этом становиться понятно, что Украина, судя по всему, пытается давить на Россию, оставалась на длительное время объектом для массовых информационных «экспериментов» со стороны США и ЕС. Попытки же украинского руководства использовать любые поводы для развязывания очередного скандала по отношению к России уже бесполезны. Поиски Украиной союзников среди противников России также вряд ли дадут положительные результаты в плане улучшения экономической ситуации в стране или ее скорейшей интеграции в ЕС. Кризис политической власти, внешнее управление в стране, отсутствие желания наладить нормальный диалог с Россией только усугубляют украинский кризис, который приобретает все более затяжной характер, ведет к дальнейшему обнищанию народных масс Украины, экономическому коллапсу и дефолту государства [54].

Что касается военной операции России в Сирии, то региональные и глобальные участники сирийского конфликта преследуют совершенно разные цели, и хотя все больше стран готовы увеличить свой вклад в борьбу с «Исламским государством», их внимание пока сосредоточивается на своих врагах. России в этой ситуации необходимо действовать прагматично, с учетом исторического опыта Советского Союза, когда союзники и друзья на Ближнем и Среднем Востоке мгновенно перестраивались после прекращения помощи [54].

1.2.4.3. Внутренние угрозы

Внутренние угрозы военной безопасности России обусловлены долгосрочными последствиями общественно-политического и соци-

ально-экономического кризиса в стране. Эти угрозы характеризуются следующими факторами [29, 65]:

- обострением межнациональных отношений, региональным сепаратизмом и религиозным экстремизмом, создающими благоприятные условия для возникновения внутренних вооруженных конфликтов;
- существенным снижением ВВП и темпов роста экономики в условиях введения экономических санкций и снижения международного финансового рейтинга страны, что принципиально ограничивает возможности государства по финансированию своих оборонных потребностей, в т.ч. в области развития ВВТ, технического оснащения и обеспечения ВС РФ;
- значительным ослаблением научно-технического, технологического и интеллектуального потенциала, а также внешней технологической, экономической и частично идеологической зависимостью страны.

Кроме того, Россия в настоящее время стала прямым объектом внешней вооруженной агрессии еще одного стремительно формирующегося мирового «центра силы»: «панмусульманского» салафитского проекта, который при поддержке нефтяных монархий Саудовской Аравии и стран Персидского залива активно формирует и поддерживает экстремистские ваххабитские движения не только в исламских регионах России, но и по всей ее территории. Данный проект ставит своей целью вычленение из состава России мусульманских регионов, создание там исламских эмиратов с зачисткой немусульманского населения. Накопившиеся в этих регионах многолетние проблемы – тотальная коррупция, клановость, деградация образования и социальной сферы в целом, имущественное неравенство, неразвитость производственных секторов экономики и безработица – стали питательной средой для политических сил экстремистского толка. После всплеска их активности в 90-е гг. XX века, новому руководству страны в начале 2000-х гг. удалось сбить ваххабитскую волну, но за последние три года приходится констатировать новое и скачкообразное усиление активности экстремистских движений и ваххабитских организаций, который подается как «исламский социализм». Неприятной новостью для структур федеральной власти стало появление экстремистских формирований на территории ранее стабильных исламских регионов страны: Татарстана, Кабардино-Балкарии, Карачаево-Черкессии. Не в последнюю очередь это связано с тем, что салафитские центры Катара

и Саудовской Аравии в ходе «арабской весны» в Судане, Египте и Ливии, отработав технологии свержения неугодных режимов, теперь решили, что вполне могут повторить подобные «революции» на территории России, а потому многократно увеличили финансирование экстремистских организаций. Кроме того, идет накопление оружия, взятия под контроль местных органов власти и захват духовных центров. Все это позволяет сделать вывод о неизбежности эскалации террористической активности в регионе, вплоть до перерастания ее в вооруженный мятеж и диверсионную войну [10, 29].

1.2.4.4. Общие выводы

На период до 2030 г. уровень существующих и потенциальных военных опасностей для РФ в значительной степени способен повыситься. Он определяется борьбой ведущих государств за топливно-энергетические и трудовые ресурсы, рынки сбыта товаров и жизненное пространство. В содержании форм и способов ведения вооруженной борьбы будет происходить переориентация от всеобщей ядерной и обычной войны на военные действия локального и регионального масштаба.

В результате проведенной системно-динамической оценки угроз для национальной безопасности РФ стало возможным сформулировать три основных сценария военных конфликтов, в которые может быть вовлечена наша страна в ближайшие 15-20 лет.

1. Большой конфликт (США, страны НАТО, Китай). По своему характеру такая война будет [29]:

- высокоинтенсивной и высокотехнологичной, поскольку каждая из указанных выше стран будет стремиться нанести первый обезоруживающий удар высокоточным оружием по нашим стратегическим ядерным силам, системам разведки, ПВО, управлению и связи в космосе, воздухе и на суше;
- с массированным применением обычных сил и средств ВТО в первом эшелоне атаки, чтобы за кратчайший срок нанести поражение нашим войскам и выполнить основные задачи до принятия решения о нанесении ответного ядерного удара, делая его невозможным, или до начала политических переговоров.

При этом на стратегическом уровне такому конфликту может предшествовать период нарастания конфликтного потенциала между

сторонами, что позволит силами и средствами разведки своевременно вскрыть военные приготовления и провести необходимые мобилизационные мероприятия.

2. Региональный пограничный конфликт (Украина, Япония, Грузия). По своему характеру такой конфликт будет [29]:

- скоротечным, ввиду ограниченности военных задач и стремления решить его без втягивания противоборствующих сторон в «полноценную» войну;
- локальным, когда регион боевых действий будет ограничен рамками непосредственной конфликтной зоны (спорные территории, анклавы проживания той или иной народности и т.п.).

При этом началу конфликта также может предшествовать заметный период нарастания конфликтного потенциала, что позволит России провести необходимые военные приготовления.

3. Внутренний военный конфликт, контртеррористическая операция. По своему характеру такой конфликт будет [29]:

- вялотекущим, поскольку противник сделает ставку на диверсионную войну и тактику «булавочных уколов», т.е. изматывание федеральных силовых структур террористическими актами и локальными ударами;
- продолжительным, т.к. победа в таком конфликте возможна только при критической усталости одной из воюющих сторон, разочарованием в целях конфликта вовлеченного в него населения и изоляцией района боевых действий, перекрытием финансовых и ресурсных источников, подпитывающих одну из сторон конфликта;
- гибридным и неимеющим полноценных боевых столкновений.

В тексте действующей Военной доктрины РФ в частности утверждается, что особенностями современных военных конфликтов является непредсказуемость их возникновения. Это будет верно только при пассивности или безответственности разведывательных сил различного назначения России [29, 56].

При всей сложности современной обстановки следует иметь в виду, что, по оценкам экспертов, наибольшая военно-стратегическая опасность для России проявится через 7-10 лет. За это время возможности глобальной системы противоракетной обороны США, как наземного, так и морского базирования, превысят действенность ее преодоления стратегическими ядерными силами России. Поэтому

времени на раскачку в решении этой проблемы у России практически нет. Более того, оно может сократиться за счет интенсификации технологического прогресса США и стран НАТО. Имеются все основания полагать, что новый этап «холодной гибридной войны» продлится достаточно долго, поскольку происходящее обострение обстановки носит системный характер. Это связано с началом процесса смены мирового гегемона, который может, по некоторым оценкам, продолжаться 15-30 лет и вызвать потрясения, сравнимые по своим масштабам с событиями 1914 и 1945 гг. [54].

Кроме того, в последнее время появились новые вызовы и угрозы национальной безопасности России, которые подлежат нейтрализации [54]:

- прежде всего, США намереваются сохранить свое доминирование в мировых процессах путем ограничения самостоятельной внешней и внутренней политики России;
- НАТО активизирует военную деятельность вблизи границ с Россией;
- США и их союзники наращивают и модернизируют наступательные потенциалы, развертывают новые виды вооружений, создают глобальную систему ПРО, прежде всего, вокруг России, размывают структуру глобальной безопасности;
- осложняется мировая демографическая ситуация, нарастают проблемы окружающей среды и продовольственной безопасности;
- ощущается дефицит пресной воды, а также последствия изменения климата;
- получают распространение эпидемии, ряд которых вызван новыми, неизвестными ранее вирусами;
- остро встает вопрос обеспечения энергетической безопасности и территориального развития.

Для нейтрализации этих угроз, прежде всего, необходимо [54]:

- восстановить экономический суверенитет России, прекратить отток из страны инвестиционных ресурсов, сформировать конкурентную экономику, основанную на новом информационно-технологическом укладе;
- продолжить формирование широкой международной коалиции, направленной на устойчивое развитие на основе равноправных и справедливых механизмов экономического сотрудничества (АТЭС, ШОС, БРИКС);

- усовершенствовать систему государственного управления;
- повысить уровень культуры, формирование русского национального менталитета, ориентированного на поддержку традиционных ценностей, принять меры к консолидации общества.

Поэтому основными стратегическими задачами для России должны быть следующие [54]:

- на ближайшее время – выдержать давление Запада и сформировать в российском обществе национальное оборонное сознание;
- на среднесрочную перспективу – укрепиться экономически, идеологически и в военном отношении, сформировать патриотически-ориентированный тип личности;
- на долгосрочную перспективу – одержать геополитическую победу и выйти в лидеры нового мирового порядка.

Для защиты своих интересов Россия проводит сегодня внешнюю политику, исключающую затратную конфронтацию, в том числе - новую гонку вооружений. Применение военной силы рассматривается как крайняя мера, которая может быть использована лишь после исчерпания политических, экономических, дипломатических и других невоенных средств. При этом Россия готова сотрудничать со всеми государствами, но на принципах равноправия, взаимного уважения, невмешательства во внутренние дела государств, взаимовыгодного сотрудничества, политического разрешения глобальных и региональных кризисных ситуаций [54].

Основными задачами России остаются улучшение жизни населения, обеспечение безопасности в сферах здравоохранения, культуры, экологии, рационального природопользования. Эти задачи четко определены в новой Стратегии национальной безопасности Российской Федерации. Особого внимания требуют также вопросы информационной безопасности. С этой целью в 2016 г. была принята новая Доктрина информационной безопасности РФ [54].

Главное, что решение всех этих вопросов невозможно без перехода на новый уровень технологического развития, повышения роли науки и технологий, качества образования, рационального импортозамещения. Оборонно-промышленный комплекс остается передовым в модернизации производства, поэтому одной из важнейших задач является диверсификация производства и увеличение выпуска гражданской продукции на оборонных предприятиях [54].

1.3. Анализ влияния информационно-технической революции на глобальные мировые тренды

1.3.1. Информатизация и глобализация общества как результат информационно-технической революции

Конец XX века характеризовался масштабными изменениями в жизненном укладе – колоссальные достижения в различных отраслях науки и техники привели к глубоким изменениям в области глобализации общества. Важнейшей движущей силой этих процессов стала информатизация: глубокое проникновение информационных и коммуникационных технологий во все сферы жизни и деятельности человека. Тотальная информатизация общества привела к тому, что среди совокупности сфер жизнедеятельности современного общества на первое место выходит принципиально новая сфера – информационная. Новой сфере жизнедеятельности свойственны как новый ресурс – информация, так и новые противоречия, вызванные борьбой за обладание этим ресурсом.

Выделяются следующие основные признаки информационного общества [16]:

- формирование единого мирового информационного пространства и углубляющаяся экономическая взаимозависимость;
- переориентация экономик наиболее развитых в информационном отношении стран в сторону максимального развития непроизводственного сектора;
- формирование информационного и технологического рынков наряду с традиционными рынками (труда, сырья и т.п.), в процессе чего информационные ресурсы становятся реальными (т.е. приносящими конкретную финансовую выгоду) ресурсами государства;
- растущая зависимость социально-экономических и государственных институтов от стабильной работы различных инфраструктур, прежде всего информационных;
- многократное повышение доступности информационных ресурсов и услуг для общественного и личного использования;

- изменение структуры рынка труда в сторону повышения доли непроизводственной и интеллектуальной деятельности, что повышает требования к квалификации и профессионализму работника, который должен полноценно использовать технические и информационные нововведения;
- повышение требований к обеспечению личной, общественной и государственной информационной безопасности: разработка эффективной правовой базы для защиты государственных интересов, гарантий прав граждан и общественных институтов на получение, распространение и использование информации, создающей устойчивый баланс интересов между этими структурами.

При этом для информационного общества характерны следующие фундаментальные принципы [79]:

- государство есть надстройка над обществом, поэтому государство не в состоянии формировать новое общество, оно может лишь не мешать и пытаться трансформироваться соответственно изменениям в обществе (например, по типу «электронного правительства»);
- современное постиндустриальное общество сохранило традиционную основу общественных отношений – иерархию, новое общество базируется на принципиально новой, сетевой модели. Информатизация и «сетевизация» общества влечет за собой колоссальные изменения в экономике, политике, самой структуре власти, обеспечении безопасности и др. Также это влечет за собой и изменение алгоритма выработки и принятия управленческих решений;
- в США в 90-х гг. XX века информационное общество практически было построено, но существенных результатов это не дало, а привело к краху высокотехнологичных биржевых индексов. То есть сама по себе информационная индустрия ничего не дает, но ее можно использовать для разработки наукоемких технологий, которые дают реальную продукцию, концептуально повышающую качество жизни человека. К таким наукоемким технологиям можно отнести: биотехнологии, нанотехнологии и энергетические технологии. Все они не могут существовать без информационных технологий, но способны выдавать вполне конкретный продукт.

Трансформации современного общества, вызванные глубоким проникновением в повседневную жизнь информационных технологий, во многом есть объективный процесс, не зависящий от проводимой государствами политики. Происходящие процессы трансформации столь фундаментальны, что несут серьезную угрозу всем, кто не учел и не адаптировался к новым условиям.

В последнее время рядом зарубежных аналитических центров проводятся исследования по изучению динамики развития инновационных отраслей мировой экономики с целью прогнозирования и выявления тех направлений развития, которые в ближайшем будущем способны привести к взрывному росту мировой экономики, что будет способствовать ее выходу из затяжного кризиса.

В этой связи уместно отметить, что рядом экспертов, занимавшихся подготовкой аналитических материалов к Всемирному экономическому форуму в 2004 г. [79], отмечалось, что последние годы характеризуются глубокими застойными явлениями в области инноваций. Большие надежды связывались с развитием и повсеместным внедрением информационных технологий, однако крах высокотехнологичного сектора экономики в США в конце 90-х гг. во многом опроверг эти ожидания. Область информационных технологий продолжит свое развитие. Основные направления развития будут сосредоточены в узкоспециализированных областях: повышение защищенности и безопасности информационных систем, борьба с несанкционированными почтовыми рассылками (спамом), развитие средств и методов хранения информации и др. Однако качественно новых достижений, эквивалентных появлению глобальной сети Интернет или персональных компьютеров (за исключением прорывных разработок в области квантовых вычислений и систем связи), в этой области уже не ожидается.

1.3.2. Глобальные мировые тренды, обусловленные информатизацией общества

Среди особенностей, характерных большинству регионов мира, стремящихся использовать достижения информационной революции, отмечаются следующие глобальные тренды [2].

1. *Разработка новых технологий будет непрерывно стимулировать информационную революцию* [2].

Среди наиболее значимых событий в области информационных технологий, которые в ближайшие десятилетия в наибольшей

степени окажут влияние на развитие ситуации в развитых странах мира, выделяются следующие [2]:

- глубокая интеграция данных, голоса и видео, как в глобальных, так и в национальных сетях;
- универсальная возможность бесшовного взаимодействия мультимедийных и вычислительных устройств для создания информационных сетей и облачных технологий;
- конвергенция различных приложений на базе Интернет сети;
- повсеместное распространение широкополосных радиоканалов;
- внедрение новых оптических технологий, позволяющих повысить пропускную способность оптических линий связи до нескольких тысяч гигабит в секунду;
- существенное увеличение плотности хранения данных;
- увеличение интеграции и совместного использования кремниевых микросхем, био- и нанотехнологий.

Разработка товаров и услуг на основе подобных технологий позволит информационным устройствам обладать высокой вычислительной мощностью, быть высокоэффективными, находиться в непрерывном контакте друг с другом. Подобные устройства обеспечат взаимопроникновение физического мира и киберпространства, позволяя информационным системам всесторонне реагировать на изменения в окружающей их среде и наоборот.

При этом такое бурное развитие информационных технологий и различия в восприятии плодов информационной революции в различных регионах мира в ближайшие десятилетия могут привести к обострению межгосударственных отношений. Напряженные отношения, являющиеся результатом подобного развития событий, затронут рост и распространение продуктов и услуг, основанных на следующих информационных технологиях, например [2]:

- развитие технологии оптической связи, сетей связи нового поколения окажет негативное воздействие на отрасли фиксированной связи, что приведет к масштабным структурным перестройкам на рынке услуг связи;
- противостояние программного обеспечения с открытыми кодами (такого как Linux) против коммерческого программного обеспечения с закрытыми кодами (на базе операционной системы MS Windows) во многом будет способ-

ствовать коренному переделу рынка программного обеспечения;

- несоблюдение интеллектуальной собственности и цифровых прав на новые программные продукты и информационные услуги создаст основу для напряженности между государствами производителями и потребителями данных продуктов.

2. *В ближайшие годы информационная революция приведет к созданию новых бизнес-моделей, которые существенно трансформируют деловой и финансовый мир* [2].

Развитие информационных технологий способствует возникновению целого ряда новых бизнес-моделей как для внутреннего использования в корпорациях, так и для их внешних коммуникаций с клиентами, поставщиками и конкурентами. Основой таких моделей бизнеса являются различные формы электронной торговли. Процесс внедрения новых бизнес-моделей, основанных на электронной коммерции, будет сопровождаться экономическими проблемами у компаний, ведущих «традиционную» торговлю.

Сегодня большая часть деловой активности, основанной на новых информационных технологиях, сконцентрирована в Северной Америке, Европе и отдельных частях Азиатско-Тихоокеанского региона. Подобное деление, по всей видимости, сохранится и в ближайшие 15-20 лет. В результате развития в данных регионах новых бизнес-моделей эти страны и регионы станут ведущими не только в технологическом плане, но и основными экономическими лидерами новой цифровой эпохи.

3. *Информационная революция существенно перестроит механизмы управления обществом и создаст новую политическую реальность* [2].

Сейчас традиционные механизмы управления обществом становятся все менее эффективными и более проблематичными, поскольку информационная революция позволяет действовать игрокам политических движений вне досягаемости национальных правительств.

Важным элементом информационной революции является появление новых политических игроков. Новые политические игроки формируются информационной революцией в бизнесе, социальных и политических сферах, на внутринациональных, межнациональных и наднациональных уровнях, которые изменяют распределение политической власти. Развитие информационных технологий создает новые способы взаимодействия на основе интернет-технологий между граж-

данами и их избранными представителями, а также между гражданами при обсуждении политических проблем. Таким образом, протекающие процессы приведут к коренным изменениям в политической сфере государственного управления, что, в свою очередь, отразится и на вопросах определения национальных приоритетов, целей и ценностей. При этом необходимо отметить, что подобное влияние виртуальной реальности на реальную политику позволяет использовать в социально-политической сфере различные инструменты информационно-психологического воздействия для осуществления манипуляции общественным сознанием, формирования необходимых политически актуальных вопросов, координации проведения социальных протестов и т.д.

В течение последних лет рядом экспертов и аналитических центров интенсифицировали работы по изучению влияния информационной революции на процессы трансформации современного общества, его политической, социально-экономической и социально-психологической сферы. В настоящее время активно ведутся исследования в области информационно-психологического воздействия, в которых обосновываются методы формирования агентов влияния и управления социумом через социальные сети, СМИ, а также другие каналы информационных коммуникаций [72, 73, 74, 75, 76, 77, 78].

4. *Информационная революция будет формироваться социальными и культурными ценностями* [2].

Информационная революция инициирована технологиями, но направляется нетехническими факторами, прежде всего как социальными, так и культурными. Социальные и культурные изменения ускорятся, если отдельные граждане, корпорации и институты государства станут полнее использовать возможности информационных технологий в политической сфере. В ходе подобных процессов возможно обострение международных отношений, связанное с культурными и социальными различиями отдельных национальностей и государств. Прежде всего, такие конфликты активизируются между «цивилизованным» миром и бедными странами.

Доступ к новым информационным технологиям внутри и между странами сохранится. В пределах стран, распространение информационных технологий усилит различия и укрепит социальное неравенство, по крайней мере, пока не будет достигнуто технологическое насыщение. Кроме того, поляризация между богатыми и бедными станет более острой в силу ее отчетливой видимости в информационном обществе.

Подобные процессы повлекут проявление различных вызовов в различных частях мира. Глобализация, ускоренная информационной революцией, продолжит формировать сложные интегральные социальные и культурные эффекты. Таким образом, в то время как экономические эффекты глобализации сегодня уже достаточно изучены, ее социальные и политические последствия до конца не ясны. В связи с этим прогнозируется углубление разрыва между политическими, интеллектуальными, экономическими элитами и остальной частью населения, прежде всего в развивающихся странах.

5. *В ближайшие время сохранится многофакторная форма и характеристика национального подхода к восприятию информационной революции* [2].

Таким образом, на основе футуристических прогнозов, обобщенных в работах [2, 79], можно сделать выводы о глобальных изменениях в мире вследствие информатизации общества.

В политической сфере:

- перенос общественно-политической деятельности в глобальную сеть. Появятся новые сетевые политические образования и даже партии. Возможно появление транснациональных политических объединений на основе сети, которые будут оказывать влияние на деятельность сразу нескольких государственных структур. Основной политической силой станут не иерархические партии, а негосударственные сетевые общественные объединения;
- углубление межличностных отношений через социальные сети, рост и развитие горизонтальных связей в еще большей степени повысят потенциал общественного мнения как критерия эффективности деятельности государственных служб;
- продолжится рост и развитие электронных СМИ. Политические кампании будут приобретать все большую виртуальность, побеждать на выборах станет не личность, а виртуальный образ политика, сформированный в СМИ;
- оппозиционная деятельность правительству также сосредоточится на использовании Интернета. Одной из важнейших транснациональных оппозиционных сил будет движение антиглобализма и террористическо-хакерские объединения.

В финансово-экономической сфере:

- продолжится стремительная трансформация экономики под влиянием новых маркетинговых концепций «сетевой торговли»;
- ключевую роль займут электронные средства платежей как на уровне юридических, так и физических лиц;
- на отдельные государства будет усиливаться давление со стороны международных финансово-экономических структур и транснациональных корпораций, а также межгосударственных объединений типа ВТО.

В промышленной сфере:

- сохранится ориентация на вытеснение человека из сферы промышленного производства и замена его робототехническими комплексами;
- развитие высокотехнологичной промышленности, биотехнологий, генетических технологий, нанотехнологий и др.;
- развитие информационной инфраструктуры в мире за счет ускорения проникновения телекоммуникационных технологий, построения доступной коммуникационной инфраструктуры для доступа в глобальную сеть.

В сфере безопасности:

- продолжится сращивание национальной и зарубежной преступности в транснациональные преступные синдикаты;
- в сферу интересов преступности попадет новая цифровая экономика. Увеличится число противоправных действий с использованием информационных технологий и против объектов информационной инфраструктуры;
- экстремистские действия приобретут характер кибертеррористических. Произойдет слияние преступных хакерских сообществ с террористическими организациями. Возможно появление высокозаконспирированного преступного сетевого сообщества, ориентированного на экстремистскую деятельность в глобальной сети.

Эти же возможности информационного общества приобретаются и субъектами вооруженных сил. Однако новые возможности приобретают не только вооруженные силы государств. К сожалению, они становятся доступными и для террористических и экстремистских групп. В результате они обретают способность противостоять военной мощи наиболее развитых государств или напрямую угрожать их национальным интересам и национальной безопасности. Стремительное

развитие информационного общества значительно увеличивает влияние информационной сферы на национальную безопасность страны.

Информатизация общества требует от государственных органов решения большого количества задач, обусловленных внедрением новых информационных технологий [79].

В государственно-политической сфере:

- совершенствование системы государственного управления. Выработка методов и алгоритмов принятия решений на государственном уровне на основе сетевой структуры. Формирование системы независимых аналитических организаций, центров, фондов и др., результаты деятельности, которые должны использоваться при выработке решений на государственном уровне;
- трансформация существующего государственного аппарата, построенного по иерархическому принципу, в сетевой с использованием опыта работы транснациональных корпораций;
- трансформация существующей политической и партийной системы с учетом приоритета негосударственных общественных объединений и влияния общественного мнения на реализацию управляющих воздействий в обществе со стороны государства.

В финансово-экономической сфере:

- усовершенствование эффективности деловых сделок;
- преобразование существующих иерархических систем в сетевые;
- развитие рыночной on-line торговли;
- горизонтальное реструктурирование организаций;
- развитие малого и среднего бизнеса.

В промышленной сфере:

- обновление структур высокой стоимости (инфраструктурных компонентов);
- преобразование существующих систем в сетевые;
- горизонтальное реструктурирование промышленного производства;
- участие в выработке основополагающих стандартов в области информационных технологий.

В сфере безопасности:

- глубокая трансформация всего научного направления, связанного с обеспечением национальной безопасности, с уче-

том изменений в обществе. Прежде всего это касается существующей и перспективной модели угроз безопасности. Понимание невозможности создания абсолютной системы безопасности и концентрация на управлении рисками;
- трансформация силовых структур, внедрение сетевого принципа их организации;
- обеспечение безопасности информационной инфраструктуры.

Все вышеизложенное позволяет сделать вывод о том, что происходящие сегодня изменения в обществе весьма серьезны, они несут в себе мощный трансформационный потенциал, способный существенно преобразить облик нового мира, при этом изменения коснутся всех без исключения сфер жизни и деятельности человека.

В условиях глобализации необходима скорейшая и кардинальная реформа системы обеспечения безопасности государств. Новая система должна быть способной адекватно отвечать на угрозы нового времени. Более того, сегодня в основу обеспечения безопасности государства должна быть положена его информационная политика, определяющая национальные интересы и приоритеты в информационной сфере. Государственная внешняя и внутренняя политика должна строиться, базируясь на информационной политике. Достижение и удержание информационного превосходства, позволяющего доминировать в ситуации, должно стать основой международной деятельности всех государственных структур [47].

1.3.3. Основные тенденции развития геополитики в мире, обусловленные развитием информационных технологий

Учитывая вышеизложенное, можно спрогнозировать следующие основные тенденции развития геополитической обстановки в мире, обусловленные развитием информационных технологий [2].

1. *В ближайшее время США останутся в авангарде информационной революции* [2]. По мнению экспертов, североамериканская (США и Канада) экономика и общество достаточно хорошо подготовлены, чтобы встретить вызовы информационной революции. Они имеют ряд преимуществ, таких как хорошо развитая инфраструктура, человеческий капитал, экономика и само общество, которые легко адаптируются к различным изменениям, а также правовое поле с хорошей защитой интеллектуальных прав собственности. Северная Аме-

рика использует эти преимущества, чтобы держаться в авангарде информационной революции.

2. *Информационная революция в Европе будет развиваться медленнее и несколько иным путем, отличным от ее развития в США и Канаде* [2]. В то время, как факторы развития информационной революции остаются теми же, что и в США, существует и ряд принципиальных отличий [2]:

- европейцы и американцы по-разному относятся к возможным экономическим и социальным изменениям, последние проще адаптируются;
- европейцам свойственна большая экономическая и социальная активность;
- европейцам присуще желание интеграции наций в единой Европе;
- более открытый рынок США и более регламентированный правительством рынок Европы;
- больший европейский акцент на нисходящем планировании правительственными и деловыми элитами.

3. *Страны Азиатско-Тихоокеанского региона продолжат стремительное развитие и наращивание сфер использования информационных технологий, что в перспективе приведет к их масштабному технологическому и экономическому рывку* [2]. В последние годы наблюдается активное развитие государств Азиатско-Тихоокеанского региона, их стремительное вовлечение в глобализирующийся мир. Граждане Южной Кореи, Китая, Японии и Австралии составляют основную часть пользователей Интернета. В отличие от ситуации в США, где основную часть пользователей составляют частные лица, большинство пользователей Интернета в Азии – это сотрудники высокотехнологичных компаний. Япония, Сингапур, Китай, Южная Корея, Малайзия, Таиланд и Филиппины в настоящее время производят до 70-80% высокотехнологичных продуктов на мировом рынке. В ближайшие десятилетия эта тенденция не только сохранится, но и будет нарастать. Уже сейчас Китай также начинает существенно повышать собственный потенциал высококлассных специалистов в области высоких технологий за счет возвращения на родину китайцев, работавших в западных компаниях, а также после получения технического обучения за границей. В результате Китай обеспечит создание мощной высокотехнологической промышленности, что позволит ему стать главным игроком на рынке высоких технологий не только в Азии, но и в мире. В то же время многие государства, прежде всего европейские,

которые сегодня являются высокоразвитыми в технологическом и информационном плане, но обременены инерцией, созданной унаследованной инфраструктурой, будут терять свои позиции.

Кроме Китая, еще одним важным игроком в информационной сфере является Индия, которая имеет следующие преимущества в глобальном высокотехнологичном соревновании [2]:

- большое количество высокообразованных специалистов и дешевых рабочих, говорящих по-английски, в области информационных технологий;
- тесные связи многих индийских предпринимателей с американскими высокотехнологическими компаниями.

В результате Индия является одним из мировых лидеров в производстве программного обеспечения, и по прогнозам ожидается дальнейший рост индийского рынка программного обеспечения и сферы услуг в области информационных технологий.

Вместе с тем развитие индийского рынка программных средств может столкнуться с рядом трудностей, связанных, прежде всего, с ускоренным развитием в этой области Китая. Кроме того, индийская высокотехническая промышленность составляет небольшую часть от общей индийской экономики. Большая часть экономики Индии соответствует аграрной эпохе развития, не достигнув даже уровня индустриальной эпохи, уже не говоря об эпохе информационной. Эти факторы могут серьезно осложнить как будущий потенциальный рост высокотехнологических отраслей, так и внутреннюю ситуацию в стране.

4. *В ближайшее время геополитические тенденции, порождаемые информационной революцией, могут спровоцировать появление новых точек напряженности и конфликты в мировой внешнеполитической сфере* [2]. Стремительное развитие информационных технологий в ведущих экономически развитых государствах приведет к появлению большого количества проигравших и отстающих в развитии государств в различных частях планеты. Многие из этих проигравших или отстающих будут представлять серьезную угрозу безопасности для развитых государств. Информационная революция позволяет разочаровавшимся нациям и отдельным политическим силам с более высокой эффективностью объединиться и организоваться. Это приведет к новым тенденциям в мире [2]:

- проигравшие в информационной революции могут стать «государствами-неудачниками». Такие государства могут стать пристанищем для террористов, которые будут угро-

жать жизненным интересам ведущих технологически развитых стран, прежде всего – США;

- стремление не отстать от США внесет напряжение в европейские экономики, общества и государства, создавая отстающих и проигравших в пределах Европы. Это, в свою очередь, может через какое-то время создать растущее напряжение и в НАТО;
- неспособность Японии достаточно измениться, чтобы справиться с информационной революцией – если это случится, то может повлечь к снижению и без того незначительных темпов роста японской экономики. Стагнация экономики Японии, в свою очередь, приведет к экономической и технологической экспансии Китая. Это серьезно укрепит позицию Китая в Азии и сделает Китай равным США конкурентом.

5. *Непредвиденные обстоятельства, которые могут изменить глобальный курс информационной революции* [2]. Многие факторы могут замедлить или ускорить темп преобразований. Неблагоприятное развитие в финансовой сфере может замедлить их, а прорывные разработки в технологической сфере – ускорить. Будущие геополитические события, подобные новой «холодной войне», глобальные военные конфликты или крупномасштабный региональный конфликт неблагоприятно отразятся на развитии различных наций, регионов и мира в целом. Постоянные, широко распространенные, разрушительные террористические акты могут иметь аналогичный эффект в отдельном регионе или мире в целом.

2. Современные взгляды на ведение войны и управление войсками в условиях информационно-технической революции

2.1. Основные факторы, определяющие трансформацию форм и способов военных действий

Оценка военно-политической и военно-стратегической обстановки в различных регионах мира показывает, что начавшаяся более двадцати лет назад трансформация форм и способов ведения боевых действий в последние годы приобретает все более актуальный характер [3].

Движущими факторами трансформации является множество явлений, лежащих в различных сферах жизнедеятельности современного общества. Наиболее значимые из них приведены на рис. 2.1.

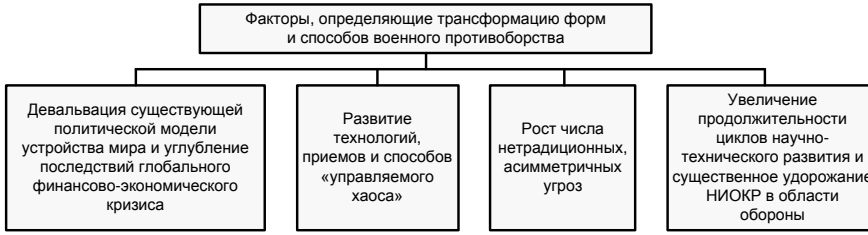


Рис. 2.1. Факторы, определяющие трансформацию форм и способов военных действий [3]

Рассмотрим эти движущиеся факторы более подробно.

1. *Стремительная девальвация существующей политической модели устройства мира и углубление последствий глобального финансово-экономического кризиса.* Результатом является то, что все большее число стран в условиях неблагоприятного развития ситуации в экономике начинают испытывать возрастающее давление со стороны оборонных расходов, что вызывает их перераспределение в сторону менее затратных систем (например, стремительнее развиваются относительно более дешевые системы ПВО, нежели более дорогая авиация). Вторым следствием этого фактора является рост внутриполитической и социальной напряженности во многих странах и регионах

мира, что изменяет баланс в сторону увеличения опасности внутренних угроз и угроз, связанных с резким ростом социальной дифференциации населения планеты (известная «теория Бреши» американца Т. Барнета приобретает все более четкие очертания). На этом фоне радикализируются многие религиозные, анархистские и иные социальные течения, зарождаются новые формы социального протеста [3].

2. *Стремительное развитие в последние годы технологий, приемов и способов «управляемого хаоса».* «Бархатные революции» конца XX – начала XXI века сегодня при соединении с современными телекоммуникационными и социальными технологиями приобретают крайне эффективные формы, позволяющие достигать политических целей «малой кровью», без применения масштабной военной силы. Это наглядно было продемонстрировано в целом ряде конфликтов последних лет, особенно ярко проявившихся в ходе так называемой «Арабской весны», когда революционные действия приобрели масштаб регионального конфликта в Северной Африке и на Ближнем Востоке. Понимание значимости стратегии «управляемого хаоса» повлекло за собой и определенные изменения стратегии: сегодня глобальные игроки все чаще стремятся достигать собственных целей не путем прямого столкновения, а через инициацию и поддержание конфликтных зон [3].

3. *Рост числа нетрадиционных, асимметричных угроз.* Сетевизация социальной структуры общества, появление в нем радикальных полупартизанских групп, стремящихся реализовать собственные идеологические установки, а также использование этих новых игроков в интересах основных геополитических центров силы ведет к тому, что традиционные силы обеспечения безопасности (как военные, так и специальные) все более утрачивают способность эффективно оперировать в новых условиях обстановки [3].

События в Ираке, Ливии, Сирии, Украине и иных странах показали, что зачастую армия, построенная на традиционных принципах, просто не успевает провести мероприятия по развертыванию и утрачивает боеспособность уже в первые часы после начала конфликта.

4. *Увеличение продолжительности циклов научно-технического развития и существенное удорожание НИОКР в области обороны.* Это приводит к тому, что новейшие образцы вооружения и военной техники разрабатываются в сроки, неприемлемые для темпов развития современного общества и меняющейся военно-политической обстановки (наглядный пример – судьба проекта американского истребителя F-35). Кроме того, конфликты последних лет

показали еще и то, что многие страны Европы за годы членства в НАТО утратили способность самостоятельно планировать и проводить операции с масштабным применением военной силы. В тех случаях, когда развитие военно-политической обстановки приводило к вовлечению в конфликт вооруженных сил одной или нескольких европейских государств вне блока НАТО, их применение оказывалось недостаточно эффективным.

Указанные (а также и другие) факторы ведут к углубляющейся перестройке форм и способов военного противоборства. При этом все чаще для достижения политических или экономических целей используется скрытое (латентное) противоборство, а также интенсифицируется применение невоенных форм борьбы [3, 121, 127, 130].

Ключевым способом такой невоенной формой борьбы является информационное противоборство. С одной стороны – инструменты и методы ведения информационного противоборства позволяют получить высокоэффективное и малобюджетное средство если не победы, то воздействия, а с другой – позволяют сформировать требуемую «информационно-виртуальную реальность», что обеспечит управление общественным мнением в подтверждение необходимости, законности и эффективности применения силы. Мощное информационно-психологическое воздействие на личный состав вооруженных сил и население страны существенно ослабит системы государственного и военного управления и сделает задачу обеспечения устойчивости управления одной из главных. Развитие средств ведения информационного противоборства в технической сфере приведет к существенному затруднению в использовании широко распространенных технических средств управления и связи. При этом использование аппаратного и программного обеспечения, разработанного иностранными компаниями, станет фактически невозможным. Таким образом, для успешного противостояния целенаправленным деструктивным информационным воздействиям на систему государственного и военного управления необходима разработка и реализация принципиально новых алгоритмов принятия решений и защищенных технических средств управления отечественного производства [3].

В сфере прямого военного столкновения доминирующее значение приобретут воздушно-космические средства вооружения, а также высокоточное оружие, что приведет к тому, что борьба за господство в воздухе и космосе во многом определит развитие операций на суши и море. Ключевыми в этом случае станут системы космической

связи, навигации, метеорологии, оптической и радиоэлектронной разведки [3, 121, 127, 130].

Вместе с тем исторический опыт 73-дневной войны в Югославии показал, что вооруженные силы, технически оснащенные по образцу семидесятых-девяностых годов прошлого века, могут успешно сохранять боеспособность даже в условиях практически полного превосходства противника в воздухе, однако для этого необходимы принципиально иные подходы к обеспечению мобильности войск, а также принципиально иные требования по маскировке. Все это, в свою очередь, влечет за собой и изменение технических средств, технологий и регламентов всех видов связи во всех звеньях военного и государственного управления – доминировать должны системы пассивной радиолокации, разведки и связи. Кроме того, требование высокой мобильности войск одновременно с отсутствием доступа к спутниковым средствам связи и навигации потребуют внесения существенных изменений в организацию связи, например возобновление широкого использования тропосферной связи и повсеместного внедрения инерциальных навигационных систем [3, 121, 127, 130].

Необходимость обеспечения боевой устойчивости войск потребует реализации на оперативном и тактическом уровнях принципа «роя» или «стаи», когда сравнительно малые по численности подразделения и части вооруженных сил смогут оперативно накапливаться в заданных районах для выполнения необходимой задачи. А по завершению задачи – также быстро рассредоточиваться и передислоцироваться в другие районы [3].

На эффективность боевого применения и боевую устойчивость войск окажут влияние средства и системы, согласующие применение различных видов и родов войск, а также концепции, устанавливающие единые требования по формированию единого взгляда на театр войны, в котором единообразно представлены цели в физическом и информационном пространствах [3, 121].

Стремительное увеличение удельного веса высокоточного оружия в общем объеме средств поражения, а также стремление противника в первую очередь поражать пункты управления повлечет за собой утрату связности и, возможно, полную децентрализацию системы государственного и военного управления уже на начальном этапе конфликта. Данное обстоятельство требует разработки систем и средств принятия решений в условиях низкой связности системы управления. Отдельные сегменты системы управления должны быть

способны решать ключевые задачи в условиях кратковременного или длительного отсутствия связи с вышестоящими звеньями управления.

Ядерный потенциал, имеющий ключевое значение для России, в случае конфликта станет целью «номер один» для высокоточного оружия и сил специальных операций противника. Учитывая тот факт, что уровень развития средств вооруженной борьбы, поддержанных полным господством противника в воздухе и космосе, может привести к тому, что Россия окажется неспособной применить свои ядерные силы, необходимо сделать ставку не только на ядерные силы, но и на неядерные компоненты, которые с большей вероятностью удастся сохранить [3].

Таким образом, в гипотетических условиях будущих военных действий, о которых говорилось выше, перспективная система управления войсками должна учитывать следующие тенденции в своем развитии [3]:

- необходимо планировать отказ от опоры на космический сегмент или существенное снижение его роли;
- стремление к всестороннему совершенствованию пассивных средств разведки, локации и связи;
- при проектировании отдавать приоритет боевой устойчивости, способности к самовосстановлению и реконфигурированию;
- развивать способность принимать решения по управлению войсками в условиях неполной или нечеткой информации;
- опираться на новые модели угроз информационной безопасности, предполагающие доступ противника к наиболее защищенным сегментам;
- реализовывать технические решения с опорой на «свободное» программное обеспечение с доступными исходными кодами;
- добиваться универсальности технических решений, модульности конструкции, позволяющих масштабировать возможности системы управления, делать ее универсальной и мобильной;
- добиваться устойчивости работы системы управления в широком диапазоне природно-климатических условий, в том числе и в полярных широтах.

2.2. Революция в военном деле как следствие развития информационных технологий в конце XX века

Коренное изменение взглядов на современное ведение военных действий, по сути, явилось следствием следующих основных факторов, таких как:

- информационно-техническая революция в военном деле;
- изменение модели угроз военной безопасности государства.

Впервые термин «революция в военном деле» был введен историком М. Робертсом в 1955 г., чтобы передать важность изменений в методах ведения военных действий, произошедших в XVI-XVII веках. Само это понятие отражает эпохальные перемены в военной организации, стратегии и технике [16].

В СССР автором советской версии концепции «революция в военном деле» считается начальник Генерального штаба ВС СССР маршал Н.И. Огарков [1], который в начале 80-х гг. указывал, что военно-техническая революция приведет в ближайшем будущем к тому, что поражающая способность обычных (неядерных) вооружений приблизится к возможностям ядерных боеприпасов малого калибра. Причем это сближение в характеристиках обусловливалось, главным образом, качественно новыми возможностями использования вычислительных средств в системах вооружений, разведки, подготовки, ведения и управления военными действиями [16].

Как показано в работах [16, 113], с момента окончания Второй мировой войны «революция в военном деле» последовательно прошла три следующих этапа.

1. *Революция в военной технике,* которая изменила облик оружия, боевых платформ и военной амуниции. Этот этап начался еще во время Второй мировой войны и фактически закончился в 80-х гг. прошлого века.

2. *Революция в военных системах обнаружения,* связанная с появлением электронных систем обнаружения и внедрением информационных систем управления оружием. С середины 70-х гг. по настоящее время существенно повысились возможности отдельных боевых комплексов (например, самолетов, кораблей, танков и т.п.) за счет более быстрой и эффективной обработки боевой информации и разработки систем удаленного управления оружием.

3. *Революция в военной связи,* начавшаяся в конце 70-х гг. минувшего столетия и продолжающаяся по сей день. Она позволила качественно улучшить системы управления и связи, что, в свою очередь, дает возможность формировать разнородные подразделения в единые группировки и координировать их действия при проведении совместных воздушных, морских и наземных операций.

Завершение каждого этапа связано с достижением пределов роста, когда дальнейшее улучшение характеристик вооружений в определенном направлении принципиально возможно, но нецелесообразно по критерию стоимость-эффективность. Опыт показывает, что качественно новые характеристики вооружений появлялись лишь в исключительных случаях и, как правило, за счет развития уже известных технологий.

Основным путем повышения боевой эффективности систем вооружений на сегодняшний день становится оснащение их современными информационными системами, обеспечивающими сбор и анализ поступающей информации, наведение оружия на цель, боевое управление и связь между участвующими в военных действиях подразделениями.

По сути в настоящее время происходит новая информационно-техническая революция, связанная с созданием принципиально новой военной техники и вооружений, объединяющая два направления [16]:

- совершенствование информационного насыщения отдельных боевых платформ, что является развитием революции военных систем обнаружения;
- координация действий различных боевых систем в рамках единого информационного пространства, а также создание концепции информационной войны как следствие развития революции систем связи.

Специфика современной информационно-технической революции в военном деле состоит в том, что она опирается на значительный технологический прорыв именно в области информационных технологий. Если ранее основные усилия концентрировались на улучшении ударных и боевых компонентов вооруженных сил, то сейчас передовые улучшения затрагивают, в первую очередь, системы управления и разведки. Техническая сторона современной революции в военном деле основана, в первую очередь, на достижениях в области информатики и электроники, на улучшении характеристик точности и дальности действия оружия, полноте и оперативности разведки и наблюде-

ния, повышении способности противодействовать и подавлять вражескую оборону и эффективно управлять войсками.

Несмотря на первоначальную сосредоточенность на технических аспектах начавшейся информационно-технической революции в военном деле, данный процесс привел к фундаментальному пересмотру всего военного строительства. Открывающиеся возможности по совершенствованию технических характеристик систем управления позволяют провести модернизацию не только отдельных образцов вооружения, но и принципов управления, применения и организации самих вооруженных сил.

На современном этапе существенно изменилось соотношение политико-дипломатических, экономических, информационных, психологических и военных средств борьбы на международной арене. Значение и удельный вес невоенных средств значительно возросли. В условиях глобализации последние приобрели более целеустремленный и скоординированный характер, повысились их технологическая оснащенность, масштабы и результативность. В последние десятилетия в ходе противоборства на международной арене без непосредственного применения вооруженной силы стали рушиться целые государства и коалиции государств. Главной причиной этого стали кризисные явления в тех или иных странах и их внутренняя неустойчивость, усугубленная воздействием внешних факторов [1].

В американской армии информационно-техническая революция в военном деле получила развитие в виде концепции «системы систем», предложенной заместителем председателя комитета начальников штабов (КНШ) МО США адмиралом У. Оуэнсом. По его мнению, решающее значение для успеха будущих военных операций приобретает создание единой системы сбора, обработки и распределения данных, получаемых от различной контрольно-измерительной аппаратуры и множества датчиков, размещаемых в космосе, в воздухе, на суше, на воде и под водой [16].

Развитие концепции информационно-технической революции в военном деле в перспективе приведет к повсеместной автоматизации процесса ведения военного противоборства, «изъятию» людей из «боевых платформ» (танков, самолетов, кораблей и пр.) и их замена так называемыми «информационными солдатами». При этом сами боевые платформы станут полностью автоматическими. Кроме того, реализация последних достижений военного прогресса позволит создать высокоточные системы вооружения, которые будут более эффективными против выбранной цели, но менее разрушительными для ее окружения

(например, для мирного населения). Это позволит снять ограничения на применение вооруженных сил в конфликтах, которые в иных условиях могли бы повлечь неоправданные по политическим и другим причинам жертвы среди мирного населения [16].

Таблица 2.1. Характерные различия в ведении боевых действий [239]

Составные элементы	**Концепции, построенные на революции в военном деле**	**Традиционная концепция «больших батальонов» (решающее значение силы)**
Задача	Поставить под контроль волю противника, восприятие и оценку им происходящего	Получить решающее военное превосходство над силами и средствами противника
Назначение военной силы	С помощью контроля над волей противника и его способностью к ориентации лишить его всякой возможности действовать или отвечать на удары	Победа над противником путем достижения превосходства над его военным потенциалом
Масштаб военной силы	Можно уступать противнику численно, главное – иметь решающее преимущество в техническом оснащении, боевой подготовке и методах ведения боевых действий	Крупные, хорошо обученные и оснащенные силы, обладающие подавляющим превосходством в технике и вооружениях
Сфера применения	Универсальная	Боевые действия группировки против группировки (а также вспомогательные операции)
Скорость	Имеет принципиальное значение	Желательна
Потери в живой силе	Могут быть незначительными с обеих сторон	Потенциально значительные с обеих сторон
Приемы ведения боевых действий	Парализовать волю противника, ошеломить его, деморализовать, сковать, уничтожить	Систематическое уничтожение живой силы и техники противника. В некоторых ситуациях может применяться тактика, изматывающая противника

Существующие и действующие модели ведения войны в новых информационных условиях требуют пересмотра. Так, после терактов в США президент Дж. Буш предложил министру обороны Д. Рамсфельду подготовить стратегическое видение модернизации американской армии для ее соответствия новым вызовам и геополитическим

тенденциям XXI века. В соответствии с новой стратегией национальной безопасности для того, чтобы отражать внезапные удары, вооруженные силы США должны перенести центр тяжести в системе оборонного планирования с модели, ключевым моментом которой является угрозы, и которая до сих пор доминировала в теории обороны, на модель, опирающуюся на силы и средства, необходимые в будущем. Вместо того чтобы концентрировать внимание на том, кто именно окажется очередным противником или где может произойти война, вооруженные силы США должны сосредоточиться на методах действий возможного противника и соответственно развивать новые возможности для его сдерживания и поражения. Вместо того чтобы планировать крупномасштабные войны на точно определенных театрах предполагаемых военных действий, считает Д. Рамсфельд, необходимо предвидеть появление новых и разнообразных противников, которые будут полагаться на фактор внезапности, обмана и на применение ассиметричного оружия для достижения своих целей [2].

В результате сформированная новая стратегия обороны США в XXI веке призвана реализовать четыре ключевые задачи [2].

1. Гарантировать союзникам незыблемость поставленных военно-политических целей и способность США выполнять обязательства в сфере безопасности.
2. Сформировать у потенциальных противников обоснованные сомнения в целесообразности проведения программ или мероприятий, которые могут создавать угрозу интересам США или их союзников.
3. Обеспечить сдерживание агрессии и силового давления за счет передового развертывания сил и средств, способных быстро остановить разрастание кризиса.
4. Предпринимать решительные действия по военной нейтрализации любого противника в том случае, если методы убеждения и сдерживания окажутся неэффективными.

Для достижения поставленных целей США должны сохранить существующее военное преимущество на ключевых направлениях и разработать новые способы лишения противников преимуществ, которые они пытаются получить, применяя асимметричные варианты действий, известные в виде принципиально новой оперативной концепции ведения противоборства, получившей наименование «сетецентрическое противоборство» или «сетецентрическая война» NCW (Network-Centric Warfare) [2].

2.3. Анализ развития способов и форм ведения военных действий

2.3.1. Войны доядерного периода

За последние 5,5 тыс. лет на Земле произошло около 15 000 вооруженных конфликтов и войн, в которых погибло примерно 3,5 млрд человек. Война, вооруженное насилие всегда были основным средством решения межгосударственных споров, элементарными формами принуждения.

Анализ истории войн и военных конфликтов показывает, что в доядерный период чередование войны и мира на Земле было естественным и даже в какой-то мере привычным состоянием. Войны никогда не прекращались, имели свое развитие: с древнейших времен и до наших дней уже сменилось, по крайней мере, четыре поколения войн и военных конфликтов. Основные рубежи смены таких поколений совпадают, главным образом, с качественными, имеющими историческое значение скачками в развитии человеческого общества, обусловившими появление принципиально новых средств поражения, что приводило к зарождению новых форм и способов ведения войны. Классификация поколений войн представлена в таб. 2.2 по данным работ [174, 269].

История свидетельствует, что первые четыре поколения войн выступали, в основном, как инструмент политики и были ее допустимым или приемлемым продолжением. Война пятого поколения – это уже ядерная война, которая может быть единственной и последней в случае ее развязывания.

Войны первого поколения в историческом плане уже выступали как способ разрешения противоречий, но не всегда носили ярко выраженный политический характер. Их зарождение следует отнести к племенной, родовой и семейно-патриархальной стадиям человеческого развития с присущим им обменом результатами труда внутри племени, рода и перерастанием товарных отношений в товарно-денежные. Вооруженная борьба в этих войнах осуществлялась на тактическом уровне исключительно живой силой – пешими воинами и конницей, оснащенными холодным оружием. Войны первого поколения велись в рабовладельческую эпоху (VI в. до н.э. – II в. н.э.) [173].

Таблица 2.2 Классификация поколений войн [174, 269]

Вооружение	**Масштаб боевых (военных) действий**	**Цель войны**
Первое поколение		
Холодное оружие	Тактический	Уничтожение противника, овладение его ценностями и территорией
Второе поколение		
Порох, гладкоствольное оружие	Тактический, оперативно-тактический	Уничтожение противника, овладение территорией или установления контроля над ней
Третье поколение		
Нарезное многозарядное оружие повышенной скорострельности, точности и дальности стрельбы	Оперативно-тактический, оперативный	Разгром группировок вооруженных сил противника, установление контроля над территорией и ее ресурсами
Четвертое поколение		
Автоматическое и реактивное оружие, танки, авиация, флот, транспортные средства и связь	Оперативно-стратегический	Разгром вооруженных сил противника, разрушение его экономического потенциала и политической системы
Пятое поколение		
ЯО и ограниченное или массированное его применение	Стратегический	Разгром вооруженных сил противника, разрушение его экономики и свержение политического строя
Шестое поколение		
ВТО наземно-воздушно-морского базирования, развитое информационно-космическое обеспечение	Стратегический, оперативно-стратегический и оперативный	Завоевание или установление контроля над мировыми ресурсами жизнедеятельности человечества, установление лояльности власти в государствах, на территории которых эти ресурсы находятся, управление массовым сознанием народов и больших групп людей

Формы и способы ведения войн второго поколения были обусловлены революцией в военном деле, связанной с развитием материального производства в феодальном обществе. Начальным рубежом этой революции можно считать появление пороха и гладкоствольного оружия. Появились новые способы вооруженной борьбы в масштабах тактики подразделений, частей и соединений. Боевой порядок войн второго поколения включал силы авангарда, кордебаталии и арьергарда, строй кильватера. Применялась линейная тактика, согласно которой в морском бою противоборствующие стороны выстраивались в линию друг перед другом в зависимости от ветра и вели артиллерийскую дуэль [173].

Капиталистическая стадия развития человеческого общества способствовала прогрессу в технологиях, появлению большого количества нарезного многозарядного стрелкового оружия и нарезной артиллерии, обладающих большой дальностью, скорострельностью и точностью. Это привело к очередной революции в военном деле, породило войны третьего поколения, которые проводились уже в оперативно-тактическом масштабе. Парусно-паровые деревянные корабли имели водоизмещение до 5-6 тыс. тонн, мощность машин до 5000 л/с, скорость до 14 узлов, с артиллерийским вооружением до 40 гладкоствольных орудий [173].

Первая мировая война (1914-1918 гг.) велась между коалициями государств Европы с широким применением различных видов оружия и техники, главным образом артиллерии и пулеметов, с целью уничтожения вооруженных сил противника и захвата территорий, установления господства более сильных государств. Наличие броненосного флота у технологически развитых государств было важным рычагом в их борьбе за мировое господство. В эту эпоху появился термин операция как форма решения задач на сухопутном театре войн.

В середине XX века произошла очередная революция в военном деле, которая вызвала появление войн четвертого поколения, которые не прекращаются и ныне, продолжая свое развитие. Войны приобрели стратегический масштаб. Они стали результатом развития капиталистического и посткапиталистического общества и возникновения двух антагонистических мировых систем, что привело ко второй мировой войне. Стратегический масштаб способствовал ускоренному созданию и принятию на вооружение в больших количествах автоматического оружия, бронетехники, боевой авиации, надводных и подводных кораблей, появлению средств радиолокации и связи [173].

Концепция войн этого поколения, основой которых являются действия большого количества сухопутных войск с бронетехникой, авиацией, флотом в их тесном взаимодействии, существует уже более 70 лет. В ходе войн и военных конфликтов ставка всегда делалась на большие людские ресурсы. Причем применяемое количество живой силы, вооружений, военной техники и боеприпасов даже в самом малом военном конфликте всегда было довольно большим, а интенсивность вооруженной борьбы и морские потери всегда были достаточно высокими.

Войны четвертого поколения характеризуются широким использованием всех видов вооруженных сил и родов войск в форме операции. Военное искусство получило дальнейшее развитие в ходе вооруженной борьбы в области стратегии и тактики. Новые принципы военного искусства, такие как комплексное огневое поражение, скрытность, внезапность, использование средств радиоэлектронного подавления и маскировки, способствовали достижению победы. В целом, во второй мировой войне и в победе союзников над Германией главную роль сыграли экономическая мощь США и СССР и их военный потенциал, который обеспечил превосходство в количестве и качестве вооружений над гитлеровской коалицией. Появились новые понятия в военной теории: военная мощь, военный потенциал и моральный фактор, которые обеспечили победу союзников во второй мировой войне [173].

2.3.2. Войны ядерного периода

Холодная война (1946-1991 гг.) по факторам сдерживания относится к ядерному периоду, так как в ее основе лежало применение ракетно-ядерного оружия. Основными формами и способами ведения холодной войны было жестокое противостояние войск и сил флота на Европейском, Азиатском и Африканском континентах и в Мировом океане [173].

Анализируя опыт войн, военных и вооруженных конфликтов, имевших место после 1945 г., можно обнаружить смену закономерности в развитии вооружений, которая была вызвана холодной войной. Борьба двух мировых систем заменила эволюционный процесс развития вооружений на скачкообразное их обновление. Началась гонка вооружений. Одновременно происходило постоянное сокращение сроков жизненного цикла каждого очередного поколения и вооружений, и военной техники. Возникло естественное противоречие между сокра-

щением сроков жизни и увеличением сроков создания новых образцов вооружений и военной техники [173].

В ходе гонки вооружений в короткие сроки сменилось несколько поколений ракет различного назначения, классов кораблей и типов самолетов, появились автоматизированные системы связи и управления, возросла роль информационного превосходства. Разработка перспективных высокоточных систем оружия, которую вели технологически развитые страны, предполагала развитие не только качественного военно-технического и стратегического превосходства, но и появления новых форм и способов ведения войны. Создавались не просто принципиально новые виды оружия, а целые боевые системы, способные выполнить объем тех задач, которые ранее возлагались в основном на живую силу и ее оружие.

Например, в войне в Корее (1950-1953 гг.) было применено девять ранее неизвестных видов оружия. В войне во Вьетнаме (1964-1975 гг.) таких видов было уже 25. В войнах и конфликтах на Ближнем Востоке (1967, 1973, 1982, 1986 гг.) – около 30, а в войне в зоне Персидского залива (1991 г.) – свыше 100 видов оружия и боевых систем. После второй мировой войны сменились 4-5 поколений ракетного оружия, выросла его дальность и точность. Боевая мощь новейших видов вооружения и военной техники непрерывно увеличивалась, а необходимость ее постоянного обновления и развития приводила к росту стоимости содержания вооруженных сил и войны в целом.

Однако следует особо отметить, что появление более совершенных видов оружия в период холодной войны не вело к революции в военном деле, к изменению стратегии и оперативного искусства. Холодная война в развитии вооружений сделала очередной шаг к смене поколения войн. В холодной войне сочетались ядерное противостояние и наращивание войск и сил флота [173].

Научно-техническая революция 50-60 гг. XX века привела к созданию ракетно-ядерного оружия, ставшего в ходе холодной войны базой войн пятого поколения. С началом этапа ядерной холодной войны снизился интерес к обычному оружию. Наступил длительный период застоя в развитии обычных вооружений, а также в развитии высокоточного оружия высокой дальности, способных эффективно поражать цели обычными боеприпасами. Для ядерного оружия высокой точности не требовалась [173].

Необходимо подчеркнуть, что во всех войнах доядерного периода главным объектом поражения непременно были вооруженные силы противоборствующих сторон, только после их разгрома, как пра-

вило, можно было разрушить экономику противника и добиться политических целей. Ввиду того, что не хватало обычных средств массированного воздействия одновременно по всей территории противника, для достижения стратегических результатов в войне приходилось вести длительные наступательные операции оперативно-стратегического масштаба, главным образом, многочисленными сухопутными группировками, и, как правило, лишь в ходе оккупации территории противника, ценой огромных потерь живой силы достигалась победа в войне.

Ракетно-ядерное оружие резко изменила стратегию войны. Первоочередными объектами поражения в такой войне выступают не только вооруженные силы, но и практически вся территория и все население воюющих сторон одновременно. То есть ареной военных действий в ракетно-ядерной войне становится вся планета, ее океанские и морские акватории, а также воздушно-космическое пространство. Ядерная война является аномальной в эволюционном процессе смены поколений войн, она не может привести к достижению стратегических и тем более политических целей. Таким образом, холодная война 1946-1991 гг. проходила при ядерном сдерживании, в условиях угрозы развязывания ракетно-ядерной войны – войны пятого поколения. Именно длительное ядерное противостояние и породило в ходе холодной войны, которая велась более 40 лет двумя противоположными мировыми системами, новый тип войны – войну шестого поколения [173].

Для всех поколений войн было характерно сочетание нового оружия и новых методов ведения вооруженной борьбы. И всякий раз вооруженные силы наиболее развитых стран, принявших на вооружение новые виды оружия, должны были готовиться к новым войнам, а остальные, не имеющие такого оружия, вынуждены были приспосабливаться к меняющимся формам и способам вооруженной борьбы и войны в целом.

Анализируя опыт войн, военных и вооруженных конфликтов, имевших место только за последние полвека, можно обнаружить смену закономерности в развитии вооружений: плавный, постепенный эволюционный процесс разработки и модернизации известных видов вооружений начал уступать место скачкообразному их обновлению [173].

2.3.3. Бесконтактные войны шестого поколения

После холодной войны мир вступил в полосу региональных вооруженных конфликтов и политической нестабильности, число крупномасштабных военных акций глобального, регионального и национального характера резко увеличилось. При этом США и другие ядерные державы оказались в тупиковой ситуации, накопив в больших количествах ядерное оружие. Например, доктрина США не допускает возможности удара даже одного ядерного боеприпаса по их территории со стороны любого ядерного государства. Они хотят быть полностью уверенными, что ядерного удара по их территории со стороны возможного противника никогда не последует. Создать абсолютно непроницаемую ПРО невозможно. Поэтому США вынуждены либо пойти на кардинальное ядерное разоружение с втягиванием в этот процесс других ядерных стран, либо согласиться на существующие двусторонние договоренности по ядерным вооружениям. Тем не менее, их стратегические ядерные силы ориентированы и на Россию, и на Китай, независимо от складывающихся с ними отношений. Аналогично и ядерные силы этих стран ориентированы на США. Следует ожидать, что вплоть до создания эффективной системы военной безопасности всех стран, с учетом их геополитического и, особенно, экономического положения, такие ядерные страны, как Россия и Китай, будут вынуждены продолжать делать ставку на свое ядерное оружие. При этом такие страны, не прекратят сопротивляться его сокращению и ликвидации до тех пор, пока не накопят достаточные запасы высокоточного оружия, а также пока не разовьют средства ведения бесконтактных войн шестого поколения [173].

Войны шестого поколения будут вестись, как правило, с применением обычного, главным образом высокоточного оружия, но при постоянной угрозе применения ядерного. При неблагоприятном соотношении сил на стратегических направлениях для стран-обладателей ядерного оружия именно оно останется важнейшим, наиболее надежным средством стратегического сдерживания агрессии и обеспечения оборонной безопасности. В связи с этим, нельзя согласиться с теми, кто считает, что ядерное оружие утратило свою сдерживающую роль и предлагает отказаться от учета эффектов его применения при моделировании войн 6-го поколения [1].

Как отмечается в работе [1], в обозримой перспективе становится маловероятной не только мировая война, но и уменьшается опасность крупномасштабного военного регионального конфликта.

Такая опасность уменьшается не только из-за снижения угрозы применения ядерного оружия, но и в связи с нахождением новых форм и способов достижения политических и стратегических целей за счет развязывания локальных войн, конфликтов, политического, экономического, информационного давления и подрывных действий внутри противостоящих стран [1].

Державы и военно-политические блоки, вооруженные силы которых обладают технологическим превосходством над любым вероятным противником, получат очевидное преимущество в выборе места, времени и масштаба боевых действий. Вместе с тем, вооруженная борьба не всегда будет вестись по законам и правилам, продиктованным стороной, наиболее подготовленной к реализации на практике передовых научно-технических достижений [203].

В условиях дальнейшего усиления экономической, экологической, демографической и гуманитарной взаимозависимости членов мирового сообщества ни одно государство не сможет позволить себе победу любой ценой. Для ведущих стран мира становятся неприемлемыми потери среди личного состава, не говоря уже об угрозе безопасности своего гражданского населения. Кроме того, начиная боевые действия, будущему победителю придется думать и о побежденных. Ведь жертвы среди мирных граждан могут повлечь серьезный международный резонанс, спровоцировать массовое движение сопротивления, а разрушение экономики чревато превращением побежденной страны в территорию постоянной нестабильности. Критическое значение приобретет и временной фактор, так как затягивание боевых действий ведет к потере инициативы, риску расширения конфликта, как по территории, так и по составу участников, повышению экономических, моральных и политических издержек [203].

В войнах шестого поколения решающая роль отводится уже не большому количеству сухопутных войск и ядерному оружию, а высокоточному обычному ударному и оборонительному оружию, а также оружию на новых физических принципах. В средствах вооруженной борьбы сегодня происходит неуклонное увеличение числа применяемых высокоточных средств поражения. Таким образом, приоритет отдается точечному, заранее выверенному воздействию на военные и гражданские объекты противника. Это достигается с помощью решения информационно-расчетных задач, позволяющих провести научно-обоснованную количественную оценку важности объектов вероятного противника, для решения задач определения объектов поражения.

В ближайшем будущем даже развитые в военно-экономическом отношении страны не будут располагать необходимым количеством высокоточного оружия для ведения крупномасштабной войны. Поэтому современная крупномасштабная война будет иметь как минимум два этапа. На первом этапе может быть реализована война нового поколения, а если военно-политические цели не будут достигнуты, наступит второй этап – вооруженная борьба предшествующих поколений с применением как обычных, так и ядерных средств поражения [163].

Существующие и разрабатываемые в ведущих странах мира высокоточные крылатые и другие ракеты наземного, воздушного и морского базирования могут быть эффективным оружием только в условиях информационного превосходства. Сейчас требуется с помощью средств информатики, разведки и связи быстро получать точную, своевременную и защищенную информацию, правильно реагировать на любой конфликт с целью немедленного овладения ситуацией и принятия необходимых решений. Для этого нужны совершенно иные, глобальные военные системы управления, разведки и связи. При этом исключительно важной и многоплановой стала роль космоса, космических сил и средств. Из космоса ведется непрерывная разведка, через космос обеспечивается управление, связь, метеообеспечение, навигация, радиоэлектронная борьба и др., а также корректируются высокоточные удары по целям на земле [163].

Весь процесс вооруженной борьбы в ближайшей перспективе вполне вероятно будет протекать скоротечно, по законам и правилам той стороны, которая в наибольшей степени подготовлена к реализации на практике самых передовых достижений в военной и технологических областях. Продолжительные войны прошлых поколений уступят место короткой молниеносной войне. Скорость, синхронность, одновременность, быстрота управления становятся решающими факторами, определяющими успех военных операций. Управление войсками и оружием будет осуществляться уже в реальном или близком к нему масштабе времени, а высокоточное оружие (ВТО) в десятки раз позволит повысить эффективность проводимых операций. Превосходство над противником в мобильности, точности поражения и информационном обеспечении позволят вести боевые действия в таком темпе и с такой интенсивностью, которую вероятный противник не в состоянии будет выдержать. Находясь в сложной, постоянно ухудшающейся обстановке, противник не сможет захватить инициативу, планировать действия своих войск и эффективно ими управлять. Бескон-

тактный характер военных действий предполагает уничтожение или выведение противника из строя на дальних подступах задолго до боевого соприкосновения. В идеальном варианте войска противника вообще не должны выйти из мест постоянной дислокации или, в крайнем случае, они должны быть уничтожены на маршрутах выдвижения. При этом даже в рамках региональной или локальной войны военные действия 6-го поколения будут вестись одновременно на всю глубину территории государства противника, на сотни и тысячи километров от линии границы [29, 43].

Наиболее полно характеристики бесконтактных войн отражены в работах В.И. Слипченко. К числу наиболее важных характеристик бесконтактных войн следует отнести такие, как [17, 29]:

- универсальная для ПРО и ведения бесконтактных войн единая глобальная разведывательно-информационная система космического базирования;
- локальный или региональный размах с основными военными действиями в воздушно-космическом пространстве;
- использование разведывательно-ударных боевых систем в формах воздушно-космическо-морских ударных операций для разрушения экономического потенциала государства-противника;
- единая система управления всеми боевыми системами, силами и средствами;
- единые унифицированные, построенные по модульному принципу высокоточные средства поражения различной дальности наземного, воздушного, морского, а в последующем и космического базирования;
- использование единой навигационной системы и различного рода систем самонаведения для нанесения ударов по любому объекту противника, независимо от погодных условий и времени суток, в любом регионе планеты бесконтактным способом;
- широкое использование информационно-технических воздействий для бескомпроматного и дистанционного поражения стратегически важных объектов противника (таких как объекты системы государственного и военного управления; промышленные объекты; управление транспортной и энергетической инфраструктурой; объекты телекоммуникационной, экономической и связной инфраструктуры);

- массированное проведение информационнопсихологических операций на всех этапах ведения войны;
- тенденция к прекращению использования активной радиолокации как в стратегических ударных, так и в стратегических оборонительных силах государств.

Несмотря на то, что войны шестого поколения являются бесконтактными, в угрожаемый период или с началом такой войны будет осуществляться стратегическое развертывание вооруженных сил (частичное или крупномасштабное) в зависимости от характера предстоящего военного столкновения. В некоторых работах приводятся утверждения о ненужности стратегического развертывания, однако практика современных вооруженных конфликтов их опровергает. Известно, что США перебросили и произвели полномасштабное развертывание коалиционных сил в 1991 г. перед войной с Ираком, причем с выполнением ряда мобилизационных мероприятий. Однако в будущем стратегическое развертывание, особенно перегруппировка, будут осуществляться по-новому.

Необходимость обеспечения высокого уровня жизни населения в постиндустриальных странах приведет к тому, что военно-политическое руководство США и стран Западной Европы только в самом крайнем случае сможет позволить себе переводить все государство на режим военного времени. В стратегическом развертывании армий развитых стран основной акцент будет делаться не столько на мобилизационные мероприятия, сколько на перегруппировку боеготовых войск (сил) с использованием их возросшей стратегической мобильности, способности поражать противника с больших дистанций, в том числе с передовых военных баз, из воздушно-космического пространства и из Мирового океана [203]. При этом для достижения внезапности действий стратегическое развертывание может осуществляться под прикрытием начавшихся воздушных операций [1].

Опыт последних военных конфликтов показывает, что для достижения своих политических целей ведущие страны действуют с опорой не только на национальные ресурсы, но и в большинстве случаев создают многонациональные коалиции, формирование которых является важным элементом стратегического развертывания. В связи с этим повысится актуальность расширения существующих и формирования еще ряда союзов, заключения соглашений в военно-политической и военно-технической сферах, создания новой системы гарантий международной стабильности [203].

У отстающих в военно-техническом отношении государств стратегическое развертывание будет сводиться в основном к мобилизации значительной части населения. Успех ее проведения будет зависеть, прежде всего, от морального духа граждан и их отношения к войне. Так, американские психологи и социологи отмечают, что военнослужащие, мобилизованные под угрозой привлечения к ответственности вопреки своему желанию, в ситуациях, связанных с риском для жизни, склонны выходить из-под контроля, дезертировать или сдаваться в плен. Не менее важен и материально-технический аспект: возможности экономики по подготовке, оснащению и содержанию дополнительно призванного личного состава. При нехватке ресурсов призванные из запаса резервисты могут предназначаться только для формирования частей территориальной обороны и иррегулярных отрядов, а в более сложных случаях мобилизационные мероприятия сведутся к раздаче оружия населению [203].

Изменится подход к формированию резерва, основу которого составят профессиональные военнослужащие, постоянно проходящие переподготовку. Это позволит избежать распыления регулярных войск (сил), затрат на подготовку специалистов по редким для армии профессиям, упростит процедуру поддержания необходимого уровня боеготовности резерва, в частности, оправдывает себя использование резервистов в подразделениях охраны, материально-технического и тылового обеспечения, на административной работе [203].

Существенно возрастет и изменится содержание начального периода противостояния. Он будет означать не только вступление в войну, но может стать ее решающим этапом. Особое значение приобретут борьба за господство в воздушно-космическом и информационном пространствах и противодействие высокоточным средствам противника большой дальности. На первом этапе ведения боевых операций особое внимание будет уделяться нанесению массированных ударов авиацией ВВС, ВМС и крылатыми ракетами по объектам систем управления вооруженными силами противника и его ПВО (в первую очередь по зенитным ракетным комплексам большой и средней дальности действия). Их уничтожение позволит авиации наносить наиболее эффективные удары управляемыми авиационными бомбами и ракетами «воздух – поверхность» со средних высот, находясь вне зон поражения основной группировки средств ПВО ближнего действия. В ходе начального периода войны должны быть уничтожены основные государственные и военные пункты управления, большинство объектов ОПК, нарушена система управления государством и ВС, выведены

и строя основные промышленные объекты, энергетика и сломана воля противника к сопротивлению [1, 19, 29].

Несмотря на то, что основные задачи по разгрому противника будут решаться не в ходе столкновения передовых частей, а путем удаленного огневого поражения, такое развитие способов ведения военных действий не приведет к полному отказу от ведения действий сухопутными войсками. Действительно, исторический опыт войн в Ираке и Югославии показывает, что технологическое превосходство в вооружении и наличие средств ВТО позволяют наносить удары по объектам противника, оставаясь вне зоны досягаемости средств ПВО и авиации. Имея современные образцы ВТО, войска США смогли почти полностью исключить прямой контакт с противником и оказывать влияние на складывающуюся тактическую обстановку, не соприкасаясь с ним.

Высокоточное оружие существенно меняет характер вооруженной борьбы, однако нет оснований утверждать, что с его появлением формы и способы ведения контактной войны теряют свой смысл [1, 29].

Война между технологически оснащенными противниками не может ограничиться только бесконтактными действиями. При ведении боевых действий в Афганистане (в районе Тора-Бора и Мазари-Шарифа) американским войскам пришлось заниматься и централизованным огневым поражением, и штурмом укрепленных позиций. Это вытекает из объективных условий, природы боевых действий. Нет никаких гарантий, что не придется решать подобные задачи и в будущем. Применительно к России роль Сухопутных войск еще более важна. Они призваны не допустить вторжения противника на нашу территорию, обеспечить устойчивость положения и действий других видов и родов войск Вооруженных Сил РФ, а также обезопасить коммуникации в глубине страны [1].

Ключевое значение приобретает и воздушно-космический ТВД, повышается роль обычного (высокоточного) стратегического оружия как решающего средства ведения войны, обеспечивающего непосредственное достижение стратегических результатов. Увеличивается пространственный размах вооруженной борьбы – оружие будущего и возросшие боевые возможности вооруженных сил позволят наносить мощные удары на всю глубину расположения воюющих государств, осуществляя не только последовательное, но и одновременное поражение его объектов. Следовательно, срыв воздушно-космического нападения приобретает для обороняющейся стороны

первоочередное значение. Таким образом, для обороняющейся страны решающее значение будет иметь совершенная система разведки с единым центром управления, сбора и обработки информации всех ее видов, высокоэффективная система ПВО и воздушно-космической обороны (ВКО) [1, 29].

Учитывая крайнюю невыгодность и опасность пассивных, чисто оборонительных действий, сражения с самого начала примут активный и решительный характер. Вслед за огневыми и радиоэлектронными ударами, наносимыми по всей глубине расположения противника, будут высаживаться воздушные десанты, развернут свои действия спецподразделения, начнется стремительное продвижение сухопутных сил. Войска будут действовать, придерживаясь тактики оперативных маневренных групп, осуществляя широкие рейдовые действия, избегая фронтальных атак, стремясь выйти во фланги и в тыл противника. Таким образом, намечается тенденция сближения способов ведения наступательных и оборонительных операций [1].

С учетом новых условий и факторов стратегия действий участников конфликтов будет определяться соотношением их возможностей и потенциалов. При этом более слабая сторона встанет на путь асимметричного противоборства [203].

Военная стратегия сильного при действиях против слабого будет ориентирована не на разгром противника в ходе одной крупномасштабной кампании, а на его последовательное ослабление за счет сочетания серии ограниченных по масштабам и времени операций с мероприятиями политического, экономического и информационного характера. Основная ставка будет делаться на упреждение противника в действиях и обеспечение полной его информационной «прозрачности», демонстративном, но, по возможности, избирательном характере применения силы. Это снизит вероятность выхода ситуации из-под контроля и необратимой дестабилизации обстановки, вызовет у противостоящей стороны чувство безысходности и убедит ее принять условия победителя. Большое внимание будет уделяться максимальной политико-экономической изоляции противника при одновременном расширении круга собственных союзников и привлечении на свою сторону местной оппозиции. При нанесении ударов более сильная сторона попытается максимально реализовать свое техническое преимущество, нанося их противнику без вхождения в его зону поражения [203].

Стратегия действий слабого против сильного будет строиться на так называемом асимметричном подходе. В его основе лежит:

- навязывание противнику боевых действий в условиях, в которых сложно реализовать свое техническое преимущество;
- расширение географических границ и длительности конфликта;
- выбор объектов нападения не с учетом их военного значения, а с учетом воздействия на моральное состояние личного состава и гражданского населения противника;
- провоцирование несоразмерного применения силы;
- активное ведение информационного противоборства.

Будут предприниматься попытки компенсировать техническое отставание за счет напряжения всех материальных и духовных сил нации, придания войне тотального характера. В технической сфере данный подход выражается в уничтожении личного состава, а также в выводе из строя дорогостоящих и сложных систем вооружения при помощи более дешевых средств. В политическом плане более слабые субъекты будут пытаться балансировать на грани войны и мира, инициировать различные переговоры с целью затягивания времени, пытаться заручиться поддержкой авторитетных членов международного сообщества [203].

Слабейшая сторона попытается обезопасить свои силы от ударов с использованием ВТО, рассредоточив их в густонаселенных урбанизированных зонах, местах выращивания сельскохозяйственных культур, дельтах рек, джунглях и горах. В подобных местностях проживает более 75% населения Земли. Как правило, для зон со сложными физико-географическими условиями характерно чередование открытых и труднопроходимых участков, в пределах которых скован маневр и снижены возможности для наблюдения, поэтому вероятность неожиданного боевого столкновения с врагом в ближнем бою, нивелирующим техническое превосходство, гораздо выше. При ведении боевых действий против превосходящих сил противника ставка будет делаться не на разгром его вооруженных формирований, а на моральное подавление, нанесение регулярных потерь путем совершения диверсий, обстрелов, действий из засад, ведения минной войны. Имеющиеся дорогостоящие образцы современного ВВТ (авиация, зенитные ракетные комплексы, тактические ракеты, бронетехника, боевые корабли и катера) слабая сторона постарается рассредоточить, замаскировать, применять постепенно и внезапно для поддержания у против-

ника состояния неопределенности в течение максимально длительного времени. Не исключена возможность совершения терактов против гражданского населения противника и местных коллаборационистов [203].

Важной особенностью современных и будущих военных конфликтов является то, что они, преимущественно, будут вестись на урбанизированной местности, в городских агломерациях и мегаполисах, а не на открытой местности. При этом поле будущего дистанционного боя условно можно разделить на пять функциональных зон таких как [28, 29]:

- зона глубокой тактической разведки и воздействия на противника дальнобойными средствами (до 100 км от условной линии соприкосновения);
- зона маневрирования (60-80 км от линии соприкосновения войск);
- зона сближения и последовательного применения огневых средств средней дальности (50-70 км от линии соприкосновения войск);
- зона ближнего боя (до 10 км от линии соприкосновения войск);
- тыловая зона (80-100 км от линии соприкосновения войск).

В военном конфликте такие понятия как фронт и тыл, линия боевого соприкосновения, фланги, район сосредоточения, рубеж перехода в атаку и прочие термины, претерпят существенные изменения [29, 58]. Проведенный анализ развития средств вооруженной борьбы позволяет сделать вывод о том, что новизна будущих операций будет определяться, прежде всего, переносом вооруженной борьбы в новые пространства – реальные и созданные искусственно. Понятие театра военных действий утратит свое исключительно географическое значение и будет восприниматься как боевое пространство, объединяющее участки суши и акватории, часто разделенные сотнями километров, воздушное пространство, космос, а также информационную среду [203].

Поле боя преобразуется в своеобразное операционное пространство, декомпозированное на малые поля. При ведении боевых действий будет возникать эффект малых боев между полностью или частично автономными группами. Они могут быть разделены территорией, на которой находятся некомбатанты, потенциальные противники, объекты жизнеобеспечения населения. В результате исчезнет возможность и необходимость создания сплошной линии фронта, войска

(силы) должны будут находиться в постоянной готовности к столкновению с противником, быстрому переходу от наступления к обороне и наоборот. Численное преимущество в каждом конкретном случае будет создаваться не общей большой численностью личного состава, а его мобильностью и досягаемостью средств поражения [203].

Воздушно-космическое пространство будет широко использоваться для нанесения ударов и обеспечения действий войск (сил). Без завоевания превосходства в воздухе и космосе станет невозможным достижение устойчивого преимущества на суше и на море. В ходе воздушно-космических операций противнику будет наноситься наибольший ущерб, поэтому по своему значению они начнут доминировать над действиями сухопутных войск [203].

Борьба на море будет направлена, прежде всего, на обеспечение устойчивости своих транспортных коммуникаций и нарушение коммуникаций противника. Эти задачи приобретут особую важность с учетом роли морского и трубопроводного транспорта в обеспечении энергоресурсами основных потребителей. Кроме того, повысится значение Мирового океана как среды, в которой могут скрытно и быстро перемещаться носители ракетно-ядерного и обычного высокоточного оружия, элементы ПРО, десантные силы, средства разведки и наблюдения. В результате количество средств поражения стратегической и оперативной досягаемости, размещенных на морских платформах, может превысить количество аналогичных средств на воздушных и наземных носителях [203].

Высокая эффективность средств поражения и динамика изменения обстановки в ходе вооруженной борьбы повысят значимость управленческих ошибок, а в ряде случаев не оставят времени и ресурсов на их исправление, поэтому стремительно возрастет потребность в упреждающей разведывательной информации. Для снижения временной задержки между получением информации и ее реализацией средства разведки и поражения будут интегрироваться в единые системы телекоммуникационными сетями, связывающими пространственно-распределенные элементы [203].

Боевые действия в войнах будущего станет труднее классифицировать по признаку их принадлежности к стратегическому, оперативному или тактическому уровню, так как активность каждого из них окажет прямое влияние на обстановку в целом. Такое встречалось и раньше, но сейчас тесная взаимосвязь событий на локальном, региональном и глобальном уровнях стала нормой. Вылазка группы боевиков или поведение солдата, участвующего в гуманитарной операции,

могут быть растиражированы СМИ и в считанные минуты оказать влияние на обстановку в зоне кризиса. Данный факт подтверждает вывод о «сжатии» элементов стратегического, оперативного и тактического уровней в объеме одного конфликта. Все чаще действие на тактическом уровне сказывается на ходе всей операции, что приводит к последствиям стратегического характера [203].

Широкое распространение получат операции и систематические боевые действия по блокированию зоны конфликта, установлению режима эмбарго. Возрастет значение операций по обеспечению безопасности территории и населения от различных разрушительных воздействий на объекты критической инфраструктуры. Ожидается, что такие воздействия будут осуществляться в форме терактов, диверсий, кибернетических атак и точечных ударов с использованием ВТО [203].

Качественно новые требования к мобильности, скрытности, приспосабливаемости, оснащенности и профессионализму боевых подразделений повлекут за собой дальнейшие изменения системы их всестороннего обеспечения. Гражданский персонал будет более активно привлекаться к решению вспомогательных задач, которые традиционно относились к компетенции военнослужащих: обслуживание техники, доставка грузов и охрана. Проведение операций на враждебной территории станет невозможным без военно-гражданского компонента, готового участвовать в восстановительных работах в интересах местного населения, решать первоочередные гуманитарные проблемы, поддерживать общественный порядок, воссоздавать лояльные местные органы самоуправления [203].

В настоящее время сущность и содержание войны продолжает коренным образом модифицироваться. Внедрение неядерных систем высокоточного оружия положило начало тенденции дистанционного воздействия на объекты противника вне зоны досягаемости его средств поражения. Развитие информационных технологий привело к тому, что война вышла за пределы материальной и физической сфер и перешла в виртуально-информационную и когнитивную сферы. Воздействие оказывается не столько на «физическую оболочку» субъектов войны (личность, армия, государство), сколько на духовную, психологическую и ментальную сферы. В ходе локальных войн, конфликтов, антитеррористических операций особое значение приобретут социально-политические, религиозно-этнические и психологические аспекты. Поэтому для разрешения конфликта ведущими, определяющими должны стать социально-политические мероприятия, помогающие заручиться поддержкой основной части населения. Боевые действия

будут носить очаговый характер и осложняться смешением населения и вооруженных формирований [1, 29, 62].

С точки зрения способов и стратегии ведения военных действий в войнах шестого поколения наиболее существенно изменяется соотношение прямых и непрямых действий. Непрямые действия, связанные с политическим, экономическим и морально-психологическим воздействием на противника, способами его дезинформации и подрыва изнутри, всегда играли большую роль. Однако в условиях войн четвертого и пятого поколений, основанных на идеях тотальной войны, прямые военные действия нередко превращались в самоцель, отодвигая на второй план непрямые воздействия информационно-психологического и экономического характера. В современных условиях, когда ядерное оружие превращается в сдерживающий фактор, а основной целью войны является поражение экономического потенциала противника, роль непрямых действий значительно возрастает. Речь идет о большей гибкости военного искусства, более полном использовании всего разнообразия средств и способов ведения, в том числе невоенных и нетрадиционных. Особое место в системе непрямых действий займут специальные методы ведения войны, начиная с психологических операций, подрывных действий и заканчивая операциями сил специального назначения. Вся вооруженная борьба будет пронизана разветвленным информационным противоборством [1].

Дистанционная война будет связана с применением новых форм и способов достижения политических и стратегических целей за счет развязывания локальных войн, конфликтов, политического, экономического, информационного давления и подрывных действий внутри противостоящих стран. Эти формы и способы являются своеобразным аналогом высокоточного оружия – при сохранении дальности и массированности поражения они используют новые сферы для осуществления воздействия: информационную, экономическую и психологическую.

Информационное оружие будет применяться на всех этапах подготовки и развития войны будущего в мирное и военное время, что определяется высокой скрытностью его воздействия. Информационное оружие будет основным средством войны в мирный период, а с началом боевых действий оно будет применяться главным образом в интересах обеспечения группировок вооруженных сил [5, 29]. При этом информационное противоборство станет неотъемлемой частью боевых действий. Без преимущества в этой сфере даже более сильная в военном плане сторона столкнется с серьезными трудностями при ор-

ганизации и ведении боевых действий. В техническом плане вывод из строя системы управления будет рассматриваться в качестве важного условия нанесения противнику поражения. Еще до начала военных действий должно быть завоевано полное информационное превосходство, а с их началом ставится задача в максимально короткие сроки добиться «паралича» системы управления противника. Нарушение работы линий связи, массовые сбои в работе вычислительных систем и отказы радиоэлектронного оборудования не позволят противостоящей стороне организованно вести боевые действия. Массированному психологическому воздействию подвергнется военно-политическое руководство, военнослужащие и гражданское население противника для подталкивания их к сознательному или спонтанному совершению определенных действий. Активная пропаганда будет направлена и на свое население, и на жителей «третьих стран» для формирования выгодных внутри- и внешнеполитических условий для дальнейшего ведения войны [203].

Дальнейшее развитие взглядов на ведение войны показывает, что предстоящая война – это, во-первых, системная война; во-вторых, война, где основными являются сложные эффекты всей системы; в третьих, война за обладание решающим потенциалом глобального управления.

Особенность вооруженной борьбы будущего будет состоять в том, что в ходе войны под ударами противника окажутся не только военные объекты и войска, но одновременно и экономика страны со всей ее инфраструктурой, гражданское население и территория. В бесконтактных войнах первой половины XXI века неизбежно возникнет ситуация, когда наличие хотя бы у одной из воюющих сторон, недостаточно эффективно обороняемых и не защищаемых объектов критической инфраструктуры (гидроэлектростанций, ядерных, химических, нефте- и газохранилищ и других подобных объектов экономики) может стать катастрофической экологической угрозой для всех окружающих стран, а не только воюющих. При этом произойдет смещение цели войны от физического уничтожения противника и оккупации его земель к подчинению противника своей воле и включению его в сферу своего влияния на приемлемых условиях [17, 27, 29].

Главной целью военных операций 6-го поколения будет разгром дистанционным способом экономического потенциала любого государства на любом удалении.

Сегодня война может вестись во всех физических средах – на суше, в воздухе, на воде и под водой, в космическом пространстве.

Однако уже сейчас, а тем более в будущем, актуальны и другие сферы: информационная, экономическая и психологическая. Поэтому содержание конкретных военных событий вооруженной борьбы будущего будет тесно взаимосвязано с другими видами противоборства – экономическим, информационным, психологическим, научно-техническим, дипломатическим и идеологическим [17, 29].

Новыми перспективными дистанционными способами ведения боевых действий являются нарушение функционирования структур управления атакуемой страны, инициирование раскола ее политических элит, нарушение социальной стабильности за счет сочетания подрывных психологических, экономических и социальных операций. Новым дистанционным способом ведения вооруженной борьбы будет удаленное поражение экономического потенциала любого государства, на любом удалении от противника [29, 58].

В войнах будущего эффективно будет применяться информационное оружие – скоординированное по времени психологические, пропагандистские и кибероперации в сочетании с экономическими и политическими санкциями как против руководителей государств – объектов агрессии, так и против элит, и простых граждан этих стран. Совокупность таких операций имеет своей целью психологическое подавление всех слоев населения стран-объектов агрессии, дезорганизацию системы управления этих стран, нарушение функционирования экономики [10, 29].

Расходование ВТО и оружия на новых физических принципах для разгрома живой силы противника может оказаться нецелесообразным, если будут разрушены в значительной мере экономика, системы государственного и военного управления.

Вооруженные конфликты и войны будущего будут порождаться не одним каким-либо, пусть даже весомым фактором, а сложным переплетением различных социально-политических, экономических, национальных и религиозных противоречий и причин.

Военный конфликт будущего будет включать в себя четыре периода [29, 58]:

- *подготовительный* (от нескольких часов до нескольких месяцев), сопровождающийся развязыванием массированного информационного противоборства и проведением подрывных экономических операций;
- *активный,* включающий в себя массированное применение ВТО, а также всех видов авиации по объектам государственного и военного управления, объектам критической

инфраструктуры, применение средств РЭП против систем связи и управления противника;

- *наземную операцию вторжения сухопутных войск* (при необходимости), включающую проведение военных операций по уничтожению противостоящих группировок войск противника, оккупацию ключевых объектов и установление контроля над его населением;
- *постконфликтный* (проведение операции по стабилизации), в котором основную роль будут играть информационно-психологические операции по обеспечению лояльности оккупированного населения.

При этом может измениться последовательность разгрома противника: если раньше оно начиналось с решительного наступления на приграничные группировки сухопутных войск, то перспективные средства высокоточного поражения позволят уже в ходе начальной операции вывести из строя важнейшие элементы системы административного и военного управления, оборонно-промышленного комплекса, транспорта и энергетики на всей территории страны [203].

В современных вооруженных конфликтах одной из особенностей ведения боевых действий является безусловный приоритет разведки, АСУ войсками и оружием и радиоэлектронной борьбы (РЭБ). Так, сетецентрическая концепция ведения боевых действий позволит решить вопросы различного воздействия на войска противника в масштабе времени, близком к реальному, без временных потерь на принятие решений и организацию последующего огневого поражения. В рамках этой концепции объединенные в единый информационный поток все виды разведки нацелены не только на вскрытие военного потенциала противника, но и на упреждение его действий, уничтожение его систем управления. При этом они, будучи объединенными со средствами поражения, в реальном масштабе времени непрерывно наносят противнику удары на всю оперативно-тактическую глубину [17, 29].

Еще одной фундаментальной характеристикой войн нового типа является приоритет ведения бесконтактных боевых действий на основе концепции максимального сбережения человеческого ресурса. Привычка к высоким стандартам качества жизни, выработанная в течение нескольких десятилетий благополучия, заставляет жителей постиндустриальных стран остро реагировать на малейшее снижение их жизненного уровня. С учетом этого обстоятельства политическое руководство США и стран Западной Европы только в самом крайнем случае сможет позволить себе масштабные мобилизационные меро-

приятия и ведение боевых действий, сопровождаемых существенными людскими потерями [203].

Войны будущего – это системная совокупность сложных процедур и технологий трансформационного и информационного воздействия на управляющие центры противника, которая лишь на конечном этапе – и то далеко не всегда – предполагает высокоинтенсивное применение обычных вооруженных сил.

Таким образом, в перспективе в XXI веке возможны различные по масштабам и содержанию войны. По типам их можно подразделить на [29]:

- традиционные (с применением силовых действий вооруженных сил);
- нетрадиционные (без применения силовых действий).

По видам их можно подразделить на [29]:

- вооруженные конфликты;
- локальные конфликты;
- региональные войны.

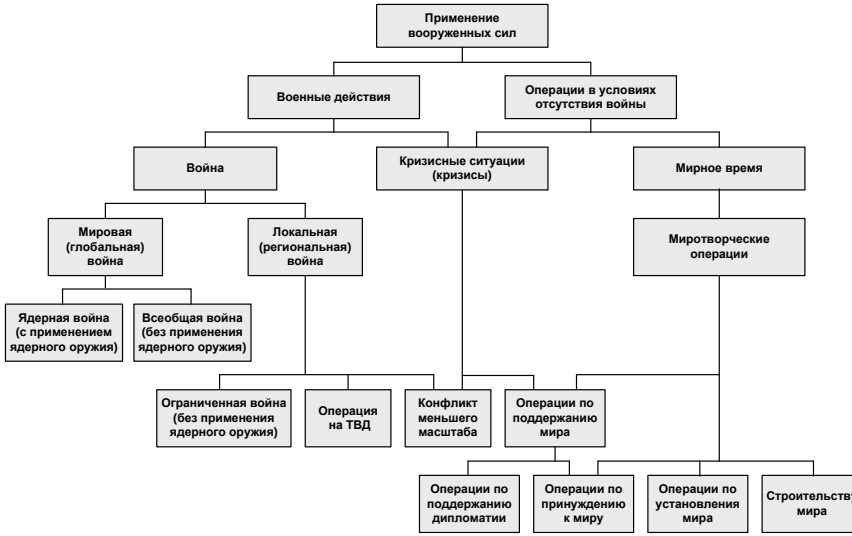


Рис. 2.2. Виды войн и вооруженных конфликтов

Таким образом, сущность и характер военных конфликтов позволяют сделать вывод о том, что при уменьшении вероятности развязывания широкомасштабной войны с применением ядерного оружия вероятность возникновения военных конфликтов регионального и локального характера не снизится. В этих условиях для реализации эф-

фективной политики сдерживания необходим более широкий спектр соответствующих сил и средств, включающих как ядерное, так и обычное высокоточное оружие, гарантирующих нанесение противнику ощутимого, но соразмерного ущерба. Кроме того, быстро меняющаяся обстановка потребует при отстаивании национальных интересов прибегать не только к сдерживанию потенциальных агрессоров, но и к своевременному проведению превентивных действий [230].

2.3.4. Современные тенденции по повышению роли высокоточного оружия, воздушно-космических и информационных средств при ведении войны

Достижения информационно-технической революции, воплощенные в ударных и оборонительных авиационных, ракетных, космических системах вооружения, в соответствии с новыми стратегическими и оперативными концепциями фундаментальным образом меняют характер и содержание вооруженной борьбы. В целом на перспективу после 2030 г. ожидается окончательное утверждение новых форм применения войск, таких как массированный удар ВТО, совместное применение средств РЭБ и огневого поражения и т.п.

Основными характерными чертами войн шестого поколения являются [17]:

- появление нового главного оружия военных действий – высокоточного оружия в обычном оснащении и массовое его применение;
- возможность поражения войск (сил), объектов тыла, экономики, коммуникаций на всей территории каждой из противоборствующих сторон без непосредственного вступления в соприкосновение с противником (бесконтактные войны);
- стремление сторон к дезорганизации системы государственного и военного управления;
- возможность асимметричного характера военных действий;
- активное информационное противоборство;
- дезориентация общественного мнения в отдельных государствах и мирового сообщества в целом;
- особая роль космических средств в ведении и обеспечении военных действий в космосе и из космоса;

- зачастую, отсутствие сплошной линии соприкосновения войск;
- зарождение новой оперативной концепции ведения военных действий – сетецентрической войны;
- участие в войне наряду с регулярными вооруженными силами других нерегулярных вооруженных формирований.

При этом для способов боевого применения именно сухопутных войск будут характерны следующие особенности [29]:

- действия войск и распределение усилий по направлениям, а не по рубежам;
- незначительная зависимость войск при создании группировки и ее развертывании от наличия объектов транспортной инфраструктуры (морских и речных портов, аэродромов и т.п.) в районе предстоящей операции;
- организация взаимодействия войск (сил) с использованием средств визуального отображения района проведения операции;
- достижение превосходства над противником за счет нанесения избирательных высокоточных ударов по целям, определяющим боеспособность противника;
- высокая автономность войск;
- высокая совместимость разнородных систем управления, разведки, связи, оружия и т.п.;
- увеличение степени рассредоточения формирований на поле боя, ведение боевых действий по отдельным, зачастую изолированным направлениям при наличии значительных разрывов в боевых порядках и промежутков в оперативном построении группировок наземных сил;
- появление новых функциональных элементов построения войск – вертолетных противотанковых и противодесантных резервов, аэромобильных десантов, воздушно-наземных тактических групп, группировок и средств разведки и РЭБ;
- значительный рост глубины эшелонирования группировок войск вследствие увеличения дальности поражения огневых средств (для корпусов – 300 км, дивизий – до 150-200 км) и перераспределение сил и средств между эшелонами;
- широкое применение формированиями наземных сил переброс по воздуху на различные расстояния, рост их до-

ступности и масштабов до аналогичных показателей наземного маневра.

Устойчивой тенденцией в изменении способов боевых действий можно считать стремление к одновременному разгрому противника на всю глубину его оперативного построения при сосредоточении огневой мощи против основных объектов, определяющих оперативную устойчивость группировки противостоящей стороны [29, 54].

В изменении характера вооруженной борьбы, как свидетельствует опыт войн и вооруженных конфликтов в течение последних десятилетий, одной из основных характерных особенностей явилось неуклонное повышение удельного веса войск, сил и средств, действующих в воздушной сфере и околоземном космическом пространстве, по отношению к другим сферам вооруженной борьбы [29, 54].

С большой вероятностью можно констатировать, что в XXI веке война окончательно станет «вертикальной». В этих условиях совокупность войск ВВС, ПВО, ПРО, ВКО (при поддержке комплексов РЭБ и ВТО) становится главенствующей, постепенно оттесняя сухопутные войска на второстепенные роли. Последние все больше будут использоваться в локальных войнах, противопартизанских и контртеррористических операциях.

Перемещение эпицентра вооруженной борьбы в воздушную и космическую сферу предопределено их особое положение и свойства [269]:

- во-первых, они занимают охватывающее, господствующее положение по отношению к другим сферам;
- во-вторых, физические свойства этих сфер оказывают минимальное сопротивление перемещению материальных тел и распространению электромагнитной энергии, что позволяет достичь высоких скоростей и больших дальностей полета, передачи информации и энергии.

В связи с этим изменяются пространственные характеристики вооруженной борьбы. Военные действия приобретают все более выраженное объемное (трехмерное) измерение. При этом усилия в них перераспределяются в пользу «вертикальных» (воздушной и космической) составляющих.

Эта тенденция связана с увеличением дальности применения высокоточного оружия и возможностью эффективного его использования для нанесения ударов по объектам, находящимся в глубоком тылу противоборствующей стороны. При этом война приобретает глобальный масштаб, что обусловлено межконтинентальными средствами

поражения, широким использованием космических систем (разведки, навигации, управления и связи), переносом главных событий военных действий в воздушную сферу и стратегическую космическую зону. С другой стороны, цели войны достигаются решением ряда задач на локальном уровне, например адресным, избирательным воздействием на наиболее важные объекты противника [269].

Театры военных действий, сформированные по географическому принципу, теряют свою значимость, поскольку все большее влияние на исход операций (боевых действий) на ТВД оказывает применение сил и средств, находящихся вне этих театров [269].

В войнах и вооруженных конфликтах XXI века будут максимально широко использоваться силы и средства воздушного, космического нападения, дальнего огневого и электронного поражения [269].

В связи с этим, для достижения поставленных целей последовательность действий группировок войск в вооруженных сил развитых государств меняется следующим образом [269]:

- вначале осуществляется завоевания информационного превосходства над противником в комплексе с применением экономических, политических, юридических и других невоенных мер;
- при обозначившемся успехе информационного противоборства проводятся воздушные наступательные операции, основу которых составляют массированные авиационно-ракетные удары. Они наносятся по ключевым элементам системы государственного и военного управления противостоящей стороны, ее важнейшим экономическим объектам, а также группировкам войск;
- обеспечивается господство в стратегической космической зоне своих космических информационных систем, а в перспективе возможны и самостоятельные военные действия в космосе в целях завоевания господства в стратегической космической зоне и защите своих космических информационных ресурсов;
- после достижения целей воздушно-наступательной операции (кампании) могут быть начаты операции наземными группировками войск.

Таким образом, силы и средства воздушного и космического нападения и обороны становятся важнейшим средством универсального назначения, основным оружием войн XXI века. Они способны самостоятельно решать в военных конфликтах не только оперативно-

тактические и оперативные, но и оперативно-стратегические и стратегические задачи даже при применении лишь обычных средств поражения [269].

Активное использование космического пространства в военных целях может обеспечить [269]:

- получение полной и достоверной информации о противнике в масштабе времени, близком к реальному, и оперативное доведение ее до всех органов управления и элементов войск (сил);
- развертывание сил и систем оружия, способствующих достижению военных целей в конфликтах низкой интенсивности с минимальными потерями и минимальным ущербом для гражданского населения и окружающей среды;
- контроль над использованием другими странами космического пространства, а также акваторий морей и океанов;
- защиту национальной территории и развернутых группировок войск от оружия массового поражения и ударов средств воздушно-космического нападения, в первую очередь от баллистических и крылатых ракет.

Совершенствование средств воздушного и космического нападения обусловливает необходимость изменения системы обороны от ударов средств воздушно-космического нападения. Оборона, даже для условий обычной войны, должна быть комплексной – противовоздушной, противоракетной и противокосмической [269].

Изменения в характере вооруженной борьбы в войнах и вооруженных конфликтах начала XXI века приводят к фундаментальным изменениям основных положений военной стратегии и оперативного искусства, а именно [269]:

- увеличиваются темпы оперативного и стратегического развертывания войск (сил) на ТВД и темп ведения военных действий;
- среди видов военных действий предпочтение отдается наступательным действиям, а оборонительные рассматриваются как вынужденные, по возможности кратковременные, с постоянным стремлением перехвата инициативы и перехода к активным наступательным действиям;
- в операциях любого уровня задействуются, в первую очередь, те силы и средства, которые обеспечивают нанесение ударов по важнейшим компонентам боевого потенциала противника;

- на передний план выдвигаются формы и способы военных действий, предусматривающие согласованное применение максимально рассредоточенных группировок разнородных сил и средств различного базирования;
- принцип массированного применения сил и средств на избранных направлениях (в заданных районах) дополняется непрерывным длительным воздействием на противника с различных направлений всеми имеющимися силами и средствами вооруженной борьбы, в том числе максимально рассредоточенными;
- возрастает роль и значение не только мобильности войск (сил) на тактическом и оперативном уровнях, но и стратегической мобильности вооруженных сил в целом.

Естественным следствием изменений в характере вооруженной борьбы, обусловленных в том числе повышением значимости космических сил и средств, является зарождение новых форм вооруженной борьбы, таких как [269]:

- космическая операция;
- информационно-ударная операция;
- высокоточное сражение и др.

Космическая операция будет, как правило, предшествовать воздушным, морским и наземным наступательным операциям. Она будет направлена на завоевание господства в околоземном космическом пространстве с целью обеспечения беспрепятственного функционирования своих орбитальных группировок, свободы доступа и действий в космосе и соответственно воспрепятствованию свободе доступа и действий в космическом пространстве противника. Опыт военных конфликтов последних десятилетий показал, что важнейшая роль отводилась ведению разведки техническими средствами из космоса с передачей разведывательной информации в масштабе времени, близком к реальному, организации связи, топогеодезическому и метеорологическому обеспечению. В связи с этим основными задачами космической операции будут уничтожение (блокирование) важнейших элементов космической инфраструктуры противника, дезорганизация его системы управления войсками (в настоящее время в ведущих армиях мира все большее применение находят линии спутниковой связи) [269].

Информационно-ударная операция представляет собой совокупность взаимосвязанных и согласованных по цели, задачам, месту, времени и способам ведения информационно-ударных сражений, ин-

формационно-огневых боев и информационных ударов, проводимых с целью дезорганизации системы управления войсками и оружием противника и уничтожения его информационного ресурса [33, 72].

Это новая форма вооруженной борьбы, характерным элементом которой являются информационные удары, переходящие, в сочетании с огневым воздействием, в информационно-огневые бои и информационно-ударные сражения.

Информационно-ударная операция обладает высокой эффективностью, поскольку способствует завоеванию инициативы и превосходства в информационной сфере (управление войсками и оружием, рефлексивное управление противником и др.). Такие операции могут проводиться как самостоятельно, так и в комплексе с общевойсковыми, воздушными, морскими и космическими операциями в наступлении и в обороне, в оперативном и в стратегическом масштабах [269].

В условиях широкого развития радиоэлектроники эффективная дезорганизация системы информационного обеспечения боевых действий противника может быть осуществлена только комплексным воздействием разнородных сил и средств радиоэлектронной борьбы совместно со средствами огневого поражения. К первоочередным объектам воздействия в информационно-ударной операции относятся информационная инфраструктура, пункты управления и узлы связи объединений и соединений, авиации, ракетных войск и артиллерии, разведывательно-ударных (огневых) комплексов, разведки, противовоздушной обороны и радиоэлектронной борьбы [269].

Высокоточное сражение – новая форма вооруженной борьбы, обусловленная интенсивным развитием высокоточного оружия, появлением новых средств радиоэлектронной борьбы и космических систем разведки и навигации [269].

По значимости высокоточное сражение относится к стратегической операции. В войнах в зоне Персидского залива, а также в Югославии и Афганистане посредством проведения высокоточного сражения, по существу, достигались основные цели войны: разгром группировок войск противника, завоевание господства в воздухе и огневого превосходства, дезорганизация системы государственного и военного управления, уничтожение (разрушение) важнейших элементов инфраструктуры [269].

Высокоточное сражение интегрирует в себе нанесение массированных ракетно-авиационных, групповых и одиночных электронно-огневых ударов, систематические боевые действия войск ПВО, мощное радиоэлектронное воздействие, применение сил специальных опе-

раций, а также действия общевойсковых формирований и морской пехоты. При этом доминирующую роль играли крылатые ракеты морского и наземного базирования, стратегическая авиация, разведывательно-огневые и разведывательно-ударные комплексы, эффективность применения которых обеспечивалась орбитальной группировкой, прежде всего системами космической разведки и навигации, а также средствами радиоэлектронной и информационной борьбы [269].

Главным способом ведения высокоточного сражения является дальний огневой разгром противника [269].

Управление большим количеством разнородных сил и средств, участвующих в проведении высокоточного сражения, разворачивающегося во всех физических средах – на земле, в воздухе, на море и космосе, было бы невозможно без информационной поддержки из космоса, создания интегрированных межвидовых систем разведки и оружия, широкого применения космической навигации для организации разведки, управления войсками, авиационной поддержки, а также без космических средств связи.

Новым элементом оперативного построения в высокоточном сражении может в перспективе стать космический ударный эшелон, который будет самостоятельно решать боевые задачи и осуществлять боевую поддержку из космоса действий наземной группировки войск [269].

2.4. Концепция сетецентрической войны как развитие системы взглядов на военное искусство с использованием преимуществ информационно-технической революции

2.4.1. Факторы, определившие разработку концепции сетецентрической войны

Необходимость в пересмотре принципов военного управления состоит в том, что изменившийся за последнее время характер угроз практически не оставил времени на принятие решений командирам всех уровней. Существовавшие ранее концепции ведения военных действий и созданные на их основе вооруженные силы плохо приспособлены к противодействию угрозам нового времени. В настоящее время уже нет возможности тратить месяцы или даже недели на разработку планов применения войск и их развертывание. Вместо этого необходимо применять силы уже в первые часы военного конфликта.

При этом первыми будут применены те средства, которые ориентированы на цели, воздействие на которые способно привести к желаемому эффекту и повлиять на дальнейшее поведение противника. Кроме того, вооруженные силы технически развитых государств, имея высокоточное оружие и глобальные средства разведки, которые способны обнаружить и поразить цель с большой точностью, испытывают сложности в информационном комплексировании и управлении для достижения информационного превосходства в скорости принятия решений [2, 29].

По мнению ряда экспертов [2, 29], ограничения традиционных вооруженных сил включают в себя:

- существенную зависимость от мест базирования;
- недостаток сил для выполнения возросших требований по эффективности и своевременности боевого применения;
- недостаточный уровень стратегической мобильности для быстрого развертывания мощных, но тяжелых сил;
- недостаточные дальности действия средств поражения.

Реальным катализатором трансформации вооруженных сил ведущих зарубежных стран послужила их совместная операция против Ирака «Буря в пустыне». Характерными для этой войны стали следующие аспекты [3]:

- противником возглавляемой США коалиции было государство, обладающее всем спектром современных вооружений;
- в войне не было использовано имеющееся у сторон оружие массового поражения;
- поражение сил и средств противника осуществлялось преимущественно дистанционно, без близкого контакта с ним;
- широкое использование новейших информационных технологий в системах боевого управления и связи.

По мнению ряда американских военных экспертов [112], новый взгляд на угрозы XXI века заключается в том, что сегодня даже среди традиционных государств, различие между враждебностью и невраждебностью практически нивелируется, поскольку новые способы воздействий (типа вторжений в компьютерные сети) мешают точно определить время начала боевых действий. Кроме того, предполагается, что в будущем основная угроза будет исходить не от регулярных вооруженных сил разных стран, а от всевозможных террористических, криминальных и других организаций, в том числе негосударственных, участники которых объединены на основе сетевых структур [2, 29].

К основным признакам таких сетевых организаций можно отнести следующие [2, 16]:

- наличие единой стратегической цели и отсутствие четкого планирования на тактическом уровне;
- отсутствие четкой иерархической структуры подчиненности, а зачастую и отсутствие центрального руководства;
- децентрализация и параллельность работы представителей организаций, затрудняющие контроль над их деятельностью, в том числе со стороны государственных и правоохранительных органов;
- многоуровневая структура с разветвленной и сложной системой связей и вложенных сообществ;
- координация своей деятельности с использованием средств глобальных информационных сетей;
- высокая динамика развития за счет хорошо налаженного обмена информацией и способности к быстрой реорганизации в случае необходимости.

Приведенные выше признаки являются характерными для сетевой формы организации, получившей при информатизации общества новый импульс для развития, поскольку их эффективность напрямую зависит от скорости и качества обмена информацией, эти характеристики должны быть гораздо выше, чем в иерархических структурах. Для обозначения подобных структур появился специальный термин SPIN (Segmented, Polycentric, Ideologically Integrated Network) (сегментированная, полицентрическая, идеологизированная сеть) [2, 16].

В ближайшие 10-20 лет вооруженным силам придется действовать в среде, характеризующейся все возрастающей сложностью, непредсказуемостью и динамизмом. Использование потенциальным противником асимметричных стратегических концепций и широкое распространение дистанционных видов оружия (прежде всего – высокоточных ракетных комплексов и средств информационного воздействия) создадут дополнительную нагрузку на все компоненты вооруженных сил и государственного управления. В будущем ведение боевых действий потребует не только повышения степени взаимодействия сил и средств, но и большего участия в них других государственных структур, ведомств и партнеров по коалициям. Чтобы добиться успеха в новых условиях, необходимо иметь способность динамически интегрировать самые разнообразные множества сил и средств для реализации новых возможностей, которые можно потен-

циально получить как за счет использования внутреннего ресурса самих вооруженных сил, так и задействования других госструктур и т.п. Необходимо уменьшить внутренние формальные процедуры согласования в интересах повышения адаптированности вооруженных сил к новым условиям. При этом повышение уровня интеграции сил и средств должно быть распространено до самого низкого уровня управления [112].

В условиях изменения модели угроз изменяются роль и место вооруженных сил в вооруженной борьбе. В большей степени акцент делается на проведение невоенных операций, что требует повышения значимости информационной сферы противоборства, а также тесного взаимодействия с негосударственными организациями и структурами.

Для организации деятельности вооруженных сил в условиях воздействия новых угроз и была разработана концепция сетецентрической войны. По мнению ее авторов, «сетецентрическое противоборство» или «сетецентрическая война» является лучшим термином, предложенным к настоящему времени для описания пути организации и ведения противоборства в информационную эпоху.

2.4.2. Теория декомпозиции стратегических целей на пять колец Джона Вардена

Джон Варден (John Warden) является специалистом в области применения ВВС, кроме того, он сформировал свое видение выбора стратегических целей для войны XXI века, которое легло в основу концепции сетецентрических войн.

В своей работе [86] Дж. Варден подчеркивает доминирование воздушно-космических сил, а также тот факт, что самым эффективным и действенным применением авиации является стратегический уровень. Концепция стратегической войны Дж. Вардена обосновывает выбор в качестве основной цели для атаки – жизненные центры противника, что позволяет достичь желательных изменений в политике. Дж. Варден в своих работах развивает стратегию выведения противника из строя через «обезглавливание» и акцентирует свое внимание на воздушных ударах по «центрам тяжести» противника. Основной мыслью работы [86] является то, что ВВС обладают уникальной способностью достичь стратегических целей войны с максимальной эффективностью и минимальной стоимостью. Присущая им скорость, радиус действия и гибкость позволяют быстро осуществлять удары по наиболее важным целям противника. К таким целям Дж. Варден отно-

сит «центр тяжести», определяемый им как «та точка, в которой противник наиболее уязвим, и точка, атака по которой имеет лучшие шансы быть решающей». Предполагается, что такие центры являются источниками как силы противника, так и его уязвимости. При этом двойственная природа «центров тяжести» используется при планировании кампании. Вездесущность ВВС теоретически делает уязвимыми для атаки гораздо большее по сравнению с другими силами число стратегических «центров тяжести».

В дальнейшем, к концу 1988 г. Дж. Варден, анализируя врага как систему, разработал модель ранжирования стратегических «центров тяжести» противника в форме пяти концентрических колец (рис. 2.3) [84].

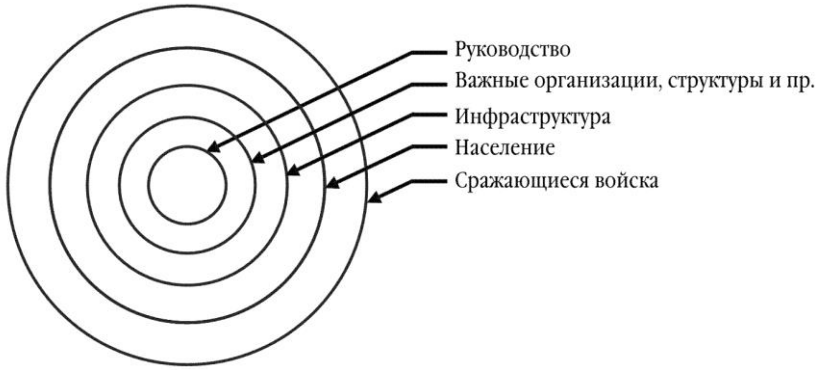


Рис. 2.3. Модель Джона Вардена ранжирования стратегических «центров тяжести» противника [84]

Дж. Варден утверждает, что все стратегические объекты могут быть разделены на пять составляющих частей. Наиболее критический элемент системы, ее самое внутреннее кольцо – это руководство. От руководства, находящегося в центре, по убывающей важности, с точки зрения способности функционирования системы как целого, расположены кольца критических объектов: инфраструктуры, населения и вооруженных сил [84].

В пределах каждого кольца существует один или несколько «центров тяжести», представляющих собой «узел силы и движения» для данного кольца. При этом если он разрушен или нейтрализован, то эффективное функционирование кольца прекращается, причем последствия этого будут оказывать влияние на всю систему (в зависимости от того, идет ли речь о внутреннем или внешнем кольце). Для точ-

ного определения ключевых узлов внутри каждого кольца Дж. Варден предлагает дальнейшее разбиение каждого из них на пять «субколец»: руководство, критические объекты и т.д., каждое из которых, при необходимости, еще раз делится на пять колец, пока не будет получена действительная картина будущих целей [84].

Центральным аспектом модели пяти колец является то, что наиболее эффективный стратегический план всегда фокусируется, прежде всего, на руководстве. Фактически внутри данных колец лежат некоторые психологические «центры тяжести», поражение которых приведет к небольшому уровню физического ущерба, но вызовет формирование понимания нецелесообразности дальнейшего сопротивления у командования противника. Таким образом, если разрушение или нейтрализация руководства приведет к полному физическому параличу системы управления противника, то успешная атака на «центры тяжести» внутри других колец приведет к мощному психологическому давлению на руководство [84].

Данная модель стратегического целераспределения была успешно апробирована на практике в войнах в Ираке в 1990-х. Из этой апробации Дж. Варден извлек несколько уроков, наиболее важными из которых были [84]:

- важность стратегической атаки и хрупкость государств на стратегическом уровне;
- фатальные последствия потери стратегического и оперативного превосходства в воздухе;
- подавляющие эффекты параллельной войны (то есть почти одновременная атака стратегических «центров тяжести» по всему ТВД);
- ценность информационных технологий и высокоточного оружия при переопределении принципов массированности сил и внезапности нападения.

На протяжении следующих 25 лет Дж. Варден разработал теоретический базис применения ВВС в XXI столетии [84]:

- при планировании операции необходимо оценить политические цели, достижение которых планируется достичь в результате военных действий;
- необходимо выбрать наилучшую военную стратегию, которая принудит противника исполнить навязываемую ему волю, как это определяется политическими целями и задачами;

- необходимо использовать системный анализ «пяти колец» чтобы определить, какие «центры тяжести» станут объектами первостепенной параллельной атаки.

В терминах целей Дж. Варден принимает максимализм Клаузевица, утверждающий, что все войны ведутся во имя политических целей. С этой точки зрения войны, по сути, представляют собой конфликт между группами политиков на каждой из сторон. Целью всех военных действий является не уничтожение вооруженных сил противника, а скорее манипуляция волей руководства противника. Дж. Варден уточняет: «Войны ведутся, чтобы склонить руководство противника сделать то, что мы хотим, чтобы он сделал, – то есть пошел на политические уступки. … Руководство противника соглашается, что оно должно пойти на определенные политические уступки, когда его стратегические «центры тяжести» находятся под угрозой или под невыносимым давлением. … Таким образом, атака на промышленность или инфраструктуру, прежде всего, проводится не из-за эффекта, который может быть оказан на вооруженные силы, а скорее для оказания прямого эффекта на систему управления противника, включая воздействие (прямое или косвенное) на национальных лидеров и командование…» [84].

Теория Дж. Вардена может быть графически изображена следующим образом (рис. 2.4).

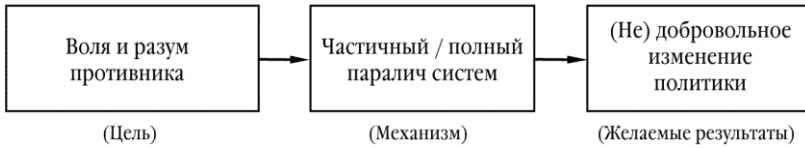


Рис. 2.4. Графическая интерпретация
теории Дж. Вардена [84]

Развивая свою теорию Дж. Варден предлагает три основных способа навязать противнику нужные действия [84]:

- стратегия принуждения;
- стратегия выведения из строя;
- стратегия полного уничтожения.

Стратегия принуждения (навязанной стоимости) предполагает, что продолжение сопротивления слишком дорого для командования противника. Эта стратегия предусматривает оценку порога неприемлемого ущерба противника на основе его системы ценностей и затем превышение этого порога столь интенсивно, насколько это возможно

через одновременную атаку множества назначенных целей. Теоретически такая атака принуждает руководство противника принять навязанные условия и изменить свою политику через фактическое достижение частичного уровня неприемлемого ущерба [84].

Стратегия выведения из строя предполагает сделать невозможным для командования противника продолжение сопротивления за счет полного и одновременного выведения из строя его критических «центров тяжести». В этом случае достигается частичный паралич системы – система противника существенно снижает свою эффективность, противник не может вести осмысленное сопротивление или же осуществлять управление [84].

Стратегия полного уничтожения предусматривает полное уничтожение всей системы противника. Примером данной стратегии могут являться действия фашистского режима по уничтожению еврейской системы. Данная стратегия редко встречается на практике, трудна в исполнении, чревата морально-психологическими проблемами и обычно не очень полезна из-за непреднамеренных последствий, которые она порождает. С учетом этих факторов Дж. Варден отвергает данную военную стратегию как политически нежизнеспособную для применения в войне XXI века [84].

При выборе целей воздействия Дж. Варден предлагает декомпозицию и анализ каждого стратегического кольца до тех пор, пока не будет выявлен компонент, являющийся тем «центром тяжести», поражение которого обеспечит частичный или полный паралич всей системы противника. Предлагаемая им последовательная декомпозиция с увеличением глубины рассмотрения системы противника позволяет вскрыть взаимозависимость и «связность» элементов системы. Как следствие – полный анализ системы может вскрыть «центры тяжести», которые имеют связи, как между кругами, так и с компонентами, находящимися в пределах кругов [84].

Таким образом, теория Дж. Вардена утверждает, что эффективная стратегия является следствием всестороннего исследования противника с учетом политических, экономических, военных и социокультурных факторов. Кроме того, несмотря на то, что модель базисных пяти колец может быть очень упрощенной, анализ «первого порядка», успешная декомпозиция колец на элементы позволит выявить динамические взаимосвязи в пределах и между кольцами, которые уникальны и важны для конкретного общества или рассматриваемой культуры. Таким образом, модель стандартных «пяти колец» является отправной точкой для последующего более глубокого анализа при ре-

шении задачи идентификации наиболее важных «центров тяжести» противника [84].

При декомпозиции и анализе системы противника на основе теории Дж. Вардена следует обращать внимание на следующие три фактора.

Во-первых, даже если анализ системы противника корректен, ключевое правило теории о первоочередном выборе в качестве цели руководства системы не обязательно является корректным. Руководство не всегда является самой важной целью. Другие кольца (или связи между ними) могут и зачастую содержат гораздо более важные «центры тяжести». Теория Джона Вардена не отрицает этого, но указывает, что в большинстве случаев цели во внешних кольцах должны быть выбраны так, чтобы влиять на расчет показателя «затраты – выгоды» именно для руководства системы, так как именно оно определяет политический курс, который необходимо изменить [84].

Во-вторых, теория Дж. Вардена дает ключ к понимаю потенциальной роли информационно-психологических, экономических и других нелетальных воздействий на руководство противника в составе общей операции. Она показывает, что поражение системы противника может быть достигнуто исключительно через информационно-психологическое воздействие на руководителей системы, через навязывание своей системы ценностей или снижение воли к сопротивлению.

В-третьих, теория Дж. Вардена имеет дело с односторонним действием, предпринимаемым против пассивного противника. Таким образом, игнорируются циклы «действие-реакция» и сопутствующие им факторы конфликтного взаимодействия систем. При этом Дж. Варден утверждает, что если нападающая сторона имеет заведомо более быстрый цикл управления «наблюдай – ориентируйся – решай – действуй», то это фактически исключает возможность реакции противника на стратегическом уровне управления [84].

В настоящее время теория Дж. Вардена широко применяется при выборе стратегических целей при планировании военных операций. Кольца Вардена вошли в военные документы вооруженных сил ряда западных государств, а разработанная Дж. Варденом теория, наряду с теорией циклов Бойда, легла в основу концепции сетецентрической войны.

2.4.3. Теория циклов Джона Бойда

Джон Бойд (John Boyd) является одним из наиболее ярких представителей военно-теоретической науки Соединенных Штатов Америки конца XX века. Теоретические положения, выдвинутые Дж. Бойдом, по оценкам современных зарубежных исследователей, не являются чем-то сверхновым, но в совокупности составляют простую и логичную концептуальную схему военной деятельности, оказавшую существенное влияние на процессы вооруженной борьбы.

В соответствии с идеями Дж. Бойда, любая деятельность в военной сфере с определенной степенью приближения может быть представлена в виде кибернетической модели OODA (НОРД): Observe – Наблюдай; Orient – Ориентируйся; Decide – Решай; Act – Действуй. Указанная модель предполагает многократное повторение цикла действий, составленного из четырех последовательных взаимодействующих процессов, таких как: наблюдение, ориентация, решение, действие (рис. 2.5).

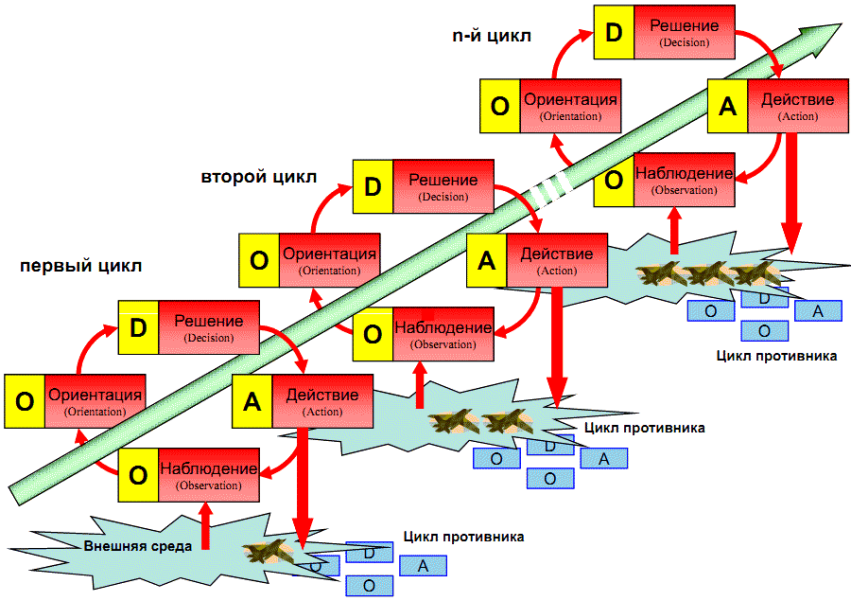


Рис. 2.5. Цикл OODA [290]

Фактически имеет место развитие ситуации по спирали, и на каждом этапе этой спирали осуществляется взаимодействие с внешней средой и воздействие на противника. Модель обычно относят к

разряду кибернетических, так как в ней реализуется принцип «обратной связи», в соответствии с которым «часть выхода из системы снова подается на ее вход», чтобы уточнить, а если потребуется, то и скорректировать развитие системы на последующих этапах [84, 290].

В англоязычных изданиях цикл OODA иногда называют циклом Бойда (Boyd Cycle). В отдельных отечественных публикациях ей присвоено также достаточно лаконичное и запоминающееся название «цикл НОРД».

В ряде официальных доктринальных документов МО США петля OODA рассматривается в качестве единой типовой модели цикла принятия решений для систем командования и управления как своих войск, так и войск противника.

Рассмотрим более подробно каждый из четырех отдельных элементов указанного цикла в соответствии с работой [290].

Наблюдение (*Observation*) – это процесс сбора информации, необходимой для принятия решения в данном конкретном случае. Необходимая информация может быть получена как от внешних, так и от внутренних источников. Под внутренними источниками информации понимаются элементы обратной связи петли. В качестве внешних используются датчики, а также другие каналы получения информации.

Ориентация (*Orientation*) – это наиболее ответственный и наиболее сложный с когнитивной точки зрения этап цикла OODA. Этап ориентации состоит из двух подэтапов: декомпозиции (Destruction) и синтеза (Creation). Декомпозиция предполагает разбиение ситуации на мелкие элементарные части, которые проще поддаются осмыслению. Человек или организация, принимающие решение, декомпозируют задачу до такого уровня, на котором вновь образованные составляющие задачи становятся близкими к стандартным или типовым ситуациям, для которых у лиц, принимающих решение (ЛПР), имеется план действий. ЛПР попросту идентифицируют текущую ситуацию по отношению к тем, с которыми он знаком, и применяют заранее заготовленный план действий для этой подзадачи. Затем эти составляющие элементарные подпланы объединяются в общий план действий, что и соответствует подэтапу синтез. Если нет планов, из числа которых может быть выбрано решение, то процесс остается на этапе ориентации и осуществляется дальнейшая декомпозиция задачи. Если не удается разработать план с реальными шансами на успех, то это может привести к остановке цикла.

Принятие решения (*Decision*) – третий этап цикла OODA. Если к этому этапу ЛПР смогли сформировать только один реальный план, то попросту принимается решение – выполнять этот план или нет. Если же сформированы несколько альтернативных вариантов действий, то ЛПР на данном этапе осуществляют выбор наилучшего из них для последующей реализации. Выбор наилучшего плана может осуществляться по критерию эффективность–стоимость.

В условиях лимита времени наиболее предпочтителен план, отвечающий требованиям быстроты и надежности.

Действие (Action) – заключительный этап цикла, предполагающий практическую реализацию избранного курса действий или плана. Действие предполагает выдачу приказа или указания, физическую атаку, активную защиту, перемещение в пространстве или управление датчиками с целью улучшения наблюдаемости объектов в следующем боевом цикле.

Отличительная черта цикла OODA от других циклических моделей состоит в том, что в любой ситуации всегда предполагается наличие противника или соперника, с которыми ведется вооруженная борьба, соперничество или конкуренция. Противник, соперник или конкурент также действуют и принимают решения в рамках своего аналогичного цикла. На рис. 2.6 представлена модель вооруженной борьбы с учетом цикла OODA для двух противоборствующих сторон [290].

При обосновании цикла OODA Дж. Бойд стремился подкрепить их философскими обоснованиями с использованием трех основных научных теорем [290]:

- теоремы Геделя о неполноте: любая логическая модель реальности не полна (и возможно не состоятельна) и должна непрерывно улучшаться (адаптироваться) с учетом новых наблюдений;
- принципа неопределенности Гейзенберга: существует предел нашей способности наблюдать реальность с определенной точностью. Любые малые ошибки наблюдений, включенные в вычисления, могут привести со временем к увеличению объема неточностей;
- второго закона термодинамики: энтропия (хаос) любой замкнутой системы всегда стремится к увеличению и, следовательно, природа любой заданной системы непрерывно изменяется, даже если принимать меры по сохранению ее в исходном состоянии. Более того, предпринимаемые нами

действия с целью повлиять на любую систему будут иметь непреднамеренный сторонний эффект, который может в действительности привести к увеличению скорости изменения энтропии системы (и, следовательно, к хаосу).

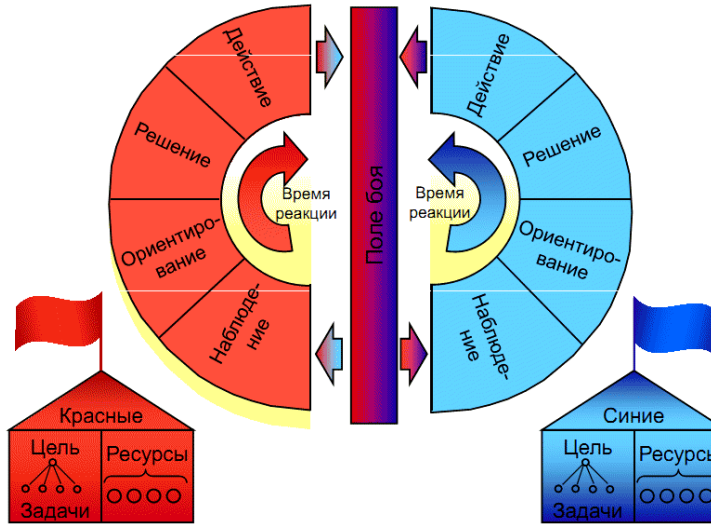


Рис. 2.6. Модель вооруженной борьбы двух противоборствующих сторон с учетом циклов OODA [290]

Именно исходя из этих соображений Дж. Бойд сделал вывод о том, что для того, чтобы соответствовать реальности необходимо осуществлять действия в непрерывном цикле во взаимодействии с окружающей средой, учитывая постоянные изменения цикла [290].

Кроме перечисленных теорем, для обоснования своих воззрений Дж. Бойд привлек теорию эволюции Дарвина. Предположив, что естественный отбор действует не только в биологической среде, но и в социальной (проявляется в выживании людей в войнах и в бизнесе, в условиях рыночной конкуренции) [290].

Объединив эти перечисленные выше положения, Дж. Бойд выдвинул гипотезу о том, что цикл деятельности и принятия решения OODA является центральным механизмом адаптации, а также о том, что преимущество в скорости своего цикла действий и точности оценок обеспечивает преимущество над противостоящей стороной и ведет к достижению победы в военных действиях.

В своих теоретических построениях Дж. Бойд подразделял войну на три состовных части [290]:

- *моральную войну* – разрушение воли противника к достижению победы путем его отделения от союзников (или потенциальных союзников) и внутреннего раздробления, подрыва общей веры и общих взглядов;
- *ментальную войну* – деформацию и искажение восприятия противником реальности, достигаемы путем дезинформации и создания неправильных представлений о ситуации;
- *физическую войну* – разрушение физических ресурсов противника (вооружения, живой силы, инфраструктуры и предметов снабжения).

Фактически Джон Бойд признавал три сферы получения эффекта от проведения военных операций, что впоследствии послужило созданию теории планирования операций на основе эффектов (EBO – Effect Based Operations).

На рис. 2.7 схематически показана примерная цепочка логических рассуждений, приведшая к созданию основного элемента теории Джона Бойда – цикла военной деятельности OODA и трех основных сфер проявления ее эффективности [290].

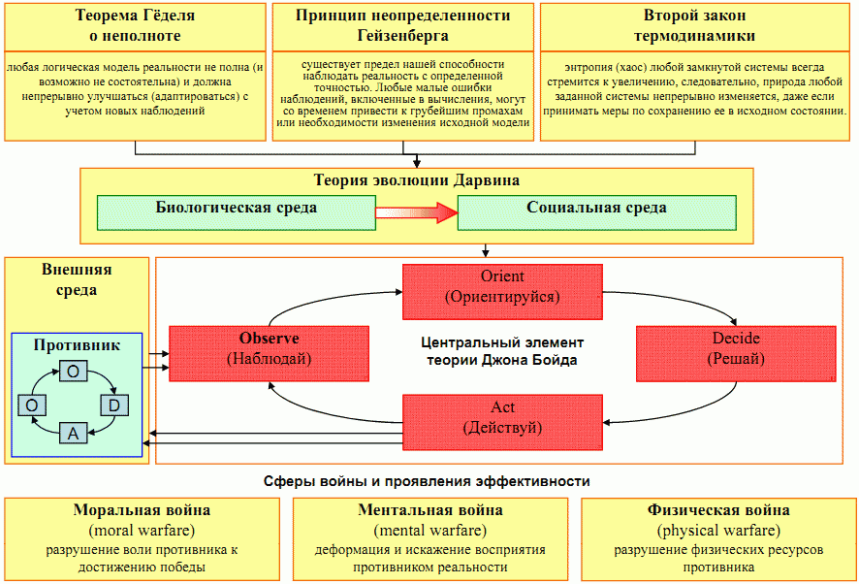


Рис. 2.7. Логика обоснования цикла военной деятельности OODA [290]

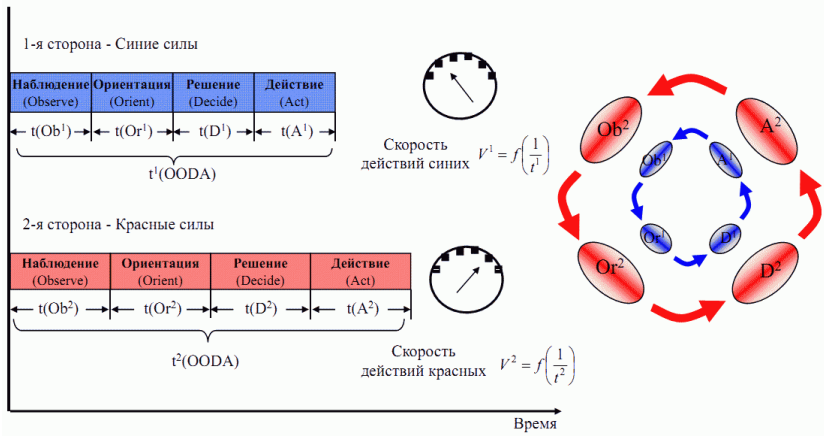
Существуют два основных способа достижения конкурентных преимуществ при осуществлении военной деятельности [290]:

- сделать в количественном измерении свои циклы действий более быстрыми, что позволит действовать первым и вынудит противника реагировать на действия;
- улучшить качество принимаемых вами решений, то есть принимать решения, в большей степени соответствующие складывающейся ситуации, чем решения противника. Более качественные решения могут привести к более предпочтительным результатам, нежели быстрые, но неадекватные или плохо просчитанные действия.

С учетом указанных соображений на каждом шаге процесса необходимо стремиться к постепенному получению качественных и количественных улучшений. Рассмотрим более подробно эти два направления получения конкурентных преимуществ [290].

Ускорение цикла OODA. В соответствии с теорией Дж. Бойда необходимо «регулировать изнутри» процесс деятельности противника или побеждать за счет более быстрой, чем у оппонента, собственной петли действий [290].

На рис. 2.8 приведена графическая интерпретация временных соотношений двух противоборствующих сторон.



а) Скорость действий определяет победителя в цикле Бойда

б) «Синие силы» действуют внутри цикла «красных сил»

Рис. 2.8. Графическая интерпретация временных соотношений OODA-циклов для противоборствующих сторон [290]

Ускорение процесса принятия решений может привести к двум видам эффекта.

Первый эффект по своей природе имеет чисто наступательный характер. Одна из сторон может начать осуществлять свой план первой и тем самым вызвать изменения в обстановке прежде, чем начнет действовать ее противник – рис. 2.9, 2.10.

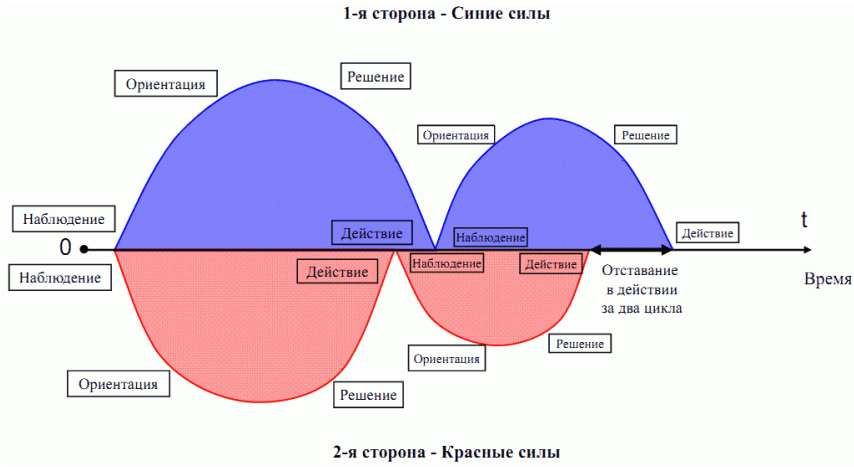


Рис. 2.9. Отставание в действии за два цикла [290]

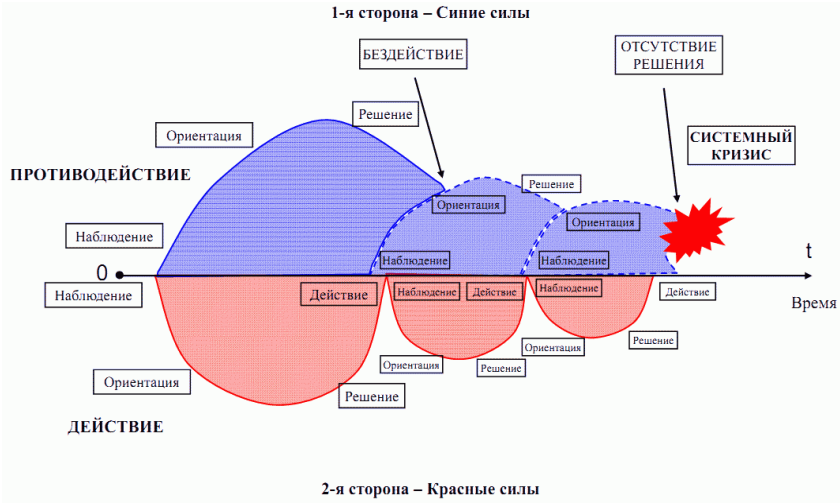


Рис. 2.10. Эффект системного кризиса [290]

Как показано на рис. 2.9, отставание в скорости действий ведет к накоплению времени отставания за несколько циклов и впоследствии к системному кризису для красной стороны. Если для осуществления плана необходимо участие противника (например, противник должен иметь определенную дислокацию), то инициатива в действиях позволяет добиться определенных условий перед началом реализации запланированных действий. Это преимущество первого удара находит свое воплощение в простой формулировке – можно убить противника прежде, чем он начнет стрелять [290].

Второй эффект сводится к ускорению собственного цикла действий OODA и носит оборонительный характер. Сторона с преимуществом в скорости цикла действий способна в ряде случаев избежать поражающего или вредоносного воздействия со стороны своего противника. Другими словами, она может стать «неуловимой целью» путем создания несоответствия ожиданиям атакующего противника [290].

Повышение качества решений. Качественное улучшение цикла OODA в данном случае означает, что качество принимаемых решений у стороны с более коротким циклом будет лучше, чем у противника. Оценка уровня качества принимаемых решений является величиной не абсолютной, а относительной, поэтому добиться конкурентного преимущества в принятии решений можно двумя способами [290]:

- совершенствовать свои решения;
- добиваться ухудшений решений, принимаемых противником.

Повышение качества собственных решений может быть достигнуто различными способами, к которым относятся:

- применение современных формальных математических методов;
- совершенствование информационно-аналитического и разведывательного обеспечения;
- применение автоматизированных систем управления, систем поддержки решений, экспертных и советующих систем.

Совершенствуя свой цикл OODA, следует постоянно помнить о том, что существуют реальные возможности снизить качество цикла принятия решений и деятельности противника путем создания помех и противодействия системам разведки и наблюдения (на этапе observe), введения противника в заблуждение (на этапах observe и orient), при-

нятия нехарактерных и непредсказуемых решений, называемых иногда сюрпризами (на этапе orient). Ослабить эффективность действий противника возможно и на этапе применения оружия (на этапе act) путем использования элементов активной защиты, например, динамической брони, тепловых и радиолокационных ложных целей [290].

Временные интервалы цикла OODA в войнах могут быть сокращены за счет применения перспективных датчиков различной природы, информационных технологий, технологий телекоммуникаций, средств вычислительной техники и быстродействующих исполнительных устройств. Наиболее сложным этапом с точки зрения сокращения времени является этап действия или применения оружия. Наиболее радикальными способами увеличения скорости поражающего фактора являются развитие гиперзвуковых технологий доставки и создание нетрадиционных видов оружия (кинетического, лазерного и сверхвысокочастотного) [290].

На основе анализа работ Дж. Бойда и его последователей в качестве постулатов теории OODA выделены следующие [290]:

1. Военная деятельность (боевые действия) противоборствующих сторон осуществляется в одинаковых кибернетических циклах OODA.
2. Содержание основных элементов цикла OODA:
   - наблюдение (Observation). Сбор информации от внутренних и внешних источников;
   - ориентация (Orientation). Формирование множества возможных планов (вариантов) и оценка каждого из них по совокупности критериев;
   - решение (Decision). Выбор наилучшего плана действий для практической реализации;
   - действие (Action). Практическая реализация избранного плана действий.
3. Цикл OODA является моделью военной и конкурентной деятельности отдельных лиц и организаций для войн и конфликтов любого масштаба (тактического, оперативного и стратегического).
4. Направления достижения победы (получения конкурентных преимуществ):
   - сокращение времени выполнения цикла OODA;
   - улучшение качества применяемых в цикле решений.

5. Увеличение скорости всех четырех элементов цикла OODA – главный путь достижения победы.
6. Эффект действий в цикле OODA может быть достигнут в трех сферах:
    - в моральной сфере: разрушение воли противника к достижению победы путем его отделения от союзников (или потенциальных союзников) и внутреннего раздробления с подрывом общей веры и общих взглядов;
    - в ментальной сфере: деформация и искажение восприятия противником реальности на основе дезинформации и создания неправильных представлений о ситуации;
    - в физической сфере: разрушение физических ресурсов противника (вооружения, живой силы, инфраструктуры и др.).
7. Любой элемент цикла OODA, в свою очередь, может быть декомпозирован на более мелкие элементы и представлен в виде внутреннего цикла OODA.
8. В цикле деятельности OODA, в ряде случаев, целесообразно выделить две фазы:
    - подготовку плана (building the plan), объединяющую этапы наблюдения и ориентации (OO);
    - реализацию плана (implementing of the plan), объединяющую этапы решения и действия (DA).

Необходимость введения 8-го постулата обусловлена применением цикла OODA для развития и практической реализации концепции сетецентрической войны. В условиях сетецентрической организации увеличение числа узлов сети (абонентов) и числа связей между ними оказывает различное влияние на повышение эффективности на этапах подготовки плана (OO) и реализации плана (DA) [290].

В соответствии с принципами сетецентрической войны компьютерные системы связывают элементы боевой техники в сеть. Это обеспечивает увеличение темпа действий OODA-цикла за счет сокращения продолжительности этапов наблюдения и ориентации. Эффективность образуемой на основе установления связей «системы систем» (systems of system) определяется также фазами принятия решений и действий [290].

В наиболее общем случае образование сетевых структур направлено на сокращение времени цикла боя и повышение темпа бо-

евых действий на всех уровнях военной организации. Из четырех этапов OODA-цикла три непосредственно связаны с обработкой информации и с компьютерными технологиями. Четвертый этап Action носит, в целом, кинематический характер и связан с перемещением в пространстве, защитой и поражением противника на основе огневой мощи [290].

Чтобы сохранить временные рамки OODA-цикла действий своих сил и обеспечить более высокий, чем у противника, темп боя, необходимо ускорить все четыре этапа цикла, реализуемые войсками (силами). В течение двадцатого века все усилия военных, ученых и инженеров были направлены на совершенствование вооружения и технологий в кинематической части петли OODA. Результатом этих усилий являлось увеличение мобильности, точности и огневой мощи вооружения [290].

Однако на современном этапе наступил технологический предел кинематической части OODA-цикла – более мощные виды оружия наносят неприемлемый сопутствующий ущерб, а более скоростные и более защищенные платформы вооружения и средства доставки поражающего фактора к цели предполагают непомерные на современном этапе материальные затраты. Пока это имеет место в случае гиперзвуковых самолетов и оружия на новых физических принципах [290].

Первые три шага OODA-цикла связаны непосредственно с процессами сбора информации, ее распределения, осмысления, анализа и принятия решений на основе полученной информации. Чем быстрее осуществляются сбор, распределение, анализ и восприятие информации, тем быстрее принимается решение. Именно скорость и правильность принятия решений наиболее важны в реальных боевых действиях. Таким образом, организация сети является механизмом ускорения этапов наблюдения и ориентации, а также повышения эффективности для этапа принятия решений [290].

Эффективность сетевых структур подтверждена математическим законом Роберта Меткалфа (Robert Metcalfe) (рис. 2.11), в соответствии с которым полезность и эффективность сети пропорциональна квадрату числа ее узлов. Этот закон, перенесенный из области вебторговли в военную сферу, дает своеобразную максимально возможную оценку эффективности системы датчиков, расположенных на платформах образцов ВВТ, в предположении, что датчики обеспечивают своевременную и достоверную информацию [290].

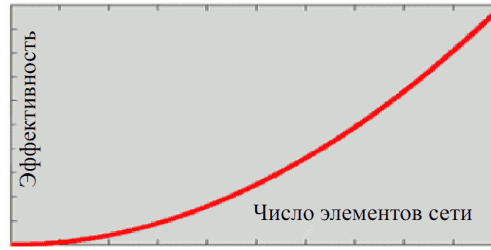


Рис. 2.11. График, иллюстрирующий
закон Р. Меткалфа [290]

Основное ограничение на эффективность в условиях сетецентрической структуры накладывают этапы принятия решений и действий. Математической моделью, наиболее близко описывающей эти процессы, является закон Амдала (Amdahl) (рис. 2.12), также перенесенный в сферу сетецентрических войн из области моделирования параллельных процессов в суперкомпьютерах. В исходном виде закон Амдала гласит: «увеличение числа ресурсов в системе обеспечивает увеличение суммарной производительности до максимума только в случае ресурсов, допускающих суммирование». Реальное увеличение ограничивается «эффектом очередей», обусловленным необходимостью строгого выстраивания и позиционирования ресурсов в процессе выполняемых действий [290].

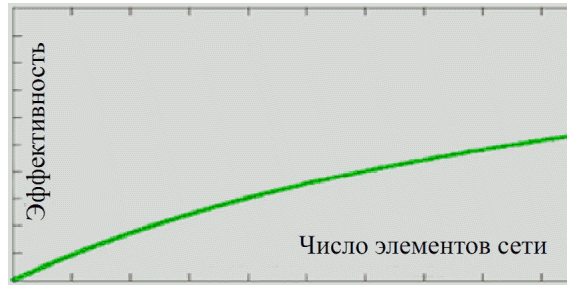


Рис. 2.12. График, иллюстрирующий
закон Амдала [290]

С методической точки зрения идеология определения нижней границы повышения эффективности военной деятельности в сетецентрической организации достаточно проста: введение сети обеспечивает существенное увеличение темпа действий до предела, связанного с информацией планирования (или прицеливания), однако это не оказы-

вает абсолютного влияния на способность и скорость доставки поражающего фактора оружия к цели. Эффективность этапа действия (исполнения плана) зависит только от возможностей платформ оружия и их количества [290].

Результаты представленных рассуждений и направления совершенствования технологий, обеспечивающих эффект сетецентричности, наглядно представлены на рис. 2.13.

Суммарно положения теории Дж. Бойда, а также некоторые перспективные направления ее развития и применения представлены на рис. 2.14.

В настоящее время петля OODA превратилась в стандарт описания цикла принятия решений во многих областях знания. Цикл OODA вошел в военные доктринальные документы министерств обороны США, Великобритании и Австралии, а идеи Джона Бойда о необходимости перманентного опережения противника во всех сферах ведения противоборства легли в основу концепции сетецентрической войны.

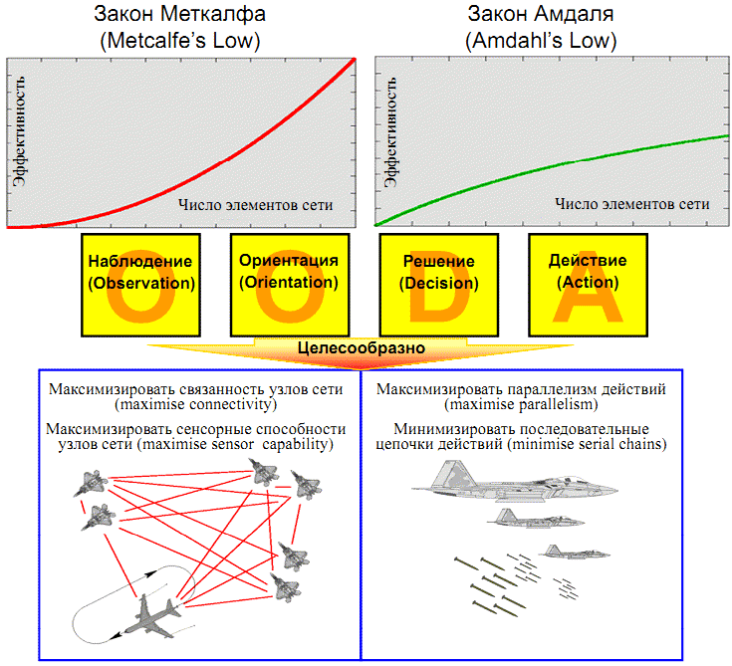


Рис. 2.13. Связь цикла OODA с законами сетецентрической войны [290]

Рис. 2.14. Постулаты теории Дж. Бойда и основные направления ее развития и применения [290]

2.4.4. Особенности сетецентрической войны

Термин «сетецентризм» впервые появился в американской компьютерной литературе как термин для объединения отдельных электронных вычислительных машин в единую сеть. Позднее идея сетецентризма была взята на вооружение специалистами вооруженных сил США.

Принцип сетецентрического управления был позаимствован из сферы бизнеса, в частности, из организации предпринимательской деятельности компании розничной торговли Walmart. Авторы концепции сетецентрической войны рассматривали эту компанию как самосинхронизирующуюся, саморегулируемую, рассредоточенную сеть магазинов, располагающую сведениями о происходящем движении товаров и торговых операциях в реальном масштабе времени. При этом управление движением товаров в компании осуществлялось по горизонтальной информационной сети, а не по вертикальной системе управления, в целом, система Walmart включает три составляющие: инфраструктурную, сенсорную и операционную. Две первые играют

ключевую роль в гарантированной ситуационной осведомленности и обеспечении превосходства в сфере торговли [95].

Таким образом, сетецентрическое управление предусматривает, прежде всего, изменение принципов управления и циркуляции информации и основывается на заимствовании перспективных принципов организации экономических процессов в ведущих корпорациях (таб. 2.3).

Таблица 2.3. Заимствование перспективных принципов организации экономических процессов и перенос их в военное дело [81]

Главные факторы	**Реализация в экономике**	**Реализация в военном деле**
Фактор производства (главный ресурс)	Информация, знание	Знание, развединформация о противнике, местности, климатических, гидрометеорологических условиях и т.п., о возможностях и расположении своих войск и т.п. Обеспечение информационного превосходства над противником
Важность нематериальных ресурсов	Ценность бизнес-организации определяется способностью создавать, приобретать, распределять и применять знания	Эффективность применения войск определяется способностью добывать, доводить до войск и правильно использовать информацию, интеллектуализацией ВВТ
Уход от массовости	Автоматизация производства, способность обеспечить индивидуализацию создания изделий с учетом уникальности ситуаций и требований	Точечность и дозированность применения средств поражения по ключевым элементам инфраструктуры и боевых порядков противника, гибкость применения ВВТ за счет ее интеллектуализации
Труд	Высококвалифицированный персонал, специализация, резкое падение взаимозаменяемости работников	Обученность военнослужащих, профессионализация армии
Инновации	Интенсификация применения новых идей, изделий, технологий, процессов и т.д.	Быстрая сменяемость поколений вооружений на основе интенсивного внедрения информационных технологий и оружия на новых физических принципах

Главные факторы	Реализация в экономике	Реализация в военном деле
Масштаб	Сокращение рабочих коллективов, распределенные системы производства, переход на принцип «коллектив под проект», виртуальный офис, миниатюризация изделий	Уход от массовых армий, сокращение расчетов, подразделений при сохранении эффективности систем оружия, повышение индивидуальных возможностей солдата, создание разнородных воинских формирований под конкретную задачу», миниатюризация средств вооруженной борьбы
Организация	Иерархические структуры уступают место сетевым, обладающим гибкостью и лишенным бюрократической надстройки	Сетецентрические принципы управления войсками
Системная интеграция	Увязывание, синхронизация действий множества источников ресурсов, потребителей и процессов производства	Оптимизация и синхронизация (на основе автоматизации) боевого применения разнородных группировок войск, их технического и тылового обеспечения
Инфраструктура	Высокоскоростные глобальные электронные информационные сети, единое унифицированное информационное пространство предприятия	Быстро сопрягаемые высокоскоростные электронные информационные сети, единое информационное пространство ТВД
Ускорение	Экономика масштаба сменяется экономикой скорости, работа в реальном масштабе времени	Превосходство над противником в скорости реализации цикла «разведка – принятие решения – управление – поражение», обеспечение действий в реальном масштабе времени

Сетецентрическая война – новая концепция ведения войн, первоначально разработанная под управлением вице-адмирала А.К. Сибровски (A.K. Cebrowski) и принятая на вооружение военным руководством США. Переосмысление военной стратегии привело к появлению в США концепции постиндустриальных или сетецентрических войн. А.К. Сибровски обобщил системное изложение основ сетецентрической войны. Идейным вдохновителем и влиятельным покровителем этого направления модернизации классической военной стратегии стал министр обороны США Д. Рамсфельд (D. Rumsfeld) [47, 127 , 129, 149, 152, 153].

Сами авторы концепции сетецентрической войны отмечают, что она является не революцией в военном деле, которая изменяет сущность войны, а скорее новый фактором, который мог бы позволить

государственному и военному аппарату осуществлять более эффективное управление силами и средствами при условии, что военная доктрина и вооруженные силы выстроены в соответствии с оценкой угрозы. Анализ концепции сетецентрической войны на основе работ [2, 29, 53, 112, 148, 329, 330, 331, 332, 333] показывает, что ее основная идея лежит не в новых формах и способах ведения боевых действий, а в изменении принципов управления войсками и оружием. Точнее говоря, это новый способ организации управления как реальный инструмент повышения боевых возможностей разнородных сил и средств за счет синергетического эффекта.

Концепция сетецентрической войны – это теория качественного сдвига в военных технологиях управления. Сетецентрическая война, в отличие от войн предшествующего периода, ведется не государствами и даже не блоками, а глобальными структурами, которые могут быть как институционализированы тем или иным образом, так и иметь подрывной террористический характер. В стремительно глобализирующемся мире вся социально-экономическая, политическая и культурная структуры пронизываются информационными каналами, которые составляют сети сетецентрической системы [148, 149].

При иерархической системе управления в ходе взаимодействия между двумя одноранговыми элементами в работу включается вся иерархическая цепочка, вплоть до общего для обоих элементов лица, принимающего решение.

Сетевая организация допускает непосредственное взаимодействие двух одноранговых элементов. В этом случае, согласно закону Меткалфа [16], потенциальная эффективность сети линейно увеличивается с ростом числа ее элементов и экспоненциально – с ростом числа связей между ними (пропорционально квадрату их числа). Однако при внедрении сетевой системы управления иерархическая структура не упраздняется, а добавляются новые связи между одноранговыми элементами. Эти связи призваны повысить скорость циркуляции информации внутри системы, но не заменить собой существующую иерархическую систему управления. Ускорение циркуляции информации в результате внедрения информационных технологий создало предпосылки для организации управления более сложными структурами, включающими в себя элементы, как классических иерархий, так и сетей. Введение в организационную структуру сетевых элементов позволяет усилить взаимодействие между отдельными ее звеньями, сделать их информационно насыщенными. Ранее это было невозможно, поскольку сложность и запутанность таких организационных

структур могли только замедлить, а то и вовсе парализовать процесс управления [16].

Существующий подход к структурному построению вооруженных сил, в основном, основывается на использовании жестких иерархических структур в звеньях ниже штабов отдельных видов и родов войск. В такой иерархической структуре отдельные и, в основном автономные звенья объединены в жестко подчиненную структуру в интересах выполнения отдельной боевой задачи. Такой принцип комплексирования имеет тенденцию создавать формальные и бюрократические барьеры для прохождения информации по всем подразделениям объединенных сил при выполнении боевой задачи. В иерархических системах управления зачастую используются штатные или системно-зависимые компоненты системы управления вооружением и обороной (СУВО), которые генерируют данные на основе независимых стратегий обработки информации в интересах информационного обеспечения конкретного вида или рода войск. СУВО, построенные по иерархическому принципу, как правило, не имеют горизонтальной интеграции с другими системами. Информационная интеграция осуществляется в централизованном командном пункте, организующем высшие уровни управления. Результатом является то, что иерархические системы СУВО не обеспечивают горизонтальных полноценных связей, что уменьшает потенциальную боевую эффективность объединенных сил. Таким СУВО свойственны «узкие» механизмы координации действий объединенных сил, а содержание, скорость доставки, форматы и качество информации, в основном, определяются процессами выполнения формальных требований управления. Такой подход создает ряд неизбежных социальных и технических барьеров беспрепятственному распределению информационных потоков, которые препятствуют интеграции боевых возможностей на тактическом уровне и, в конечном итоге, снижают общую эффективность действий объединенных сил. Предполагается, что если компоненты объединенных сил будут интегрированы в единое информационное пространство и будут полностью использовать доступные информационные ресурсы, то боевые возможности, которые появятся в результате этого, значительно повысят боевую эффективность применения вооруженных сил [112].

Современные достижения в области информационных технологий существенным образом повышают возможности всех компонентов вооруженных сил по обмену информацией. Это ведет к появлению новых принципов ведения боевых действий и, в целом, к повышению

боевой эффективности вооруженных сил. При этом под взаимодействием понимаются совместная выработка единого замысла, принятие решения или разработка каких-либо других материалов для решения боевых задач. Такое взаимодействие позволяет командирам транслировать собственное понимание и видение вариантов решения задач собственным подчиненным для более качественного их уяснения; оценивать возможные варианты действий; вырабатывать критерии оценки; принимать решения о своих дальнейших действиях и реализовывать принятые решения. Таким образом, в рамках сетевой концепции взаимодействие направлено на повышение качества информационного обмена, осведомленности и взаимопонимания между всеми командирами объединенных сил в интересах поддержки принятия решений и координации боевых действий [112].

Переход от иерархической структуры управления к сетевой требует преодоления внутренних и внешних организационных и технических барьеров, стоящих на пути повышения качества информационного обмена и синергического применения боевых возможностей вооруженных сил. Такое изменение должно быть поддержано гарантией того, что компоненты вооруженных сил будут иметь технические возможности по использованию информационных сетей независимо от их географической или организационной принадлежности. Таким образом, необходимость обеспечения гибкости действий вооруженных сил требует формирования новых принципов сетевого взаимодействия их компонентов, а также возможностей устанавливать и использовать горизонтальные связи с взаимодействующими силами при выполнении боевой задачи [112].

Концепция объединенной функциональной сетецентрической среды – NCE JFC (Net-Centric Environment Joint Functional Concept) описывает возможности, вытекающие из использования единого информационного пространства и технической совместимости всех компонентов вооруженных сил с целью повышения эффективности боевых действий [112].

Концепция сетецентрической среды основана на информационном превосходстве в области принятия решений и описывает возможные способы и методы действий объединенных сил в информационно-сетевой среде в ближайшие 10-20 лет. В рамках этой концепции включение в сеть всех компонентов объединенных сил создает возможность для беспрецедентного совместного использования информации при взаимодействии, введения адаптивных организационных структур и повышения степени единства действий путем синхрониза-

ции и интеграции компонентов сил, в том числе и на самых низших уровнях. В данной концепции термины «сеть» и «сетевой» используются как синонимы понятия «сетецентричности» [112].

Концепция объединенной функциональной сетецентрической среды предполагает [112]:

- формализацию сетецентрической среды и описание порядка действий будущих ВС в такой среде;
- выявление и описание сетецентрических принципов, возможностей и атрибутов, а также функциональный контекст для развития концепции совместных операций (JOC – Joint Operating Concept) и концепции совместной интеграции (JIC – Joint Integrating Concept);
- создание единых рамок оценки совместных инициатив для обеспечения системы интеграции и развития совместных возможностей (JCIDS – Joint Capabilities Integration and Development System);
- наличие возможности проведения военных экспериментов и учений.

Сетецентрическая среда – это область, включающая человеческие и технические ресурсы, а также технологии, обеспечивающие эффективное их взаимодействие, функционирующая в интересах исполнителей, обеспечивающая пользователей необходимой им информацией в понятной им форме и с заданной достоверностью. Эта же среда обеспечивает свойства информационной безопасности (конфиденциальности, целостности, доступности) в условиях функционирования средств несанкционированного доступа и воздействия противника [112].

Сетецентрические операции – использование человеческих и технических возможностей в сетевой среде, охватывающее все элементы вооруженных сил, обеспечивающие информацией об интегральных возможностях, осведомленности, знаниях, опыте для принятия решений с целью достижения высокого уровня гибкости и эффективности ведения боевых действий в условиях, характеризующихся инвариантностью, децентрализованностью, динамизмом и непредсказуемостью. Сетецентрические операции также можно определить как военные операции, проводимые в рамках сетецентрической среды [112].

Сетецентрические возможности являются эффектом от взаимодействия лиц, принимающих решения, и боевых подразделений в едином информационном пространстве, созданном на основе инфор-

мационных технологий. Повышение эффективности боевых действий будет достигаться за счет эволюционного развития таких составляющих, как [112]:

- военная доктрина;
- организационная структура войск;
- подготовка к боевым действиям;
- материальное обеспечение;
- военное управление;
- военное образование;
- личный состав и различные вспомогательные средства, которые должны быть соответствующим образом подготовлены для применения в сетецентрической среде.

В конечном итоге вооруженные силы смогут получать и использовать информацию более высокого энтропийного уровня в процессе принятия решений, а также использовать свои боевые возможности для решения поставленных задач более эффективно, целенаправленно и гибко. Это позволит вооруженным силам и союзникам при выполнении задач действовать более эффективно (быстрее и качественнее). Важно, что эти новые возможности позволят применять вооруженные силы принципиально новым образом за счет интеграции действий боевых подразделений на более низких уровнях управления [112].

Новая теория активно внедряется в практику ведения боевых действий США и уже была успешно обкатана в Ираке, Афганистане и других государствах, а сетецентрические технологические подходы тестируются на учениях и обыгрываются на симуляторах. Разработчики этой теории убеждены, что в ближайшем будущем она «если не заменит собой традиционную теорию войны, то существенно и необратимо качественно изменит ее» [149, 152, 153].

Основная задача концепции сетецентрической войны – предложить военному руководству теоретическую и оперативную базу для организации противодействия в условиях новых угроз за счет объединения в единую информационную сеть всех участников боевых действий [2, 29].

2.4.5. Основные принципы военного искусства в сетецентрической войне

Большенство традиционных принципов военного искусства сохраняют свою актуальность в концепции сетецентрической войны.

Однако за счет использования сетецентрической среды на первое место выходят новые принципы, характерные для этой новой концепции. Анализ работ [2, 29, 112, 149, 154, 155, 157, 159, 160, 161] позволил сформулировать эти основные принципы сетецентрической войны, приведенные на рис. 2.15 и подробно рассматриваемые ниже.

Рис. 2.15. Основные принципы сетецентрической войны и сетецентрических военных операций

Опора на превосходящие знания. Владение самыми современными технологиями, основанными на последних достижениях научно-технического прогресса, позволит изменить стратегию и тактику боевых действий. Быстродействие сложных информационных систем обеспечит возможность моделировать действия врага, учет собственного потенциала, факторов окружающей среды и ТВД. Улучшенное ситуативное планирование на основе такого моделирования позволит достичь превосходства в оперативности и качестве принимаемых решений, а также в несколько раз увеличить темп, связанность и эффективность боевых действий. Считается, что чем больше известно о противнике, окружающей среде и о самом себе, тем более эффективно можно использовать собственные возможности для достижения желаемых результатов [2, 29].

Основой ведения сетевых войн является проведение операций, базирующихся на эффектах. Это важнейший принцип в данной теории.

Операции, базирующиеся на эффектах (EBO – Effect Based Operations) – *совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуациях мира, кризиса и войны* [149, 154].

Эффект – физический, функциональный или психологический результат, событие или последствие, которое следует за единичным действием или совокупностью действий. Действия на основе эффектов разработаны с целью объединить и учесть во всем боевом пространстве причинно-следственные связи от высокоточных ударов, маневров силами и средствами, а также информационных операций с целью вызвать изменения в поведении противника [2, 29].

Иными словами, операции, базирующихся на эффектах, – это такое качественное влияние на среду, при котором управление участниками среды осуществляется не напрямую, а косвенно, за счет навязывания определенных моделей поведения, предусмотренных более глобальной моделью управления. Развитие методического аппарата такого влияния означает заведомое установление контроля над всеми участниками актуальных или возможных боевых действий и манипулирование ими в складывающихся ситуациях: в угрожаемый период, в процессе войны и в условиях стабилизации обстановки после победы. Такая сетевая война постоянна, и ее цель – обеспечить тем, кто ее ведет, способность всестороннего управления всеми действующими силами.

Информационное превосходство – способность собирать, обрабатывать и распределять непрерывный поток информации различного характера, препятствуя противнику делать то же самое [270].

Информационное превосходство также может быть определено и через показатели динамики обработки информации.

Информационное превосходство – способность обеспечивать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать на всем протяжении ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях [270].

Информационное превосходство реализуется через:

- искусственное увеличение потребности противника в информационном обеспечении, а также одновременное снижение доступности его собственных информационных ресурсов и информационных каналов поступления ему разведывательных данных;
- обеспечение широкого доступа к собственным информационным ресурсам через сетевые механизмы с одновременной защитой их от воздействия противника;
- организацию информационного обеспечения собственных сил и средств за счет предоставления доступа к широкопо-

лосным каналам оперативного и динамичного информирования о складывающейся обстановке.

Всеобщая осведомленность включает в себя:

- построение интегральной информационной сети, постоянно обновляемой через сырые и уже обработанные данные, поставляемые разведкой и иными информационными каналами;
- превращение абонентов информационного обмена в поставщиков информации, способных при необходимости незамедлительно активировать обратную информационную связь;
- обеспечение информационной безопасности интегральной информационной сети от воздействий противника одновременно с максимальной доступностью этой сети для подавляющего числа своих пользователей.

Намерение командира. В сетецентрических войнах понятие намерение командира (англ. commander's intent) призвано заменить собой традиционную форму приказа. Приказ является крайне формализированной версией решения командира на ведение боевых действий. Исполнение формального приказа существенно ограничивает свободу действий и тех, кто его отдает, и тех, кто его исполняет. После отдачи/получения приказа цепочку действий можно остановить только другим столь же формальным приказом, что часто в условиях ведения динамичных боевых действий оказывается проблематичным. Задача расширения формальных рамок приказа в сетевых войнах решается с помощью намерения командира. Методичное выстраивание контактов командиров с подчиненными позволяет командиру избежать строгой и однозначной формализации управления с помощью приказов, передавая исполнителям свое общее представление о задаче и предполагаемых результатах ее выполнения, предоставляя подчиненным возможность самим искать пути для ее наиболее эффективного решения в зависимости от конкретной обстановки.

Снижение длительности цикла управления (букв. «скорости командования»). Длительность циклов управления на всех уровнях должна быть снижена, что позволит:

- повысить скорость принятия решений и их передачи за счет адаптации к условиям боя, переводя это качество в конкретное оперативное преимущество;

- в ускоренном темпе противодействовать реализации решений противника и обеспечить заведомое превосходство над ним по показателю своевременности принятия решений.

Основной эффект от снижения цикла управления заключается в том, что если одна из противоборствующих сторон выполняет приказ быстрее, то она лучше и результативнее выполняет и общую поставленную задачу, а в результате – получает стратегическое преимущество в опережении реакции противника.

Самосинхронизация (англ. self-synchronization) призвана обеспечить возможность базовых боевых подразделений действовать практически в автономном режиме, самим формулировать и решать оперативные задачи на основе принципов «всеобщей осведомленности» и «намерения командира». Для этого следует:

- усилить значение инициативы командиров базовых боевых подразделений для повышения общей скорости ведения операции;
- соучаствовать в реализации вышестоящего «намерения командира», которое отличается от формального приказа и представляет собой осознание командиров базовых боевых подразделений финального замысла операции, ее целей и задач;
- быстро адаптироваться к важным изменениям на ТВД и устранить логику пошагово-иерархического принятия решений, а также проведения операций в соответствии с традиционной военной стратегией.

Самосинхронизация означает, что базовое боевое подразделение само формулирует и решает тактические боевые задачи на основе всеобщей осведомленности. Каждый боевой элемент, действующий в рамках сетецентрической войны, способен самостоятельно поставить себе цель в соответствии со складывающейся текущей обстановкой, конечными целями операции, а также в зависимости от своего местоположения и порядка взаимодействия с другими элементами сети.

Распределенные силы. Данный принцип формулирует задачу перераспределения сил и средств от четких боевых порядков на поле боевых действий к ведению точечных операций. Для этого следует:

- перейти от формы физического занятия обширного пространства к функциональному контролю над наиболее важными стратегически элементами;
- перейти к нелинейным действиям во времени и пространстве с целью обеспечения возможности в нужный момент

сосредоточить необходимое количество сил и средств в конкретном месте;

- усилить тесное взаимодействие разведки, оперативно-тактического и стратегического командования для реализации и обеспечения точных эффектов во времени и пространстве с помощью рассеянных сил.

Основной упор в данном случае делается на свойство распределенности – как на переход от линейной конфигурации (развертывание фронта) к ведению точечных операций, что на практике означает использование тактики партизанской войны, но в стратегическом масштабе. Наступать не фронтом, а мелкими бригадами, синхронизированными между собой. Все это создает предпосылки к снижению значения массированности сил и средств и к существенному росту важности логистики боевых подразделений. При этом под логистикой понимается способность в сжатые сроки нарастить силы и средства в заданное время и в заданном месте, провести слаженную боевую операцию и, достигнув необходимого эффекта, «распределить» подразделения в интересах следующих операций.

Демассификация. Данный принцип является логичным следствием принципа «распределения сил» и предполагает:

- использование превосходства для достижения желаемых эффектов и ограничивает необходимость сосредоточения крупных сил и средств в конкретном месте;
- навязывание противнику слишком высокого для него темпа боевых действий за счет увеличения скорости перемещения своих боевых подразделений, а также сил и средств обеспечения на поле боя.

Глобальное разведывательное обеспечение (букв. с англ. «глубокое сенсорное проникновение»). Этот принцип сетецентрической войны требует увеличения количества и повышения качества разведывательных датчиков и каналов получения информации, как в районе боевых действий, так и вне него. Глобальное разведывательное обеспечение реализуется за счет:

- объединения в единую базу данных сведений, получаемых системами разведки, наблюдения и распознавания;
- массированного использования в качестве разведывательных датчиков высокомобильных мультисенсорных технических средств (БПЛА, робототехнических комплексов, датчиков охраны периметра и др.);

- использования датчиков и точек наблюдения как инструмента морального воздействия на противника;
- снабжения каждого боевого средства (комплекса) от отдельного бойца до спутника разнообразными датчиками и информационными сенсорами.

Глобальное разведывательное обеспечение означает, что информация собирается от различных источников, при этом различные боевые единицы оснащены максимальным количеством средств наблюдения.

Изменение начальных условий ведения военных действий. Еще классическая военная стратегия обнаружила, что эффективность ведения войны во многом зависит от начальных условий. От того, в каком контексте, а также при каком балансе сил и средств начнется война, во многом зависит как будут протекать дальнейшие боевые действия. В этой связи, задача сетецентрических войн заключается в том, чтобы:

- заранее повлиять на начальные условия войны, заложить в них такую структуру, а также баланс сил, средств и принципов управления, которые заведомо приведут либо к победе, либо обеспечат подавляющее преимущество в ведении войны;
- спровоцировать сочетание во времени и в пространстве ряда событий, которые призваны повлиять на потенциального противника и блокировать его ответную инициативу.

Изменение стартовых условий ведения боевых действий близко к принципу «операций, базирующихся на эффектах». То, в каких конкретно условиях (геополитических, экономических, военных, социальных, демографических и др.) стороны начинают войну, на 90% определяет ту действительность, в которой они окажутся по результатам ведения своих боевых действий.

Сжатые операции. Сжатые или компрессионные операции – это такие операции, в которых преодолеваются структурные и процедурные разграничения между различными военными службами, а полный доступ к разнородной информации обеспечивается даже на низшем уровне управления боевых подразделений. Для этого:

- повышается скорость развертывания и применения сил, а также их тылового обеспечения;
- отменяется фрагментация процессов (организация, развертывание, использование, обеспечение и т.д.) и функцио-

нальных областей (боевых подразделений, разведки, службы тыла и т.д.);

- отменяются структурные разграничения при организации взаимодействия на нижних уровнях управления.

Таким образом, сжатые или компрессионные операции состоят в преодолении структурных процедурных ограничений между военными службами и полный их доступ к разнородной информации в интересах достижения цели проводимой операции.

Анализ вышеприведенных принципов позволяет сформировать основные направления трансформации принципов ведения войны, представленные в табл. 2.4 по информации из работы [80].

Таблица 2.4. Трансформация принципов ведения войны [80]

Принципы современной тактики		**Принципы тактики сетецентрических действий**	
Наименование	**Содержание принципа**	**Наименование**	**Содержание принципа**
Сосредоточение усилий на главном направлении (принцип массирования)	Достижение решающего превосходства над противником в силах и средствах во всех сферах: на земле, в воздухе, информационном пространстве	**Сетецентричность**	Уход от фронтального противоборства. Достижение сетецентрического эффекта путем концентрации усилий на избранном направлении в сочетании с одновременным рассредоточением сил и средств на других направлениях в целях активизации всего боевого пространства и введения противника в заблуждение. Применение «роевой тактики», «тактики стаи», «тактики муравейника», «тактики боевых групп»

Принципы современной тактики		Принципы тактики сетецентрических действий	
Наименование	**Содержание принципа**	**Наименование**	**Содержание принципа**
Сосредоточение усилий на главном направлении	Нанесение по противнику одновременных ударов с фронта, тыла и фланга, создание плотной группировки пехоты, танков, артиллерии на главном направлении	**Сетецентричность**	Переход в тактическом звене от огневого воздействия на противника к информационно-огневому и энергетическому. Увеличение глубины ближнего и дальнего боя. Трансформация факторов поля боя – скорости, времени, пространства, фронта и тыла, «цены успеха», «боевых и маневренных возможностей», соотношения сил и средств. Превалирование глубинного боя над ближним, неконтактных действий над контактными. Действия в длительном отрыве от своих войск, «с нечетким фронтом». Нацеленность действий войск на выявление и уничтожение «критических объектов» (пунктов управления и средств поражения)
Боевая активность	Действия, направленные на захват и удержание инициативы, нанесение максимального поражения противнику всеми имеющимися средствами и успешное выполнение боевых задач	**Асимметричность**	Противодействие противнику в захвате огневой и тактической инициативы, упреждение его в действиях по принципу «первым разведал – первым поразил». Применение по всей глубине расположения противника ВТО различной дальности, сопряжение действий средств поражения с системами разведывательно-информационного обеспечения; применение малых разведывательно-ударных БПЛА, наземных разведывательно-ударных комплексов, роботов. Опережение противника в циклах разведки, применение «сетевых» принципов управления оружием, применение энергетических ударов, оружия на новых физических принципах в сочетании с использованием оружия ближнего и дальнего боя с оптическими, лазерными и радиолокационными системами наведения на цель. Активность боевых действий во всех сферах – на земле, в воздухе и в информационном пространстве; Поддержка противника в постоянном напряжении

Принципы современной тактики		Принципы тактики сетецентрических действий	
Наименование	**Содержание принципа**	**Наименование**	**Содержание принципа**
Взаимодействие	Согласование действий войск по цели, задачам, месту, времени и способам выполнения задач для достижения победы в бою	**Единение боевых усилий в информационно-коммуникационном пространстве**	Объединение боевых усилий «ударного блока» (средств поражения) со «вспомогательным блоком» (средствами обеспечения) по правилу «все в одном». Согласование действий «боевых модулей» (автономных боевых групп) для достижения общей цели через единое информационное поле боя, позволяющее поднять взаимодействие на качественно новый уровень, повысить степень согласованности и целенаправленность действий общевойсковых подразделений и частей со средствами поддержки Модель сетецентрического взаимодействия заключается во взаимоувязке элементов сети (частей и соединений) с управляющим блоком, командно-штабным центром и блоком обеспечения (разведкой, РЭБ, РХБЗ, инженерным обеспечением)
Маневр	Маневр – организованное перемещение войск в целях создания необходимой группировки сил и средств, занятие выгодного положения по отношению к противнику, вывода войск из-под ударов	**Ударно-огневой маневр**	Ударно-огневой маневр основывается на триаде: превентивность, мобильность, внезапность. Цели маневра: концентрация и перераспределение усилий ударно-огневых средств с одного направления (объекта) на другое; эффективное использование результатов огневого поражения; своевременное сосредоточение, наращивание и перенос усилий; распределение ударов и огня для одновременного или последовательного захвата (поражения) одного или нескольких объектов в тактической глубине. Маневр поражением, средствами РЭБ, инженерными заграждениями. Противодействие маневру противника

Принципы современной тактики		Принципы тактики сетецентрических действий	
Наименование	**Содержание принципа**	**Наименование**	**Содержание принципа**
Внезапность	Неожиданные, непредвиденные действия по времени, месту, масштабам, составу и способам применения сил и средств с целью обмана противника и дезорганизации его действий	**Синергетический эффект («эффект шока»)**	Первоочередной вывод из строя «критических объектов». Достижение «энергетической внезапности» путем массового ввода в действие ранее неизвестных противнику видов оружия; неожиданное для противника создание зон энергетического поражения в уязвимых для него местах. Применение новых способов боевых действий – нанесение «обезоруживающего», «мгновенного», «нарастающего» удара. Массированная роботизированная атака (ввод в действие информационно-управляемых роботов)
Защита	Система мероприятий, проводимых с целью не допустить или максимально ослабить воздействие оружия противника, сохранить боеспособность и обеспечить выполнение боевой задачи. Защита достигается устойчивым управлением, своевременным рассосредоточением сил и средств, использованием защитных свойств местности и ее фортификационным оборудованием, своевременным восстановлением боеспособности войск	**Структурная защита**	Активно-упреждающий характер, ориентир на защиту не только от существующих, но и от перспективных видов оружия; комплексность защиты (сочетание тактических, технических и специальных мероприятий, направленных на противодействие радиоэлектронным, энергетическим ударам и информационно-психологическому воздействию противника). Блоки структурной защиты: разведывательно-информационный; инженерно-технический; войсковой

Принципы современной тактики		Принципы тактики сетецентрических действий	
Наименование	**Содержание принципа**	**Наименование**	**Содержание принципа**
Управление войсками	Целенаправленная деятельность командиров, штабов по поддержанию боевой готовности частей и подразделений по подготовке их к бою и руководству ими при выполнении боевой задачи. Управленческий фактор приравнивается по своей значимости в достижении успеха к материальному фактору (количеству и качеству войск и вооружения)	**Интеграционное управление войсками и оружием**	Переход от иерархической системы управления к более гибкой модели управления разновидовыми тактическими группами в едином информационном поле. Смена алгоритма работы командира и штаба, переход от последовательного метода планирования к параллельному за счет автоматизации обработки информации. Формирование единой цифровой карты оперативной обстановки, позволяющей повысить качество восприятия обстановки на поле боя, а также создания информационно-управляющей сети, где тесно связаны между собой органы управления и объекты управления. Ввод в действие систем «человек – оператор», «человек – машина»

2.5. Сетецентрическая среда как ключевой элемент концепции сетецентрической войны

Сетецентрическая среда – это область, включающая в себя человеческие и технические ресурсы, а также технологии эффективного их взаимодействия, функционирующая в интересах участников выполнения боевых задач, обеспечивающая пользователей необходимой им информацией в понятной им форме и с заданной достоверностью. Эта же среда обеспечивает выполнение требований информационной безопасности (конфиденциальности, целостности, доступности) от средств несанкционированного доступа и воздействия противника [112].

2.5.1. Области сетецентрической среды

Сетецентрическая среда, оперирующая возможностями и условиями (атрибутами), может рассматриваться в виде модели, состоящей из двух областей (рис. 2.16) [112].

1. Области знаний.
2. Технической области.

Область знаний включает в себя [112, 149]:

- когнитивную область;
- социальную область.

Техническая область включает в себя [112, 149]:

- физическую область;
- информационную среду.

Рис. 2.16. Сетецентрическая среда [112, 149]

Каждая из областей имеет важное самостоятельное значение, но решающий эффект в сетецентрических войнах достигается синергией (однонаправленным действием) всех этих элементов. При этом ни одна из этих составных частей сетецентрической среды возможностей не может существовать изолированно, так как существуют зависимости между областями, между возможностями внутри самих обла-

стей и возможностями в рамках областей. Общие возможности в рамках сетецентрической среды шире, чем просто сумма возможностей области знаний и технической области. Эти две области интегрированы между собой для более полного использования их эмерджентного потенциала [112].

Рассмотрим данные области сетецентрической среды более подробно на основе анализа работ [112, 149].

Физическая область – это традиционная область войны, в которой происходит столкновение средств вооруженных сил во времени и в пространстве. Эта область включает в себя среды ведения боевых действий (море, суша, воздух, космическое пространство), средства (комплексы) вооружений и военной техники, а также физические средства информационно-вычислительных сетей. Эти элементы физической области лучше всего поддаются измерению и оценке, и ранее именно оценка средств физической области являлась основой при определении силы ВС и способности вести боевые действия. В эпоху сетевых войн следует рассматривать физическую область как некоторую предельную возможность использования сил и средств при применении сетевых технологий управления, основная часть которых расположена в других областях, но которые проецируют на средства физической области свои эффекты.

Информационная область – это сфера, где создается, добывается, обрабатывается и распределяется информация. Эта область покрывает системы передачи информации, базовые сенсоры (датчики), модели обработки информации и т.д. Это преимущественная среда эпохи сетевых войн, которая выделилась в самостоятельную категорию – инфосферу и, наряду с физическими средами, приобрела важнейшее, если не центральное значение. Информационная область в эпоху сетевых войн связывает между собой все уровни ведения войны и является приоритетной. При этом преимущества или недостатки в накоплении, передаче, обработке и охране информации приобретают постепенно решающее значение.

В инфосфере выигрываются или проигрываются современные войны. Если о той или иной операции не сообщили по телевидению, не дали репортаж в СМИ, то этой операции как бы не существует, она отсутствует в информационной картине дня, а значит, не учитывается [149].

Когнитивная область – это сознание бойца. Она является тем пространством, где преимущественно осуществляются операции, основанные на эффектах. Все основные войны и битвы развертываются

и выигрываются именно в этой сфере. Именно в когнитивной области располагаются такие явления, как намерение командира, доктрина, тактика, техника и процедуры. Сетецентрические войны придают этому фактору огромное значение, хотя процессы, происходящие в этой сфере, измерить значительно сложнее, чем в физической области. Но их ценность и эффективность подчас намного важнее.

Таким образом, чуть шире – когнитивная сфера – сфера сознания боевой единицы. В сетевых войнах понятие солдата или боевой единицы – это, прежде всего, интеллектуальная реальность. Когнитивная сфера или внедрение возможности мыслить, распространение разумных паттернов на различные сферы деятельности – важные элементы сетевой войны. Намерения командира являются той лакмусовой бумажкой, которая определяет степень когнитивности, т.е. то, в какой степени боец может расшифровать задачу командира, в такой степени он и является адекватным для ведения сетевых войн [149].

Социальная область – представляет собой поле взаимодействия людей. Здесь преобладают исторические, культурные, религиозные ценности, психологические установки и этнические особенности. В социальной области развертываются отношения между людьми, выстраиваются естественные иерархии в группах – лидеры, ведомые, пассивные массы и т.д., складываются системы групповых отношений. Социальная область является контекстом сетевых войн, который следует принимать во внимание самым тщательным образом.

Пересечение областей. Войны информационной эпохи основаны на сознательной интеграции всех четырех областей. Путем их избирательного наложения и создается сеть, которая лежит в основе ведения военных действий. Речь идет о том, что война в сетевом смысле выигрывается на четырех уровнях, из этого и складывается сетевое управление.

Сферы пересечения этих областей имеют принципиальное значение. Гармоничная настройка сети усиливает военный эффект от действий вооруженных сил, в то время как прямые действия, направленные против противника, хоть и расстраивают его ряды, но при этом разводят эти области между собой, исключая тем самым важнейший фактор превосходства [149].

Функционирование в сетецентрической среде в значительной степени зависит от наличия возможностей области знаний в сочетании с возможностями, достигнутыми в области техники. Ни одна из этих возможностей не может существовать в изоляции – существуют взаимозависимости между областями, между возможностями разных обла-

стей и между возможностями внутри одной области. Область знаний включает индивидуальные и коллективные возможности (например, понимание и принятие решений), появляющиеся в результате взаимодействия, вариантов организационных схем и распределения сил.

Сетецентрическая среда значительно расширит боевые возможности сил и средств за счет коллективного распределения и обработки информации. Процесс понимания обстановки становится распределенным процессом понимания обстановки, а процесс принятия решения становится коллективным. Возможности в технической области предоставляют средства для достижения большей эффективности в области знаний [112].

2.5.2. Принципы построения сетецентрической среды

Анализ доктринальных и уставных документов ведущих зарубежных стран показывает, что основой для реализации современной концепции сетецентрической войны является сеть. Более того, все сетецентрические концепции ведущих зарубежных стран строятся на возможности организации взаимодействия и объединения всех разрозненных боевых элементов в подсистемы, а затем и всех сформированных подсистем в единую структуру через сетецентрическую среду. Такая организация взаимодействия подразумевает не только объединение платформ, узлов, средств, линий связи в техническом смысле, но и организацию когнитивного взаимодействия между личным составом и органами управления [43].

Сетецентрическая среда значительно расширит боевые возможности сил и средств за счет коллективного распределения и обработки информации. Вместе с тем, создание эффективной сетецентрической среды основано на новых технологических принципах получения, передачи и обработки информации всеми участниками боевых действий. Ниже представлены основные из них.

Распределенная информационная инфраструктура включает в себя физические компоненты сетецентрической среды. Она делает возможным циркуляцию информации и тем самым позволяет организовать взаимодействие индивидуальных и коллективных пользователей сети. Инфраструктура должна иметь распределенную архитектуру, поддерживать организационные структуры, процессы и потоки информации, необходимые пользователям для взаимодействия в сетецентрической среде. В широком смысле, разработка, развертывание и

использование инфраструктуры должны осуществляться по следующим правилам [112]:

- адаптация к изменяющимся требованиям, приоритетам и воздействиям при передаче информации внутри инфраструктуры;
- связывание коллективных и индивидуальных пользователей в глобальную сеть, устранение барьеров, создаваемых географическими условиями (естественными и искусственно созданными), физическое перемещение своих компонентов.

Инфраструктура должна быть способной обеспечивать постоянную глобальную совместимость, но в то же время позволять пользователям сохранять необходимые им тактические и оперативные возможности в случае отключения от сети.

Инфраструктура должна обеспечивать следующий минимум функций [112]:

- локальное объединение абонентов в сети (peer-to-peer) даже при отсутствии внешнего подключения к глобальной сетецентрической среде;
- кэширование и репликацию информации;
- возможность ввода обновленной локальной информации в ручном и/или автоматизированном режиме с автоматической синхронизацией данных с данными, уже хранящимися в глобальной сетецентрической среде;
- синхронизацию данных при восстановлении подключения к сети;
- регулирование процесса подключения к сети и визуальную доступность данных на основе прав доступа пользователей;
- динамическое регулирование безопасности сети по мере изменения ролей ее участников и с учетом наличия преднамеренных воздействий на сетевую инфраструктуру со стороны противника;
- обеспечение автоматизированного управления информацией, ее обработку, использование средств вывода новых данных и их визуализацию.

Индивидуальное управление информацией. Достижения в области информационных технологий позволят инфраструктуре перемещать большие объемы высококачественной информации от источников информации к ее потребителям с большей скоростью. Главным преимуществом такой возможности является то, что требования к ин-

формации могут быть динамически определены ее потребителями. Таким образом, управление информацией перестает быть функцией системы управления и становится индивидуальной функцией участника боевых действий [112].

Развитие процессов принятия решений в СУВО подразумевает, что ЛПР, в случае необходимости должно уметь фильтровать, структурировать и визуально представлять информацию в понятном для него виде, без снижения качества и важности информации. Это позволит повысить скорость и качество принятия решений и обеспечит высокую ситуационную осведомленность и информационное превосходство над противником [112].

Для обеспечения индивидуального управления информацией необходимо использовать высокоскоростные средства обработки и анализа информации, средства формирования и обработки метаданных, а также средства формирования баз знаний на основе онтологий. Эти средства должны обеспечить функционирование интеллектуальных программ, отвечающих за доступ к информации тех пользователей, которым она необходима [112].

Бесшовный информационный обмен является одним из основных принципов сетецентрической среды и подразумевает открытость информации для всех компонентов объединенных сил в сетецентрической среде. Информация, генерируемая, обрабатываемая и используемая в сетецентрической среде, должна быть видимой, доступной, понятной, проверяемой, свежей и достоверной [112].

Доступ к информации и ее доступность для других пользователей будут регламентироваться уровнем их доступа, а также на основе задач, выполняемых отдельными и коллективными пользователями в составе объединенных сил. Доступ пользователей к информации должен предоставляться в соответствии с динамическим требованием «необходимо знать». Это позволяет закрыть важную информацию от тех пользователей, у которых есть доступ к информации, но нет «необходимости ее знать». Для обеспечения требований по регламентированию доступа к информации необходимо существенно развивать в целях обеспечения динамической ролевой безопасности такие технологии, как система ключей общего доступа и система биометрической идентификации [112].

Устранение барьеров на пути свободной циркуляции информации и обеспечение ее защиты требуют создания открытых информационных структур и процессов. Принцип бесшовного информационного обмена основан на переходе от информационной модели

«предоставлять информацию выборочно» к модели «закрывать информацию выборочно». Повышение уровня открытости информации для тех, кто ее потребляет, обрабатывает и создает, позволит территориально удаленным друг от друга индивидуальным и коллективным пользователям объединить их возможности для совместного решения задач [112].

Взаимозависимость – это форма действий, основывающаяся на более высокой степени взаимного доверия, в которой разные участники вносят свой вклад в достижение общих задач и полагаются друг на друга при использовании важных взаимных возможностей, не дублируя эти возможности своими силами [112].

В настоящее время интеграция объединенных сил, как правило, осуществляется на уровне их штабов и часто характеризуется автономностью и бесконфликтностью, характерными для самых низших уровней интеграции. В этом случае возможности каждого подразделения остаются полностью отделенными от других и даже если они пересекаются с возможностями всей организации, то это происходит на более высоком уровне управления. Поскольку подразделения редко используют сразу все возможности, имеющиеся в их распоряжении для решения поставленных перед ними задач, то значительная часть возможностей внутри объединенных сил остается незадействованной [112].

Устраняя барьеры на пути информационных потоков и соединяя географически удаленные компоненты объединенных сил, сетецентрическая среда предоставляет им возможность использовать преимущества специализации каждого компонента при выполнении боевой задачи. Подразделениям всех эшелонов объединенных сил уже не нужно будет обладать штатным набором одинаковых возможностей для выполнения своих боевых задач, поскольку они смогут получать гарантированный доступ к тем или иным необходимым им возможностям, которые имеются у других подразделений, организаций или отдельных специалистов. Специфические возможности, которые характеризуются невысокой степенью использования, могут находиться «в запасе» или предоставляться тем подразделениям, которым они крайне необходимы [112].

2.5.3. Функции сетецентрической среды

Сетецентрическая среда как информационная среда управления войсками и оружием должна обладать следующими функциональными возможностями.

Возможность формировать или генерировать информацию заключается в сборе данных и преобразовании этих данных в информацию. Она включает обработку данных как непосредственно в месте получения данных (на борту носителя разведывательных датчиков), так и/или передачу этих данных другим внешним средствам анализа и обработки [112].

Возможность хранить, распределять информацию, а также обмениваться ею. К данной функции относятся все действия, необходимые для накопления и распределения информации и данных, а также обмена ими. Данные должны быть соответствующим образом идентифицированы, снабжены метаописанием и помещены в базу данных или хранилище информации. О наличии этих данных должны быть оповещены те, кому они могут понадобиться, при помощи соответствующих средств. К таким средствам может относиться программный инструментарий, позволяющий пользователям самим находить данные или информацию и/или средства для своевременного предоставления данных или информации их потребителям (своевременное принудительное уведомление о поступлении данных или push-технологии). Используемые методы накопления (хранения) данных или информации должны максимально облегчать доступ наиболее заинтересованным в ней пользователям (технологии ступенчатого контента или интеллектуального хранения). Одновременная работа с данными и информацией должна быть обеспечена в многопользовательском режиме. Кроме того, должны быть предусмотрены функции обновления и архивирования данных и информации [112].

Возможность создавать информационную среду. Такая возможность подразумевает выработку критериев, процессов и порядков действий применительно к накоплению и распределению данных и информации, включая распределение их в самых различных условиях в интересах постоянной информационной поддержки многочисленных пользователей объединенных сил. Постоянно меняющаяся обстановка и высокие темпы ведения боевых действий потребуют от сетецентрической среды способности достигать быстрого распределения информационных ресурсов в соответствии с изменением приоритетов источников и потребителей информации, а также в соответствии с планами

командования (динамичное распределение информационных ресурсов на основе приоритетов) [112].

Возможность обрабатывать данные и информацию. Пользователь должен иметь возможность фильтровать, сопоставлять и синтезировать данные и информацию в приемлемых для него формах. Такая система обработки информации должна обладать способностью выполнять своего рода посредническую функцию и осуществлять трансляцию данных между различными системами с разными характеристиками [112].

Возможность использовать геопространственную информацию. Все навигационные координаты абонентов сетецентрической среды должны быть зарегистрированы и соотнесены с другой геопространственной информацией, используемой в базе данных информационного обеспечения боевых действий (например, по климату, населению, средствам и возможностям, транспорту, службам). Эта функция сетецентрической среды обладает гораздо более широкими возможностями, чем использование обычного топографического обеспечения, поскольку она позволяет осуществлять стратификацию информации (отображать ее по слоям или уровням) и отрабатывать ее использование в учебно-тренировочных целях [112].

Возможность использовать информацию. Наличие информации в сети будет бесполезным без средств предоставления ее пользователям в удобной для них форме. Форматирование информации должно обеспечивать ее трансляцию или подразумевать использование различных интерфейсов в степени, достаточной для обмена информацией между различными системами [112].

Возможность находить и потреблять информацию. Пользователи должны иметь возможность находить требуемую информацию и выбирать ее. Эту способность обеспечивают различные средства поиска информации, в том числе за счет использования поисковых программ-агентов, средств выбора информации по технологии pull/push [112].

Возможность обеспечить пользователям безопасный доступ к информации. Сетецентрическая модель боевых действий может привести к изменению функций и ролей пользователей в соответствии с требованиями по выполнению задачи. Такое изменение потребует доступа к новой информации и соответственно выполнения новых требований по обеспечению безопасности такого доступа. Поэтому необходимо разработать и внедрить механизмы контроля «ролевого» доступа к информации отдельных пользователей и коллективного

доступа для заинтересованных сообществ. В таких механизмах контроля должны быть реализованы жесткие процедуры идентификации пользователей. Кроме того, должен быть реализован принцип многоуровневой безопасности с тем, чтобы обеспечить распределение информации между пользователями, имеющими разные уровни доступа к информации.

Возможность обеспечивать достоверность информации и доверие ее источнику. Данная функция должна удовлетворять потребности пользователей в достоверной информации. Для этого необходимо использовать технологии восстановления сетей, систем и данных, а также технологии гарантированной доступности данных, технологии обеспечения их целостности, достоверности и обновления на всем протяжении жизненного цикла этих данных.

Возможность устанавливать и развертывать сети. В целом сетецентрическая модель боевых действий зависит от возможности подключения к сетецентрической среде там и тогда, где и когда это необходимо. Сетецентрическая среда должна иметь возможность быстро развертываться в районах боевых действий с учетом требований, предъявляемых к выполнению конкретной боевой задачи. Она должна также быть способной динамически менять свою конфигурацию по мере изменения боевых задач, а также функционировать в жестких и/или не имеющих соответствующей инфраструктуры средах [112].

Возможность функционировать и управлять доступом. Развернутая сетецентрическая среда должна обладать способностью динамически распределять информационные ресурсы, функционировать независимо от географических условий (больших расстояний, условий местности и т.д.), осуществлять информационную поддержку всех проводимых операций на всех уровнях управления, в том числе в подготовительный период. Она должна управлять доступом к сетевым информационным ресурсам, обеспечивая в то же время изначальное подключение к ним различных элементов объединенных сил. Сетецентрическая среда должна также обеспечивать непрерывную, быструю и бесперебойную доставку информации.

Возможность сохранять устойчивость. Развернутая сетецентрическая среда должна обладать способностью сохранять свою функциональность в условиях как физического, так и информационного воздействия. Она должна обеспечивать свое устойчивое функционирование с учетом приоритетности обеспечиваемых функций по мере того, как системы или оборудование среды подвергаются воздействию

или получают повреждения. Сетецентрическая среда также должна осуществлять динамическую перемаршрутизацию информационных потоков и реконфигурацию информационных ресурсов по мере выхода из строя сетевых узлов и/или изменения требований к распределению информационных потоков. В ней также должны быть реализованы функции резервирования ресурсов для того, чтобы она была способна, в случае необходимости, поддержать или повысить свою производительность [112].

Возможность предоставлять сетевые услуги. Сетецентрическая среда должна обладать способностью предоставлять услуги, обычно ассоциируемые с сетевыми операциями, такие как:

- подключение всех сетевых средств;
- распределение и синхронизация информации между всеми участниками работы в сети;
- архивирование больших объемов информации;
- поддержание подключения к среде;
- загрузка информацией всех сетевых узлов;
- информационное обеспечение отдельных групп заинтересованных сообществ;
- поддержка узлов, не имеющих географической привязки.

2.5.4. Основные эффекты для объединенных сил, которые обеспечиваются за счет использования сетецентрической среды

Рассмотрим основные эффекты (в виде способностей объединенных сил), которые обеспечиваются за счет коллективного распределения и обработки информации в сетецентрической среде (рис 2.18).

Способность синхронизации действий. Высокая динамичность операций, проводимых в сетецентрической среде, требует от участников их проведения способности быстро синхронизировать свои действия между собой, независимо от указаний сверху (автономная синхронизация). Это позволит им гибко адаптировать свои действия, а также уменьшить влияние изменяющихся имеющихся или появляющихся новых угроз. Данная способность позволяет шире использовать проведение операций и их планирование на основе достигнутых результатов [112].

Способность синхронизации и распределения осведомленности об обстановке. Участники тех или иных действий должны не только вырабатывать собственное виденье ситуации, но также делить-

ся своим виденьем и осведомленностью о текущей ситуации с другими участниками операции. Различные участники боевых действий должны видеть, каким образом другие оценивают обстановку, а также иметь возможность обрабатывать информацию, поступающую от многих источников, уделяя при этом основное внимание выполнению текущей задачи [112].

Рис 2.17. Основные эффекты (в виде способностей объединенных сил), которые обеспечиваются за счет коллективного распределения и обработки информации в сетецентрической среде [112]

Способность синхронизации и распределения понимания обстановки. Если осведомленность об обстановке понимается по формуле «кто, где и что делает» применительно к сфере знаний о боевом пространстве, то понимание обстановки соответствует формуле «что это означает и как это использовать в своих интересах». Для достижения требуемого уровня понимания необходимо использовать соответствующие методы и средства принятия решений. Синхронизация и распределение такого понимания среди широкого круга участников действий обеспечит синергизм, который приведет к более высокому качеству коллективно принимаемых решений [112].

Способность осуществлять совместное принятие решений и планирование. Постоянно изменяющийся характер условий боевого пространства потребует от командиров и начальников использования в процессе принятия решений многих факторов, включая учет возможностей других командиров. В таких условиях для достижения успеха в процессе принятия решений потребуется взаимодействие и использование совершенных средств поддержки принятия решений. Также потребуется быстрый анализ потенциально возможных действий с такой степенью детализации, которая позволит рассматривать потенциальные результаты последующих действий второго и третьего порядков.

Процесс совместного принятия решений позволит командирам быть постоянно осведомленными об изменениях задач и целей, решаемых и достигаемых другими подразделениями, а также об их способности выполнять эти задачи [112].

Способность достигать конструктивной взаимозависимости. Совместные операции требуют установки формальных правил с целью комбинирования возможностей, имеющихся у разных видов ВС, что позволит формировать новые возможности объединенных сил. Возможность создания конструктивной взаимозависимости еще сильнее развивает этот аспект, используя сетевые взаимодействия (как на уровне людей, так и техники), что позволит осуществлять практически неограниченное комбинирование незадействованных возможностей видов ВС и их отдельных частей и обеспечить ранее недостижимые новые боевые возможности [112].

Сетецентрическая среда, создаваемая в интересах обеспечения информационного превосходства, предполагает создание мощной информационной инфраструктуры на ТВД, при этом предполагается, что она обеспечит лиц, принимающих решения, информацией такого уровня и качества, которые не были доступны ранее [2].

Сетецентрическая среда, интегрированная из коммуникационных сетей и сетей датчиков, программного обеспечения и организационных структур, обеспечит [2, 121, 127]:

- сбор информации с разнородных средств разведки в интересах ее последующего комплексирования;
- высокопроизводительную обработку в реальном времени информации, отображающей общую картину ситуации, складывающейся на ТВД;
- ведение каталогов баз данных, относящихся к зоне операции и способностям противника, а также доступ к этим базам лиц, принимающих решения, всех уровней военного управления;
- единое информационное пространство для информационного обмена участников операций и доступа к информационным услугам, основанное на устойчивых и высокоскоростных средствах связи и телекоммуникации;
- оперативное доведение информации (в масштабе близком к реальному времени) о ходе проведения операций, точные и своевременные разведывательные данные о местоположении и действиях как противника, так и своих войск;

- способность одновременно проводить взаимоувязанный комплекс операций на всем ТВД, выполняемых непрерывно с рассредоточенных основных мест применения сил и средств;
- наличие встроенных способностей к самозащите и противодействию подсистем информационной системы, воздействию широкого спектра средств противника (в том числе воздействиям в информационном пространстве).

Сетецентрическая среда ТВД – это совокупность подсистем для сбора, обработки, анализа, архивирования и распределения информации, которые, собственно, и призваны обеспечить достижение информационного превосходства объединенных сил над противником.

2.5.5. Влияние сетецентрической среды на строительство вооруженных сил

Операции, проводимые с использованием сетецентрической среды, будут значительно отличаться от операций, проводимых при существующей системе иерархического управления. Использование сетецентрической среды позволяет реализовать информационное обеспечение всех фаз операций (рис. 2.18).

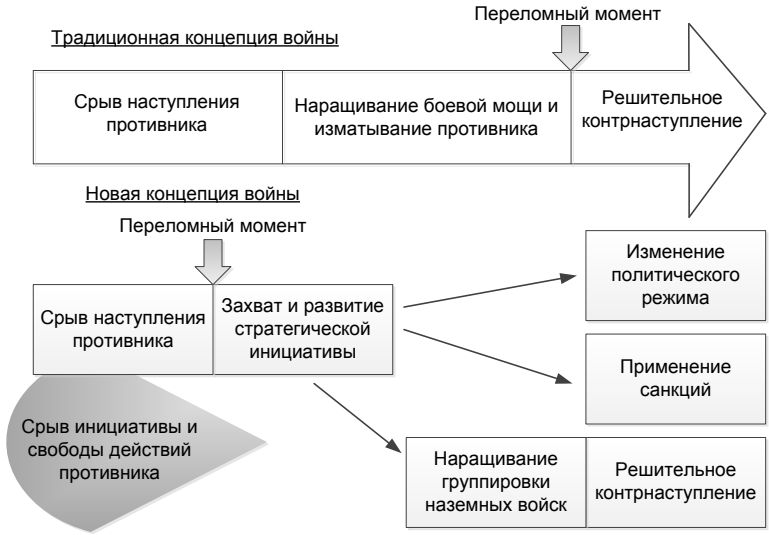


Рис. 2.18. Этапы вооруженного конфликта

Коллективное распределение и обработка информации в сетецентрической среде приведет к необходимости развития организационных принципов управления. Объединенные силы, функционирующие в сетецентрической среде, при проведении операций в меньшей степени будут зависеть от неповоротливых административно-директивных механизмов синхронизации действий, поскольку право доступа к информации об обстановке, данные о принятых решениях и об ответственности за них будут циркулировать в едином информационном пространстве. По мере выполнения задачи или при динамичном изменении оперативной среды доступ к объектам информационного пространства будет меняться в соответствии с изменением ролей и задач, выполняемых подразделениями объединенных сил [112].

Гибкость, с которой объединенные силы будут способны перейти от выполнения одной задачи к другой, будет являться значительным преимуществом их функционирования в сетецентрической среде. Данное преимущество станет результатом того, что будут сняты ограничения на пути информационных потоков, что увеличит прозрачность информации и соединит подразделения объединенных сил в едином информационном пространстве [112].

Использование сетецентрической среды в интересах Вооруженных сил окажет существенное влияние на их функционирование, управление и применение, в частности на [112]:

- доктрину;
- организационную структуру;
- средства связи и управления;
- масштаб вооруженной борьбы;
- подготовку и обучение личного состава;
- руководство и управление;
- личный состав;
- объекты различного назначения.

Рассмотрим влияние использования сетецентрической среды на развитие вооруженных сил более подробно.

Доктрина. Использование достижений информационно-технической революции изменит применение принципов войны и роль информации в ней, что найдет более яркое отображение в доктрине [112]:

- доктрина по-прежнему будет содержать руководящие принципы и являться практическим руководством применения вооруженных сил;

- тактика, способы и формы ведения боевых действий будут развиваться с учетом возрастающего значения информации для всех аспектов военных операций;
- развитие доктрины будет осуществляться с учетом возросшего динамизма боевых действий, а также роли «невоенных» способов противоборства, на ее развитие все большее влияние будут оказывать результаты военных игр и компьютерного моделирования военных потенциалов;
- объединение сил для совместно проводимых операций станут нормой для низших уровней организационных структур.

Организационные структуры. Эффективное применение сетецентрической среды потребует внедрения новых организационных связей как между подразделениями вооруженных сил, так и между министерством обороны и другими силовыми ведомствами, а также органами государственной власти при выполнении военных задач [112]:

- в рамках объединенных сил организационные структуры будут трансформироваться в интересах повышения эффективности распределения информации и принятия решения. Организационные структуры станут более «плоскими», а горизонтальные связи между подразделениями (формальные и неформальные) будут приобретать все большее значение;
- сетецентрическая среда в значительной мере облегчит формирование новых объединений сил и средств с более разнообразными структурами, ресурсами и задачи;
- системы связи таких организационных структур будут приобретать все возрастающее значение, поскольку они будут обеспечивать подключение и взаимодействие с сетецентрической средой.

Средства связи и управления. Внедрение сетецентрической среды в повседневную деятельность вооруженных сил потребует разработки средств широкополосного доступа к этой среде тех подразделений, которые в настоящее время не могут воспользоваться ее преимуществами по той причине, что они находятся в удаленных районах дислокации или действуют в жестких средах, например под водой. Эти средства должны обеспечивать почти непрерывный доступ к сетецентрической среде независимо от местонахождения подразделения или скорости его передвижения. При этом системы управления должны

предусматривать, с одной стороны, использование всех преимуществ сетецентрической среды, с другой – продолжать функционировать после отключения их от среды, а также автоматически проводить информационную интеграцию и синхронизацию при восстановлении подключения. К основным тенденциям в развитии систем связи и управления стоит отнести [112]:

- средства связи и управления должны поддерживать технологические решения в области информационной безопасности с учетом динамичного изменения параметров модели безопасности при получении, передаче, хранении и обработки информации;
- технологии верификации/идентификации получат широкое распространение в средствах связи и управления с целью обеспечения динамической ролевой безопасности;
- на информационном и физическом уровнях сетевые возможности пользователей должны характеризоваться высокой степенью интероперабельности. Для обеспечения интероперабельности в технической области необходимо модернизировать сетевые протоколы с учетом функционирования конечных пользователей в сетецентрической среде в реальном масштабе времени;
- в системах управления получат широкое распространение интеллектуальные методы поддержки принятия решений с учетом всех функциональных областей ведения боевых действий, а также текущей конфигурации и возможности доступа подразделений к сетецентрической среде;
- средства визуализации и моделирования обстановки, а также средства поддержки принятия решений должны стать максимально эргономичными и обеспечивать максимально подробное представление информации, поступающей из сетецентрической среды в интересах принятия решений на новом качественном уровне. Эти средства обеспечат более широкие возможности в области планирования и анализа обстановки, что, в свою очередь, существенно расширит возможности ведения боевых действий, моделирования и имитации при оценке проводимых действий и прогнозировании их результатов;
- интеллектуальные средства обработки «Больших Данных» сетецентрической среды позволят лицам, принимающим решения, фильтровать, классифицировать предварительно

поступающую информацию, что позволит командирам и их штабам получать быстрый и эффективный доступ к аналитически обработанной информации о текущей обстановке и прогнозу ее развития. Использование настраиваемых пользователем интеллектуальных средств обработки «Больших Данных» позволит выявить скрытые закономерности в изменении обстановки, тенденции в развитии действий противника, а также модифицировать процессы сбора и обработки информации для повышения ее оперативной ценности:

- внедрение новых средств связи и управления должно тесно увязываться с модернизацией средств вооружения, а также с решениями по обучению, подготовке и планированию применения личного состава вооруженных сил.

Концепция сетецентрической среды разработана в интересах командующих объединенными силами оперативного уровня вооруженных сил США на ближайшие годы и может быть использована во всех звеньях управления, от стратегического до тактического. Концепция сетецентрической среды является основой и аналитическим шаблоном для других руководящих документов, директив, решений, планов по развитию структуры управления вооруженные силами, их применению, а также модернизации вооружений, средств связи и управления.

2.5.6. Влияние сетецентрической среды на применение Вооруженных сил

Основной составляющей кардинального повышения боевых возможностей вооруженных сил является достижение информационного и технологического превосходства, которое преобразит современные понятия о маневре, ударе, защите и тыловом обеспечении и приведет к появлению новых оперативных концепций [2, 95, 121, 127].

1. «Господствующий маневр».
2. «Высокоточное сражение (бой)».
3. «Всеобъемлющая защита».
4. «Целенаправленное тыловое обеспечение».

Военные стратеги США считают, что реализация этих концепций будет давать их войскам всеохватывающее господство – подавляющее превосходство над противником на земле, в воздухе, на море, в космосе и в информационной сфере [95].

Рассмотрим эти оперативно-стратегические концепции более подробно.

«Господствующий маневр» – способность объединенных сил достигать превосходства над противником, прежде всего, за счет высоких темпов переброски войск и ведения боевых действий группировками наземных, морских, воздушных и космических сил, активно использующих маневр для решения поставленных задач. Сочетание позиционных преимуществ с высокими темпами перемещения войск и ведения боевых действий дает возможность применять силы и средства для нанесения ударов по важнейшим компонентам боевого потенциала противника на всех уровнях, вынуждая его воевать в невыгодном для него положении. «Господствующий маневр» предполагает наличие сил, способных развертывать превосходящие группировки в одной с противником среде боевого пространства, а также добиваться решающего превосходства посредством нанесения ударов по противнику носителями оружия из другой среды (авиация и ВМС – по наземным целям и др.) [95].

«Высокоточное сражение (бой)» – боевые действия, основанные на огневом поражении противника с использованием информационной интеграции двух компонентов:

- разведывательно-сенсорных систем;
- высокоточных средств поражения.

При этом разведывательно-сенсорные системы обеспечивают функции наблюдения, обнаружения и распознавания объектов (целей) противника, а также анализ технических параметров признаков их проявления в интересах максимально эффективного применения средств поражения [95].

Основной целью реализации этой концепции является придание вооруженным силам способности высокоточного воздействия на цели в кратчайшие сроки и на большие дальности с использованием набора ударных средств в обычном или ядерном оснащении, а также посредством проведения космических, информационных и специальных операций. Для достижения поставленной цели развернуты работы по созданию новейших типов высокоточных мобильных стратегических неядерных вооружений, в том числе таких, как планирующие и маневрирующие гиперзвуковые боеголовки, высокоточные крылатые ракеты, проникающие в грунт боеголовки, баллистические ракеты с боеголовками индивидуального наведения в обычном оснащении. По мнению ряда военных аналитиков, эти меры снизят роль ядерного оружия в будущих конфликтах за счет существенного расширения об-

ласти применения неядерных стратегических сил, оснащенных высокоточными средствами поражения, что обеспечит решение значительно большего круга задач с меньшими затратами и потерями [95].

«Всеобъемлющая защита» – эшелонированная (многослойная) защита своих войск (сил) от современных и перспективных средств поражения. Она предусматривает такую организацию подготовки и ведения боевых действий, при которой войскам обеспечивается максимальная безопасность при выдвижении и развертывании, а также при вводе в сражение. При этом предполагается, что эшелонированное охранение будут иметь не только принимающие непосредственное участие в операции силы, но и важные объекты в глубине оперативного построения. Особое внимание уделяется совершенствованию существующих и созданию новых систем идентификации своих войск («свой-чужой») с тем, чтобы исключить потери от собственных огневых средств [95].

«Целенаправленное тыловое обеспечение» – гибкое, в масштабе времени, близком к реальному, тыловое обеспечение войск. Материально-техническое обеспечение должно осуществляться по графикам, рассчитанным по часам и дням, а не по неделям, чтобы оперативно отслеживать наличие и местоположение материальных средств и при необходимости производить их переадресовку. Доставка материально-технических средств непосредственно в войска в ходе боевых действий на стратегическом, оперативном и тактическом уровнях предполагается осуществлять специально подготовленными комплектами («пакетами»). Такое обеспечение будет достигаться путем использования новейших технологий в области информатики, логистики и транспортных средств [95].

Основополагающими стратегическими концепциями применения единых сил на перспективу останутся [95]:

- передовое присутствие;
- обеспечение решающего превосходства;
- распространение силы;
- стратегическая гибкость.

При этом военные эксперты США, рассматривая возможные угрозы и вызовы будущего, особое внимание в подготовке объединенных войск уделяют способности вести боевые действия в условиях нетрадиционных форм проведения операций и так называемых асимметричных подходов к вероятным конфликтам.

2.6. Сетевые архитектуры, используемые для организации взаимодействия сил и средств в сетецентрической войне

Особенностью концепции сетецентрической войны является то, что объединение сетецентрической средой охватывает не только системы боевого управления, связи, вычислительной техники, разведки и наблюдения, но и боевые платформы, в первую очередь – носители средств огневого поражения. Это и определило формирование новой системы взглядов на формы и способы ведения вооруженной борьбы. Все более актуальным и приоритетным направлением развития вооруженных сил является достижение синергетического эффекта за счет интеграции через сетецентрическую среду средств поражения и информационных систем управления, связи и разведки (таб. 2.5) [43].

Таблица 2.5. Элементы сетевой инфраструктуры, интегрируемые через сетецентрическую среду [50]

№ п/п	Наименование элемента	Задачи элемента	Состав элемента
1	Средства разведки	Сбор информации, необходимой для обеспечения принятия решения	Разведывательные датчики, носитель (платформа), программное обеспечение, аппаратура связи
2	Центры обработки и корреляции информации	Прием, обработка и корреляция поступающей разнородной информации и подготовка данных ситуационной осведомленности на поле боя	Оборудование для отображения информации, инструментарий обеспечения подготовки принятия решения, аппаратура анализа, системы хранения и извлечения (поиска) информации, программное обеспечение (алгоритмы) корреляции информации, аппаратура связи

Продолжение табл. 2.5.

№ п/п	Наименование элемента	Задачи элемента	Состав элемента
3	Терминал связи (доступа) между системой передачи информации и системой коммутации	Предоставление (подключение) пользователю необходимых средств связи и отображения	Оборудование для отображения информации, инструментарий обеспечения подготовки принятия решения, инструментарий организации взаимодействия, системы хранения и извлечения (поиска) информации, средства обеспечения жизнедеятельности персонала, аппаратура связи
4	Базы данных	Обеспечение доступа пользователей к информации, ее поиск и извлечение	Оборудование для формирования электронных баз данных, инструментарий поиска и извлечение информации, программные средства управления базами данных, средства обеспечения жизнедеятельности персонала, аппаратура связи
5	Коммутационные центры («Хабы»)	Коммутация каналов между пользователями в сети (терминалами связи)	Средства коммутации, средства обеспечения жизнедеятельности персонала, программное обеспечение автоматической коммутации, средства связи и передачи данных
6	Центры управления локальной сетью (Концентраторы)	Разграничение доступа и распределение ресурсов	Оборудование центров управления, средства обеспечения жизнедеятельности персонала, программное обеспечение мониторинга сети, инструментарий распределения ресурсов, аппаратура связи
7	Каналы связи и передачи данных	Обеспечение передачи информации путем соединения коммутационных центров, баз данных, оконечных пользователей и др.	Средства связи и передачи данных (КВ, УКВ и др.), средства обеспечения жизнедеятельности персонала, аппаратура связи

Понятие «сетецентрическая война» или «ведение боевых действий в едином информационном пространстве» рассматривает вооруженные силы как элементы, подключенные к сетецентрической среде. В зависимости от выбора сетевой архитектуры и ее типа, элементами среды могут быть корабли, воздушные суда, высокоточные средства поражения, системы управления, связи, разведки, воинские подразделения, а также их комбинации. Возможности таких объеденных боевых формирований определяются не столько их индивидуальными характеристиками, сколько возможностями всей группы как единого целого с учетом их взаимодействия в сетецентрической среде. В свете этого факта изучение различных аспектов сетевых архитектур, являющихся основой сетецентрической среды, является важным условием изучения возможностей объеденных боевых формирований, построенных на новых принципах [43, 96].

В работах А.Е. Кондратьева [43, 52] для изучения сетевых архитектур сетецентрической среды предложено использовать научно-методический аппарат таксономии, являющейся частью теории классификации и систематизации сложноорганизованных областей действительности, имеющих иерархическое строение. Более того, как показано в [43, 52], научно-методический аппарат таксономии может использоваться при планировании операций, организации способов боевых действий и при обосновании организационной структуры вооруженных сил.

Качественные категории сетевых архитектур, основанные на таксономии сетей, можно оценить с использованием следующих понятий [52]:

- равноценность – неравноценность;
- однородность – неоднородность;

а также классифицировать сетевые архитектуры на [52]:

- централизованную;
- запросную;
- стайную (в виде «роя»);
- комбинации различных базовых архитектур.

Сетевая архитектура равноценна, если все элементы, подключенные к сетецентрической среде, идентичны, и потеря одного из них равнозначна потери другого. В свою очередь, архитектура сети неравноценна, если один подключенный элемент имеет большую ценность и значимость для всей сети по отношению к другим элементам [52].

Сетевая архитектура является однородной, если все подключенные элементы идентичны, и неоднородна, если эти элементы различны [52].

Комбинируя категории равноценности и однородности с классификацией сетевых архитектур, можно получить «треугольник возможностей» (рис. 2.19), потому что однородная архитектура может быть как равноценной, так и неравноценной (содержащей центральный координирующий элемент – «хаб»). Каждый из узлов этого треугольника соответствует определенной сетевой архитектуре. Можно выделить три типа основных сетевых архитектур:

- тип A – централизованная;
- тип E – архитектура «сети по запросу»;
- тип G – архитектура «стаи» (архитектура «роя»).

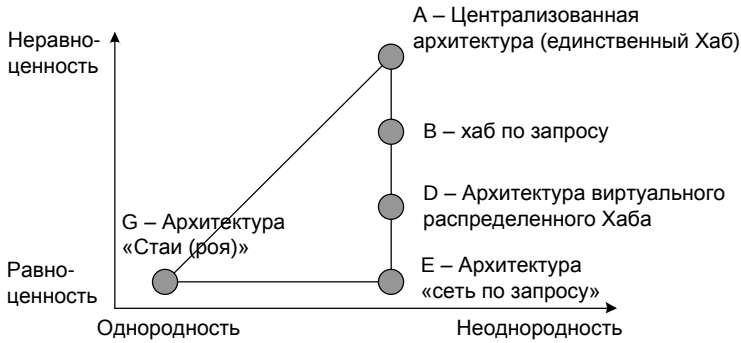


Рис. 2.18. Основные типы сетевых архитектур, используемых для организации взаимодействия в сетецентрической среде

Рассмотрим особенности данных архитектур более подробно в соответствии с материалами, представленными в работах [43, 52].

2.6.1. Централизованная архитектура

В централизованной архитектуре используется единственный ценный элемент – хаб, окруженный множеством других элементов меньшей ценности. Еще в 1873 г. К. Клаузевиц назвал подобный ценный элемент «центром тяжести», от которого зависит успех операции, а его потеря приводит к невозможности для вооруженных сил выполнять поставленные задачи. Как правило, наличие центрального «хаба»

повышает возможности элементов сети, которые он объединяет, но различные типы хабов вносят различный вклад в увеличение этих возможностей [52].

Как показано в работах [43, 98], командование ВС Великобритании во время конфликта на Фолклендах в качестве центрального «хаба» авиационной группы использовали топливозаправщики. Это позволило за счет дозаправки существенно увеличить дальность полета группы и его продолжительность, расширить общие возможности по применению боевых самолетов и, кроме того, возложить на топливозаправщик функции воздушных центров управления и связи.

Центральный хаб, как правило, имеет период доступности, вследствие необходимости проведения регламентных работ, возобновления ресурса и т.д. Поэтому для обеспечения устойчивого функционирования сети необходимо его резервирование. При применении сетевой архитектуры типа «А» для центрального хаба должна быть обеспечена высокая степень живучести, так как без него другие элементы сети не смогут выполнять боевые задачи. Центральный «хаб» обеспечивает синергетический эффект, за счет объединения отдельных средств участников операции значительно повышается эффективность всего формирования. Он обеспечивает координацию действий боевых средств, повышая их боевую эффективность по сравнению с эффективностью каждого средства в отдельности [52].

Например, до недавнего времени ВМС США имели на вооружении 12 авианосцев для одновременного обеспечения двух-трех океанских операций. При этом каждый авианосец сопровождают около восьми судов обеспечения (фрегаты, подводные лодки, крейсера и др.). Несмотря на то, что они оснащаются наступательным ракетным вооружением, основной их задачей является обеспечение безопасности центрального «хаба» – авианосца. При проведении операции авианосец выступает центром управления и связи, координируя действия авиационной группировки с нанесением ударов средствами судов обеспечения [52].

Как показано в работах [43, 52, 99], полностью централизованной система управления и связи может быть тогда, когда решены основные оперативные и тактические задачи, а хаб имеет доступ ко всей требуемой информации и необходимые возможности для подготовки принятия решения и быстрого распределения информации. Полностью централизованная архитектура хорошо подходит для воздушного и морского пространства, а также может быть использована для управления наземной операцией [43].

В случае если в системе управления для повышения устойчивости управления силами и средствами используются несколько центральных «хабов», то она приходит к сетецентрической архитектуре типа «B» хаб по запросу или типа «D» виртуальный распределенный Хаб [52].

2.6.2. Архитектура «сеть по запросу»

Архитектура «сеть по запросу» представляет собой объединение через сетецентрическую среду множества одинаковых по ценности, но неоднородных элементов. Особенностью такой архитектуры является то, что она состоит из средств, имеющих, с одной стороны, узкую специализацию (средство разведки, средство управления, средство огневого поражения и т.д.), а с другой стороны – высокое качество выполнения конкретного типа задач [43, 52].

В основу такой архитектуры положены Mesh-технологии объединения в сеть разнообразного телекоммуникационного оборудования с последующей интеграцией сети в состав системы управления. Особенностью Mesh-сетей является возможность установления связей и объединения в сообщества без посредничества центральных Хабов. При использовании архитектуры «сеть по запросу» потоки данных и сигналы управления передаются по сети, при этом элементы сети обладают свойством самосинхронизации и самостоятельно определяют потребителя информации. Управление силами и средствами на основе архитектуры «сеть по запросу» требует заблаговременной разработки и внедрения единых протоколов информационного пространства, которые позволяют обеспечить связь между собой всех элементов сети, задействованных в операции [43, 52].

В настоящее время именно в соответствии с данной архитектурой ведется создание сетецентрической среды. Ее техническую основу составляют распределенные децентрализованные сети связи на основе Mesh-протоколов, особенности построения которых более подробно рассмотрены в работах [271, 272, 273, 274, 275].

2.6.3. Архитектура «роя»

Наиболее сложной, но в то же время и наиболее перспективной считается архитектура «роя», представляющая собой комбинацию полностью равноценных и однородных элементов (сети боевых самолетов, морских кораблей, боевых машин пехоты, танков и т.д.). Каж-

дый из таких элементов имеет свои (хотя и с ограниченными возможностями) средства разведки, поражения, связи и управления [43, 52].

Для эффективного выполнения боевой задачи такие элементы должны обмениваться между собой информацией, самоорганизовываться и самосинхронизироваться для повышения собственных возможностей. Для достижения мультипликативного эффекта «рой» идентичных элементов дополняется специальным центральным «хабом», выполняющим координирующие функции [52].

Архитектура «роя» может иметь несколько типов [43, 52]:

- управляемый рой;
- иерархический рой;
- распределенный рой.

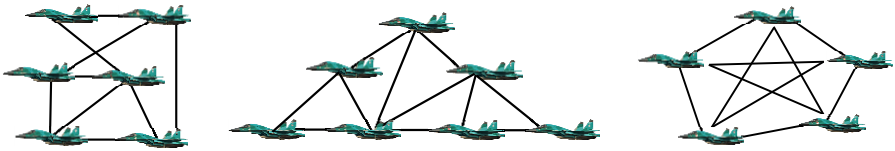


Рис. 2.20. Типы сетевой архитектуры «роя» [43, 52]

Архитектура типа «управляемый рой» соответствует случаю, когда один из элементов выбирается в качестве временного узла-хаба (разница с централизованной архитектурой в том, что все элементы роя идентичны, т.е. равноценны и однородны). Выбор узла-хаба осуществляется с учетом складывающейся обстановки, распределения элементов, их боевых возможностей и других факторов. Такой подход иногда применяется в группах сил специальных операций, где члены группы могут принимать управление на себя. В этом случае данные разведки посылаются узлу-хабу, где они обрабатываются и интегрируются в данные о ситуационной осведомленности, на основании которых формируется решение о действиях каждого элемента сети, после этого данные ситуационной осведомленности и решения о действиях распределяется другим элементам. В случае изменения обстановки сеть может быть реконфигурирована, и в ней может быть назначен новый узел-хаб. Такая архитектура ограничивает количество пользователей сети, но позволит расширить возможности по эффективному управлению сетью [43].

Архитектура типа «иерархический рой» близка к традиционной централизованной архитектуре построения систем управления и

наилучшим образом подходит для решения сложных задач. При использовании централизованной архитектуры управления общая картина данных о ситуационной осведомленности и замысел операции (боя) подготавливаются центральным элементом, доводятся нижестоящим звеньям управления в тактическое звено, где на них накладывается необходимая командирам этого звена управления информация. При отсутствии технических средств управления и связи такая архитектура была наиболее предпочтительной, но она не обеспечивала необходимую скорость принятия решения и управления подчиненными силами и средствами [43].

В архитектуре типа «распределенный рой» нет центрального элемента, а все решения принимаются в результате достижения консенсуса или определенных договоренностей между элементами сети. При этом каждый элемент подготавливает свои данные о ситуационной осведомленности и участвует в распределенном принятии решения. Такая архитектура требует высокой пропускной способности сети связи и быстродействия локальных систем управления в каждом элементе. Выполнение данных требований позволяет такой архитектуре обеспечить высокую эффективность управления [43].

Архитектура типа «распределенный рой» свойственна формированиям, выполняющим независимые боевые задачи. Боевое формирование с архитектурой построения сети типа распределенный «рой» можно сравнить с муравьиной колонией, где нет четкого централизованного управления. Ни один элемент не может оценить глобальные потребности всего формирования, глобальную цель его существования и свое место в ее достижении. Возможности отдельных элементов ограничены, и каждый из них может принимать только элементарные решения в рамках своей компетенции. Такая архитектура лишает элементы сети одного из преимуществ использования сетецентрической среды – ситуационной осведомленности. В связи с этим, эффективность использования такой архитектуры для управления боевыми действиями вызывает много вопросов у зарубежных военных экспертов [43].

Одним из вариантов использования такого типа архитектуры является применение автономных средств – БПЛА, автономных подводных аппаратов, распределенных наземных робототехнических группировок для доставки к линии боевого соприкосновения средств поражения, а также для барражирования, поиска целей и их поражения [43].

Смешанная архитектура типа «рой» основана на одновременном использовании и архитектуры «роя» и архитектуры сети «по запросу». Такой способ построения сети применяется при использовании равноценных и неоднородных элементов (в чем-то схожих, а в чем-то различных). Например, авиационная группа БПЛА может иметь общие возможности, но одновременно с этим разную специализацию (БПЛА-разведчик, ударный БПЛА, БПЛА-ретранслятор) [43].

На практике, как правило, не встречается какой-либо одной архитектуры и реальные архитектуры сетецентрической среды имеют черты нескольких базовых архитектур. Например, система ПВО ВМС США CEC (Cooperative Engagement Capability) использует архитектуру распределенный «рой» для передачи данных о ситуационной осведомленности, но при выборе целей применяется архитектура управляемый «рой» с использованием головного корабля в качестве «узла-хаба». Таким образом, внутри сети разведывательных средств используется архитектура распределенный «рой», а в сети средств управления – управляемый «рой» [43].

В общем случае, разработка архитектуры сетецентрической среды на основе роя является перспективным направлением исследований в области военного управления. Техническим аспектам реализации роевого управления посвящены работы в области многоагентного (мультиагентного) интеллектуального управления.

2.6.4. Смешанные архитектуры

Зарубежные аналитики выделяют два подтипа смешанных архитектур [43]:

- объединение нескольких типов неоднородных, но равноценных средств;
- объединенная сеть.

Объединение нескольких типов неоднородных, но равноценных средств применяется, например, для информационной интеграции техники, разрабатываемой по программе «Перспективные боевые системы» СВ США – 14 комплексов, включая машины управления, гаубицы, минометы, БПЛА, наземные роботизированные комплексы и т.д. В таком объединении архитектура иерархического «роя» применяется для получения и распределения данных ситуационной осведомленности. Вместе с тем архитектура распределенного «роя» применяется для выполнения перспективными наземными комплексами боевой задачи. При этом для информационного сопряжения неоднород-

ных элементов может использоваться и архитектура формирования «сети по запросу» [43].

Объединенная сеть – самый сложный вариант архитектуры сети, который объединяет в себе все имеющиеся сетевые архитектуры, характерные, в первую очередь, для управления операциями объединенных сил в сетецентрической войне. Центральный хаб в такой объединенной архитектуре сети будет выполнять задачи именно центрального узла. Группы равноценных и равнозначных элементов будут объединяться архитектурой «рой», а архитектура «сети по запросу» будет использоваться для информационного сопряжения неоднородных сетей и средств [43].

По мнению военных аналитиков [43, 52], применение архитектуры объединенной сети для построения сетецентрической среды позволит обеспечить вертикальную и горизонтальную интеграцию всех участников боевых действий и обеспечить необходимый уровень информационного комплексирования систем управления, связи, передачи данных и огневого поражения объединенных сил.

2.6.5. Живучесть типовых сетевых архитектур

Как правило, каждый тип сетевой архитектуры имеет свои уязвимые элементы в виде центральных узлов-хабов, линий связи и уязвимых элементов и т.д. В этой связи для изучения живучести перспективных сетевых архитектур, применяемых для формирования единого информационно-коммуникационного пространства сетецентрической среды, целесообразно использовать специализированные научно-обоснованные методы. К данным методам можно отнести методы теории сложных сетей, представленные в работах [277, 278, 279, 280], которые позволяют определить центры тяжести сетей (как их системообразующие элементы) и выявить критически уязвимые элементы таких сетей.

При этом ряд специалистов в своих работах [43, 52, 101, 103, 104, 277] обращают внимание на различность понятий «центра тяжести» и «критически важных уязвимых элементов», т.к. первый термин применяется для всей системы, а второй – именно для подготовки удара (воздействия) на систему. Например, для уничтожения или вывода из строя всей авианосно-ударной группы необходимо выделить авианосец в качестве ее центра тяжести. В дальнейшем необходимо исследовать авианосец уже как самостоятельную систему и обнаружить у него «центр тяжести» или выявить его «критически важные уязвимые

элементы», поражение которых выведет авианосец из строя и приведет к невозможности для авианосно-ударной группы выполнять свои задачи [43].

Центр тяжести – базовый термин, ранее уже используемый в военно-теоретических изысканиях. Немецкий военный теоретик и историк Клаузевиц первым начал обсуждать и создавать теорию центров тяжести, понимая под центром тяжести некоторую «центральную точку» вооруженных сил и государства [100].

С другой стороны, доктор Дж. Стрэйндж (Jonathan Strange) и полковник СВ Великобритании Р. Айрон (R. Iron) в своей работе «Понимание центров тяжести и уязвимых элементов» [101] отмечали, что «центральная точка», имеющая отношение к вооруженным силам противника, может быть как физической, так и моральной и может находиться на стратегическом, оперативном или тактическом уровнях.

В доктрине НАТО [102] центр тяжести описывается как потенциал или место, где государства, альянсы, боевые формирования или другие типы группировок концентрируют свои возможности для достижения свободы действий, физической мощи (силы) и готовности вести борьбу.

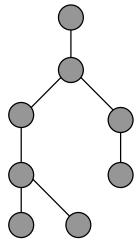
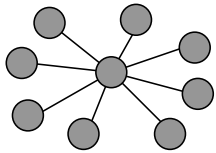
Директор управления национальной безопасности Института стратегических исследований Колледжа СВ США А. Эчеваррия в своем труде «Центры тяжести Клаузевица – это не то, что мы думаем» [103] дал несколько другое описание. В отличие от предыдущих исследователей он уточнил, что центр тяжести – это центростремительная сила, связывающая воедино разрозненные компоненты вооруженных сил противника. Однако если применить комплексный подход для изучения факторов, связывающих разрозненные части воедино, то можно найти и центр тяжести противника.

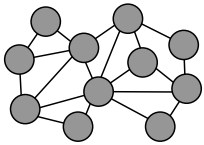
Сотрудник Колледжа Королевских ВС Швеции Дж. Варден в работе «Центры тяжести в военных операциях» [104] применил схожий подход. Он соглашался, что противник должен изучаться как система, состоящая из разнообразного количества взаимосвязанных элементов. Базовый элемент такой системы – это энергия различного вида: физическая (люди, здания, системы связи и оружия) или психологическая (сила воли, возможности и способности), и если есть возможность направить поток дестабилизирующих воздействий в центральную часть такой системы, то вся система может быть уничтожена или выведена из строя. Он также отмечал, что во всей такой системе, построенной из определенного количества элементов (узлов), объединенных сетью, имеется, как правило, несколько ключевых элементов,

воздействие на которые и может привести к выходу всей системы из строя.

Одним из основных и неотъемлемых элементов методологии исследования устойчивости управления войсками и силами является оценка живучести сетевых архитектур. Использование методов теории сложных систем, представленных в работах [277, 278, 279, 280], позволило выявить центры тяжести и уязвимые элементы сетевых архитектур, представленные в табл. 2.6.

Таблица 2.6. Уязвимые элементы типовых сетевых архитектур [43, 52]

Тип сетевой архитектуры и ее особенности	**Уязвимые элементы сетевой архитектуры**	**Возможные способы воздействия**
Иерархическая архитектура с четко определенной структурой управления и связей 	Подобная структура критична к временным параметрам управления сверху-вниз. В качестве ключевых узлов выступают узлы с наибольшем количеством связей либо центры принятия решений. Также уязвимыми по свойствам информационной безопасности элементами являются передаваемые по сети информационные потоки	Иерархическая структура управления уязвима к воздействиям, связанным с нарушением связности структуры, реализуемых как огневыми средствами, так и средствами РЭП. Метод воздействия – сверху-вниз. Из-за отсутствия дополнительных связей в структуре легко нарушить управление между отдельными звеньями управления и боевыми формированиями
Централизованная архитектура основана на подчинении всех элементов одному центральному хабу. 	Наиболее уязвимым элементом такой архитектуры является центральный хаб. При организации воздействия на него из строя будет выведена вся сеть	Способ воздействия на такие сети аналогичен воздействию на иерархическую архитектуру сетей. Главным объектом воздействия является центральный хаб. Возможно также осуществление информационных воздействий на подключенные элементы в целях дестабилизации управления в такой сети

Тип сетевой архитектуры и ее особенности	Уязвимые элементы сетевой архитектуры	Возможные способы воздействия
Распределенная сеть характеризуется отсутствием традиционных принципов иерархического управления. Вся информация, циркулирующая в сети, доводится до каждого ее элемента. В такой сети пути выдачи управляющих воздействий многократно зарезервированы. В случае выхода отдельных элементов из строя, управляющие воздействия будут перенаправлены 	Возможным уязвимым элементом может стать именно отсутствие четко централизованного управления. В качестве уязвимых элементов сети выступают: узлы с наибольшим количеством связей; узлы, входящие в распределенную сеть принятия решений; узлы обработки информации; связи с максимально высокой информацио-нной нагрузкой; связи, имеющие низкую разведзащищенность и безопасность. Также элементами, уязвимыми по свойствам информационной безопасности, являются передаваемые по сети информационные потоки	Данная сеть довольно устойчива к воздействиям, ориентиро-ванным на поражение отдельных узлов и связей, благодаря высокой связности сети. Вместе с тем, отсутствие элементов централизованного управ-ления и обработки информации делает эту архитектуру уязвимой к дезинформации, а также к внедрению ложных элементов в сеть. Кроме того, в таких сетях значите-льная часть ресурсов затрачивается на передачу служебной ин-формации, необходимой для постоянной синхронизации сети управления и репликации данных об обстановке, что делает такую архитектуру уязвимой к поражению служебно-обеспе-чивающей части сети

Таким образом, каждая типовая сетевая архитектура имеет свои уязвимые элементы. Кроме того, для каждой архитектуры целесообразно применять специальный подход для организации и осуществления мероприятий по повышению ее живучести в интересах обеспечения устойчивости управления войсками и силами.

При этом представленная классификация сетевых архитектур, ранее предложенная в работах [43, 52], позволяет обосновать вскрытие структуры управления силами и оружием в условиях сетецентрической войны. Кроме того, наиболее перспективными архитектурами являются распределенные архитектуры типа «рой», возможности которых в настоящее время представляются еще в недостаточной степени исследованными. Однако актуальность применения их существенно возрастет с ростом числа роботизированных боевых комплексов, привлекаемых для решения боевых задач. К наиболее актуальным ис-

следованиям относится совмещение роевой архитектуры сети управления с децентрализованной системой коллективного интеллекта, что позволит не только обеспечить автономность действий роя робототехнических средств, но и существенно повысит адекватность и интеллектуальный уровень принимаемых таким роем решений на применение оружия.

2.7. Уязвимости и недостатки концепции сетецентрической войны

2.7.1. Критика концепции сетецентрической войны

Первоначально подходы к сетецентрической войне были предложены еще в конце прошлого века вице-адмиралом ВМС США А.К. Себровски и экспертом министерства обороны Дж. Гарсткой (J. Garstka) в работе [329], а позднее – законодательно оформлены в виде ряда официальных концепций. Вместе с тем нельзя не отметить, что, являясь на данный момент реальным инструментом повышения боевых возможностей, концепция сетецентрической войны от этого не становится панацеей для решения всех проблем военного управления. Подтверждением этому служит состояние сообщества военных экспертов в США, которое разделилось на сторонников, серьезно сомневающихся, и противников этой инновационной концепции.

Одним из первых критиков концепции сетецентрической войны еще на этапе ее зарождения стал Т. Барнетт (Thomas Barnett) со своей статьей «Семь смертных грехов сетевой войны» [240], вышедшей в январе 1999 г. В ней он отмечал, что практическое внедрение концепции сетецентрической войны потребует больших расходов, кроме того, данная концепция замедлит адаптацию военной системы США к операциям вне условий войны. Далее Т. Барнетт критиковал одну из парадигм концепции, отстаивающую принцип «много и дешево», вместо «мало и дорого», задаваясь вопросом о том, как же это будет возможно. Кроме того, он увидел в новой концепции возрождение старого мифа о стратегической бомбардировке и вместе с критикой статьи А.К. Себровски и Дж. Гарстка [329] поставил под сомнение модель колец Джона Вардена о последовательности поражения целей, а также подверг критике и петлю «наблюдай» – «ориентируйся» – «решай» – «действуй» из теории Дж. Бойда. Децентрализация тоже не ускользнула от внимания профессора. Он отметил, что нет таких военных в мире, которые хотели бы максимально децентрализовать

власть принятия решений. Тяга к получению информации, согласно Т. Барнетту, грозит перерасти в информационную перегрузку органов управления, поэтому оптимальным решением будет наличие достаточно ограниченного уровня командования [239, 240].

В книге Дж. Гарстки, Д. Альбертса и Ф. Штайна (J. Garstka, D. Alberts, F. Stein) «Сетецентричная война» [330] одна глава посвящена мифам и заблуждениям, сложившимся вокруг концепции сетецентрических войн. Несмотря на то, что с момента выхода этой книги прошло более десяти лет и ряд тезисов авторов можно подкорректировать с учетом прошедших изменений, целесообразно рассмотреть эти мифы, чтобы проследить динамику перемен, как в теории, так и на практике. При этом по мнению авторов, они вообще не являются экспертами в области концепции сетецентрических войн, более того, на момент написания книги эта концепция являлась скорее абстрактным процессом, а не конкретной реальностью. Лишь гораздо позже будет осознан весь потенциал сетецентрической концепции, а еще позже она начнет широко применяться в практике ведения боевых действий.

Мифами и заблуждениями концепции сетецентрической войны, на взгляд авторов работ [239, 330], является следующее.

1. *Концепция – это уже почти все*. Для воплощения концепции в реальность необходим перевод информационных возможностей в реальные боевые операционные возможности, для чего нужны концепции операций, новые организационные формы, новая военная доктрина, модернизация структуры вооруженных сил.

2. *Сетецентрическая концепция и всеобщая сеть – одно и то же.* В действительности сетецентрическая концепция скорее связана с преимуществами, которые дает внедрение сетевого принципа управления, а не с сетями передачи данных как физической инфраструктурой информационного обмена. При этом концепция действительно ориентирована на увеличение боевой мощи за счет эффективной связи элементов наблюдения, управления и воздействия, распределенных как пространственно, так и иерархически. Включение этих элементов в единую сеть дает им возможность получать распределенную информацию, взаимодействовать друг с другом и достигать необходимой степени самосинхронизации.

3. *Сетецентрическая концепция изменит природу войны*. По выводам авторов, сетецентрическая концепция лишь усовершенствует возможности для достижения основных целей войны за счет снятия информационных и бюрократических барьеров. Сами принципы войны остаются неизменными – атака, экономия сил, внезапность и объ-

единенное командование, но все они могут быть улучшены при принятии на вооружение сетецентрической концепции.

4. *Сетецентрическая война может вестись только при широкомасштабном конфликте, когда силы противников примерно равны*. К такому выводу можно прийти, если рассматривать сетецентрическую войну как некие тактические сенсорные стрельбы, которыми являлись ранние эксперименты Пентагона по внедрению этой концепции. Однако принципом атаки является действие, а не реакция и диктат в отношении времени, цели, масштабов, интенсивности, а также места операции. Все это связано с осведомленностью о месте боя, со скоростью командования и сохранением активного состояния. Соответственно все эти особенности сетецентрической войны по навязыванию менее развитому технически противнику своего темпа ведения боевых действий нашли отражение в войнах последних десятилетий, которые носили явно выраженный локальный и асимметричный характер.

5. *Сетецентрическая концепция делает вооруженные силы более уязвимыми для асимметричных атак*. Степень уязвимости зависит от степени защищенности сетецентрической среды, от того, как принципы сетецентрического управления будут внедрены в концепции проведения операций, доктрину, структуру вооруженных сил и все другие элементы.

Растущая угроза асимметричного воздействия на сетецентрические системы управления заключается в возможности воздействия на нее принципиально новыми способами, например, информационным оружием. Повышение информационной связности и взаимозависимости элементов делает сетецентрическую систему уязвимой в информационной сфере. Эта уязвимость продолжит нарастать, так как и в военно-политических и в технических аспектах сетецентрической концепции различные ее функции и элементы становятся все более сложными и информационно-зависимыми.

Однако, по мнению авторов работы [330], было бы глупо отказаться от концепции сетецентрической войны как раз по этим причинам. Наоборот, необходимо, руководствуясь знанием об уязвимости концепции, исследовать потенциальные уязвимые места и создавать информационную инфраструктуру, акцентируя внимание на ее безопасности в сетецентрической среде и, прежде всего, по отношению к информационным атакам.

6. *Для достижения полного задействования концепции сетецентрической войны для всего спектра выполняемых задач необходима соответствующая инфраструктура*. Опыт внедрения концепции сетецентрической войны в США показывает, что действительно для внедрения этой концепции требуется развертывание сильносвязной информационной инфраструктуры. Это является дорогостоящей, но отнюдь не невыполнимой задачей. При одномоментном развертывании соответствующей информационной инфраструктуры дальнейшие задачи по оптимизации структуры вооруженных сил, боевому слаживанию подразделений на основе новых принципов управления, объединению сил и средств в рамках единого информационного пространства решаются постепенно и эволюционным путем.

7. *Коммерческая среда покажет, что делать*. Отдельные принципы сетецентрической концепции были заимствованы из коммерческой сферы. Однако эффективные принципы коммерческого управления не всегда могут быть преобразованы в настолько же эффективные принципы военного управления. Утверждение экспертов в области сетецентрической войны, «что хорошо для бизнеса, полезно и для войны», является опасным упрощением. Однако обратное утверждение, что «уроки, полученные в коммерческом секторе, не имеют применения в мире войны», тоже неверно.

8. *Концепция сетецентрической войны дает власть для доминирования над противником*. Очевидно, что те, кто утверждает, что концепция сетецентрической войны является ответом на все вызовы и современные угрозы, вообще не понимают, что представляет собой данная концепция. Она позволят получить максимум от людей и технических средств. Тем не менее улучшенное информационное взаимодействие, высокая скорость командования и другие атрибуты сетецентрической войны не сделают из несовершенного оружия идеальное. Важно помнить, что нужна сбалансированная совокупность возможностей для выполнения боевых задач. Для некоторых видов операций вполне достаточно и иерархической системы управления. Сетецентрическое управление может улучшить боевой потенциал, но не является панацеей.

9. *Концепция сетецентрической войны не выдержит столкновения с реальностью, когда начнутся первые затруднения, противоречия или сложности реальной войны*. Дело в том, что война всегда характеризуется сложностями, затруднениями и противоречиями. Описанные факторы не умаляют преимуществ, которые концепция сетецентрической войны может предоставить вооруженным силам в

плане улучшенной осведомленности в отношении поля битвы и доступа к информационным активам.

10. *Концепция сетецентрической войны – это попытка полностью автоматизировать войну, что в итоге приведет к поражению.* Концепция не связана с переносом сражения «в сеть» или с надеждой на более автоматизированные инструменты. Она связана с обработкой информации для максимизации боевой мощи посредством предоставления доступной информации автономным боевым элементам, что позволит им быть более эффективными и рациональными. Концепция развивает среду взаимодействия между командирами, подразделениями и средствами поражения, что облегчит координацию их реакции на складывающиеся ситуации. Однако в рамках концепции могут применяться и автоматические робототехнические комплексы. Таким образом, потенциально, многого можно будет достичь при благоразумном применении автоматизированных процессов.

11. *Концепция сетецентрической войны станет погоней за своим хвостом, а не ответом на вызовы сражений*. Такое мнение высказывалось об эффекте повышения скорости командования. Оно состоит в том, что можно развить такую скорость, которая достигнет таких значений, что лица, принимающие решения, будут бежать «впереди себя» на поле битвы, реагируя не на действия противника, а на свои собственные действия (гоняясь за своим хвостом). Опыт использования концепции сетецентрических войн в реальных операциях показал новые принципы управления, которые дают возможность увеличивать скорость командования, когда это необходимо. Нет необходимости форсировать события, если в этом нет нужды.

Начиная с 2000 г. министерство обороны США осуществляет масштабные мероприятия по реализации концепции сетецентрической войны в вооруженных силах. Положения о необходимости «сетецентричности» и выгодах, которые она представляет, занимают значительное место в доктринах по ведению боевых действий группировками войск и применению видов вооруженных сил. США планируют завершить создание глобальной информационно-управленческой сети к 2020 г. Совет по сетецентрическим возможностям в ходе разработки требований к ВВТ оценивает будущие системы оружия с точки зрения возможности их встраивания в данную информационную сеть. Министерство обороны США затратило и продолжает расходовать миллиарды долларов для создания «сетецентрических» вооруженных сил [82, 112].

В первые годы после официального провозглашения концепции сетецентрических войн, она находилась вне критики. Так, профессор военно-морского колледжа США М. Вего (Milan Vego) в 2003 г. в своей работе [87] указывал: «Концепция ведения боевых действий в единой информационной среде все больше превращается в новую религию – совокупность верований, которую нельзя серьезно оспорить. Ее недостатки или уязвимые места не подвергаются публичному обсуждению, с ними неохотно соглашаются». Оппоненты концепции сетецентрических войн вполне справедливо спрашивали, как это становится возможным, что недостатки концепции остаются непризнанными, несмотря то, что серьезные ошибки были выявлены в ходе ее критического анализа и опытных испытаний.

Некоторые эксперты отмечают, что приверженность военного руководства концепции сетецентрических войн подавляет полезную критику со стороны командующих оперативными объединениями. По их мнению, американские военные трансформируют свои войска для того, чтобы вести войны, которые они хотят вести, вместо того, чтобы готовиться к войнам, которые, скорее всего, придется вести. Если предполагается, что сетецентрические войны будут скоротечными, то более слабый противник, вероятно, может попытаться втянуть американские войска в затяжной конфликт низкой интенсивности и будет пытаться победить, избегая разгрома, в то время как политики капитулируют перед лицом растущих расходов [82].

Как показывает анализ открытых источников, в последнее время в американской печати значительно уменьшилось количество публикаций по вопросам супервысокой эффективности сетецентрических войн, появляются материалы критического характера. Начальной точкой для критического анализа явились полученные данные о том, что технологическое превосходство сыграло намного меньшую роль в успехе Многонациональных сил во время первой иракской войны (2003 г.), чем раньше считалось [82].

Отдельные специалисты утверждают, что концепция сетецентрической войны остается непроверенной с научной точки зрения. Они говорят, что эта концепция не может претендовать на научный статус, несмотря на ее «очаровывающий трансформационный блеск», она преувеличивает надежды на информационно-коммуникационную технологию и в то же время не способна адекватно и полностью реализовать потенциал, который представляют технологии.

Так, критики концепции сетецентрических войн приводят следующие аргументы [82]:

- до сих пор отсутствует подходящее определение «сетецентрических операций» (хотя сторонники концепции утверждают, что опытные испытания подтверждает научную гипотезу их концепции);
- экспериментальные данные в равной степени подтверждают многочисленные альтернативные толкования значительного улучшения эффективности боевых действий с применением информационных систем;
- выводы сторонников концепции сетецентрической войны базируются на непродуктивном принципе логического мышления, который называют индуктивизмом.

Некоторые критики сетецентрической концепции утверждали, что сетецентрическое видение, которое, возможно, приемлемо для ведения удаленных боевых действий на море и в воздухе, где нет таких сдерживающих препятствий как население и местность, слабо подходит к сухопутным боевым действиям с их неожиданностями и сложностями. Они ставят под сомнение эффективность сетецентрических операций и их уместность в ближним бою в городских условиях. Так, полковник сухопутных войск США Х.Р. Макмастер (H. R. Macmaster), например, приводил доводы, что ожидание информационного превосходства отвлекает от бесконечного многообразия ситуаций на поле боя, представляя ложный образ транспарентного поля боя [82, 85].

Аналитики отмечают, что в ходе операции «Анаконда» по уничтожению боевиков организации «Аль-Каиды» в Панджшерской долине, проведенной в марте 2002 г., разведка Пентагона, которая использовала новейшую беспилотную технику, космические разведывательные аппараты, радары, тепловизоры, средства радиоперехвата и радиоэлектронного подавления, вскрыла менее половины объектов и целей талибов. При этом талибы оказывали серьезное сопротивление и после массированных бомбежек, и после применения высокоточного оружия [82, 82].

Сложности использования концепции сетецентрической войны в тактическом звене управления сухопутных войск продемонстрировал и бой за овладение мостом через реку Евфрат в Ираке. Батальонной тактической группе была поставлена задача захватить мост и удерживать его до подхода основных сил, не давая противнику возможности разрушить его. Задачу ставили исходя из отсутствия какого-либо противника – полученные со спутника изображения показывали,

что мост без охраны. Однако доразведка, выполненная командиром группы, показала, что близлежащие улицы города, пальмовые заросли и оросительные каналы вокруг моста были буквально оккупированы иракскими войсками. Они скрывались в разветвленной сети траншей, бункеров и укрытий. От американских спутников и БПЛА они прятались, просчитывая режимы их полета и используя вполне обычные способы маскировки [121, 127].

Офицер разведотдела 3-й пехотной дивизии подполковник Ш. Уид подтвердил впоследствии, что замедление прохождения информации о противнике «сверху-вниз» чрезвычайно негативно сказывалось на оперативности принятия командирами тактического звена управления решений. В частности, он подчеркнул: «Для того чтобы получить свежие разведданные, нам приходилось останавливать движение вперед и с головой погружаться в массивы баз данных». Процесс подключения к общей базе данных мог занять несколько часов, а скорость передачи была настолько низкой, что порой командиры за время остановок даже не успевали скачивать необходимую им информацию. Приходилось втягиваться в бой вслепую [121, 127].

Когда сетецентрические действия ведутся против обычных войск, разведывательные системы передают информацию в систему принятия решений, выбирается имеющееся в наличии средство поражения и цель уничтожается. Однако когда противник прячется за стенами, зданиями, в подвалах, разведывательным системам обнаружить его практически невозможно. Отсюда очередной вывод, говорящий о невозможности использования разведывательной информации, а следовательно, и сетецентрической технологии управления в условиях города [121, 127].

Некоторые обозреватели отмечают, что американские войска во время войны в Ираке для вскрытия группировки войск и намерений противника выходили из укрытий и встречали его на местности, понимая, что эффективная разведка зачастую требует столкновения с противником в ближнем бою. Участники боевых действий в Ираке отмечали, что современные технические средства разведки не изменили этого условия и весной 2003 г., и в последующее время, во многих случаях не обеспечивали американские войска необходимыми сведениями о противнике. Следовательно, необходимо пересмотреть некоторые положения концепции сетецентрических операций и снизить значимость технических средств в обеспечении превосходства в войне. Значение огромных разведывательных ресурсов, таких как средства разработки и проведения эффективных военных операций,

переоценено, так как процесс принятия важных военных решений нельзя сводить только к анализу информации [121, 127].

Официальные представители министерства обороны заявили, что в обозримом будущем в операциях вооруженных сил США будут доминировать столкновения с иррегулярными вооруженными силами. Соответственно некоторые эксперты ставят под сомнение целесообразность применения сетецентрических операций в боевых действиях в городе и против повстанцев и задаются вопросом, не слишком ли большой упор в вооруженных силах США делается на высокие технологии. Так, в операциях в Афганистане и в боевых действиях в городах Ирака повстанцы смешивались с населением и могли близко подходить к американским войскам. Одна такая тактика могла свести на нет технологическое и военное преимущество превосходящих коалиционных сил [82].

Отдельные эксперты обращают внимание на явную невозможность сбора и анализа того объема информации, который необходим для того, чтобы сделать возможным ведение адекватной сетецентрической войны. Другие эксперты утверждают, что массовое включение сил и средств в единую сетецентрическую среду может породить проблемы с безопасностью информации [82].

Большинство экспертов сходятся в том, что техника может диктовать свои условия военной стратегии, и заявляют, что чрезмерная опора на высокие технологии может представлять новую уязвимость, которой воспользуются противники. Кроме того, они ставят вопросы:

- о совместимости информационных систем объединенных войск;
- о наличии достаточной емкости каналов связи и вычислительных ресурсов для создания адекватной информационной модели сетецентрической войны, а также о возможности оперирования гигантскими объемами информации в ходе ее ведения;
- о возможности непредвиденных последствий, когда организации полагаются на системы, зависимые от информации и т. д.

Например, заместитель директора Института по проблемам обороны США А. Кауфман считает, что технологии занимают слишком много места в американской военной стратегии, неправомерно навязывая ей свою логику. Опыт использования концепции сетецен-

трической войны в локальных войнах показал ряд ее проблемных аспектов. К числу главных из них относятся следующие [95]:

- переоценка способности человека адекватно перерабатывать большой объем противоречивой информации;
- недостаточный учет быстроменяющейся обстановки на поле боя;
- упрощенное видение противника и, в конечном итоге, – его недооценка;
- чрезмерная зависимость от информации;
- ускорение процесса боевого управления, поскольку «..скорость принятия решений не должна приобретать господствующей роли в ущерб человеческим факторам, лежащим в основе процесса управления войсками»;
- уязвимость боевой техники и программного обеспечения военного назначения от воздействия средств радиоэлектронной борьбы и информационного оружия.

В настоящее время практическое использование на пунктах управления технических решений для управления сетецентрической войной привело к перегрузке лиц, принимающих решения, информацией. Для решения этой проблемы в настоящее время специалисты Пентагона разрабатывают так называемые центры «слияния информации», в которых планируется применять специальное программное обеспечение в целях фильтрации данных о боевой обстановке и устранении той, которая в данный момент не нужна для ведения боевых действий [95].

Тот факт, что среди американских военных экспертов есть не только сторонники, но противники сетецентрической концепции отмечен в докладе исследовательской службы Конгресса США от 15 марта 2007 г. [82].

Критика концепции сетецентрической войны, звучала и со стороны противников ведения каких-либо боевых действий, тем более со стороны критически относящихся к военно-политическому доминированию США. Заместитель редактора международного издания «Eurasia Critic» Дж. Курдж в работе [243] отмечал, что «эта концепция используется в качестве политического дискурса для оправдания войны, презентуя войны как более гуманные, с меньшими жертвами среди гражданского населения из-за высокотехнологичного оружия, которое более точно, чем когда-либо. И как технологический лидер мира США являются предшественником в приспосабливании своей военной мощи в соответствии с принципами и идеалами сетецентрической войны для

того, чтобы удерживать свое военное превосходство. С другой стороны, концепция сетецентрической войны – это источник иллюзии для вооруженных сил и для общества. Как теоретическая конструкция эта концепция находится далеко от земной реальности и природы войны. Вера в то, что технология может решить все проблемы, которые поставлены противником, независимо от их тактики и природы, была, к сожалению, разрушена серьезной ситуацией в Ираке и Афганистане, когда обычные военные действия закончились. Поэтому концепция сетецентрической войны – это не революция в военном деле, которая изменяет самую сущность войны, а скорее множитель силы, который мог бы позволить государственному военному аппарату бороться эффективнее при условии, что доктрина и организация или вооруженные силы выстроены в соответствии с оценкой угрозы».

Вышеизложенные доводы критиков концепции сетецентрических войн подкрепляются обобщением опыта военных операций в Афганистане. Некоторые американские специалисты отмечают, что военные успехи в афганской кампании вовсе не должны делать из нее модель войны будущего «по-американски». Высокоточное оружие и новейшие технологии сами по себе не гарантируют победу. Как и прежде, война складывается из сочетания огневого поражения и маневра силами и средствами. Талибы не стали ждать расправы превосходящего противника, а быстро адаптировались к американским атакам. Всего через несколько дней они научились эффективно маскировать технику подручными средствами [82].

На основании анализа результатов последних войн сотрудники корпорации RAND (Research and Development – американский стратегический исследовательский центр) пришли к выводу, что «...по мере того, как удаленные средства становятся более совершенными, возникает вероятность того, что вооруженные силы потенциального противника будут развивать контртехнологии и становиться более подготовленными в вопросах организации защиты, оборудования укрытий, обмана и радиоэлектронной борьбы. С учетом всего этого сетевой эффект на самом деле превратится в уменьшение знания обстановки и, в конечном итоге, в снижение ситуационной осведомленности на поле боя» [95].

В целом, судя по материалам зарубежной печати, содержащим критические оценки концепции сетецентрической войны, отмечается, что вооруженные силы США готовы, в основном, воевать лишь с регулярной армией любого государства. Реальный же противник, как это показывает опыт партизанской войны в Афганистане и Ираке, оказы-

вается неявным, в том смысле, что он не имеет прямого отношения к государственным институтам и четко определяемой социальной базе, не является участником международных соглашений и организован по «сетевому» принципу. Такого противника нельзя победить только на поле боя, используя «сетецентрические» принципы управления группировками войск.

2.7.2. Основные уязвимости и противоречия концепции сетецентрической войны

Вышепредставленный анализ позволяет критически осмыслить концепцию сетецентрической войны и выделить ее основные уязвимости и диалектические противоречия, что было сделано в работах А.В. Копылова [82, 94]. Ниже представлены основные из них.

«Механистический взгляд» на природу войны. Сторонники концепции сетецентрических войн имеют свою точку зрения на природу войны, весьма отличную от взглядов Карла фон Клаузевица и других классиков военной мысли. Они твердо убеждены в том, что ходом войны можно управлять как работой хорошо сконструированной машины. Они считают, что в новую информационную эру классическая военная теория потеряла свое значение. Однако никакой технический прогресс, каким бы значительным он ни был, не может изменить истинную природу войны. К. Клаузевиц считал, что война никогда не является одномоментной и единой акцией, но представляет собой совокупность бесчисленных и взаимосвязанных явлений. Ее характер определяется природой человека, особенностями человеческого поведения во всей его сложности, физическими способностями и ограничениями человека.

Перенос моделей ведения бизнеса в военную сферу без их глубокого переосмысления и существенной переработки. Как известно, идеи ведения сетецентрических войн были заимствованы из сферы бизнеса. Министерство обороны США в свое время было очаровано организацией предпринимательской деятельности в американской компании розничной торговли. Будущие разработчики концепции «сетецентрических войн» оценивали эту компанию как самосинхронизирующуюся, рассредоточенную сеть магазинов, располагающую сведениями о происходящем движении товаров и торговых операциях в реальном масштабе времени. Вместе с тем бизнес-схемы не могут быть непосредственно применимы в военном деле, так как вооруженная борьба и бизнес, несмотря на некоторые сходные моменты, – это диа-

метрально противоположные сферы деятельности. Если в предпринимательской деятельности наиболее важным показателем является прибыль, то в вооруженной борьбе – боевая эффективность.

Бизнес-модели в неизменном виде невозможно использовать даже в материально-техническом обеспечении военных действий. Условия рынка и условия боевой обстановки различаются между собой. Ошибки в доставке или невозможность доставить определенные товары на рынок не вызовут потери в живой силе или разрушение материальных средств, в то время как недостаток горючего, боеприпасов или воды может привести к неудачам в вооруженной борьбе и большим потерям в живой силе.

Ряд экспертов отмечает, что количественные методы имеют ограничения при оценке боевой обстановки. В конечном итоге успех военных действий будет зависеть от решения, принятого командующим на основе его мнения и опыта. Используя модели предпринимательской деятельности без их критического переосмысления, в вооруженных силах США упустили из виду чрезвычайно важный вопрос об управлении войсками и о человеческом факторе в войне. Модели ведения бизнеса, возможно, допустимы в деятельности министерства обороны США и министерств видов вооруженных сил по планированию развития вооруженных сил, при разработке и приобретении вооружения и военной техники. Но прямое использование методов коммерческой деятельности в планировании ведения войны и в военных операций может привести к катастрофическим последствиям.

Ускорение процесса боевого управления. Апологеты концепции «сетецентрических войн» считают, что информационное превосходство приведет к превосходству в принятии решений и позволит проводить параллельные и непрерывные операции. С этим нельзя не согласиться. «Однако скорость принятия решений не должна приобретать господствующую роль в ущерб человеческим факторам, лежащим в основе процесса управления войсками», – говорят их оппоненты. Слишком большое внимание к скорости управления может привести к поспешным и непродуманным решениям. Выигранное при этом время должно быть использовано для наилучшего анализа информации и планирования.

Недооценка противника. Успех сетецентрической войны в значительной степени зависит от развертывания датчиков разведывательной системы для обнаружения движения и местоположения своих войск и войск противника. Однако в результате исследований, проведенных в 2002 г., сотрудники корпорации RAND пришли к выводу,

что если вооруженные силы потенциального противника будут эффективно развивать контртехнологии и становиться более подготовленными в вопросах организации маскировки, оборудования укрытий, военного обмана и радиоэлектронной борьбы, то эффекты от применения принципов сетецентрического ведения боевых действий могут сойти на нет.

Противники США в Ираке и Афганистане предпринимали действия, чтобы обойти американские сетецентрические датчики и снизить их эффективность за счет применения дешевых, но эффективных способов маскировки, а также новых способов иррегулярной войны. Примером этому может служить использование в террористических акциях смертников с минами замедленного действия, смешивание войск противника с местным населением, привлечение партизан и снайперов, которые, действуя на коротком расстоянии, наносили удары и затем быстро рассеивались.

По мнению специалистов из корпорации RAND, другими высокоэффективными способами борьбы с противником, ведущим сетецентрическую войну, могут быть: использование мощных устройств направленной энергии для подавления сигналов со спутников, применение малогабаритных устройств направленной энергии для того, чтобы на расстоянии вывести из строя элементы компьютерных схем, а также введение в информационную сеть вредоносных компьютерных программ с целью нарушения работы компьютеризированных систем управления оружием.

Ограниченные возможности против иррегулярных действий в условиях города. Когда сетецентрические действия ведутся против обычных войск, разведывательные датчики обнаруживают цель, передают информацию в систему принятия решений, выбирается имеющееся в наличии наиболее эффективное средство и цель поражается. Однако когда противник активно применяет маскировку, сетецентрическим датчикам будет трудно его обнаружить. Если противнику легче прятаться, чем войскам его находить, то войска становятся более уязвимыми. Более того, в таком случае информация о противнике не поступает в сетецентрическую систему и создается ложный эффект «отсутствия противника».

Чрезмерная зависимость от информации. Значение огромных информационных ресурсов как средства разработки и проведения эффективных военных операций может быть переоценено, как и то, что процесс принятия важных военных решений нельзя сводить только к мыслительному анализу информации. Ряд экспертов утверждают,

что дискуссии о трансформации вооруженных сил были чрезмерно сфокусированы на преимуществах, которые дает информация, и что виды вооруженных сил, органы обеспечения национальной безопасности и разведывательное сообщество не изучили, как следует риски, связанные с военной доктриной, в основе которой лежит информация. Ниже представлены некоторые проблемы, которые были подняты специалистами:

- опора на современные информационные системы может привести к необоснованной самоуверенности лиц, принимающих решения;
- количественные изменения в информации и ее анализе очень часто ведут к изменениям в поведении отдельных людей и организаций, которое иногда приводит к обратным результатам. Например, информационные технические средства позволяют обнаруживать большее количество целей, боеприпасы могут расходоваться быстрее, что ведет к большей зависимости от материально-технического обеспечения;
- обстановка, характеризующаяся обилием информации и возможностей, может изменить ценность информации, заставить пересмотреть цели военной миссии и, возможно, увеличить вероятность принятия ошибочных решений.

Невозможность эффективно работать с чрезмерным объемом информации. Высокая насыщенность поля боя разведывательными датчиками создала проблему «перегрузки информацией». Огромные потоки входящей информации могут ошеломить пользователей и создать угрозу для процесса принятия решения. В настоящее время ведутся разработки специального программного обеспечения для того, чтобы фильтровать информацию о боевой обстановке с целью отсеять ту ее часть, которая не нужна военнослужащим, ведущим боевые действия.

Увеличивающаяся сложность военных систем. Боевые системы и программное обеспечение становятся все более сложными. Программное обеспечение предназначено для обработки информации, определения положения противника и своих войск, комплекса целей, подачи сигнала тревоги, а также для координации и управления действиями экипажных и безэкипажных боевых средств на земле, на море и в воздухе.

Например, по оценкам специалистов, для работы перспективной боевой системы сухопутных войск потребуется 31 млн строк ко-

дов компьютерных программ. Кроме того, многие боевые системы, работающие с собственным оборудованием, в конце концов, будут объединены в сетевые системы. Однако по мере увеличения сложности компонентам сетевых систем придется обрабатывать информацию, получаемую от систем, возможности и надежность которых не всегда известны.

Вот что говорится о сложности компьютерных систем военного назначения в статье, изданной Институтом по разработке программного обеспечения К. Меллона (K. Mellon): «Когда говорят о современных метасистемах (системах систем), то их часто называют «неограниченными», потому что они охватывают неизвестное количество участников или, другими словами, требуют, чтобы отдельные участники действовали или взаимодействовали в условиях отсутствия необходимой информации. Для сложных метасистем, созданных сегодня, практически невозможно, чтобы человеческий или автоматизированный компонент обладали полным знанием состояния системы. При этом каждый компонент такой метасистемы должен зависеть от информации, полученной от других систем, возможности, цели и надежность которых неизвестны». В статье отмечается, что зачастую, когда возникает проблема совместимости в сложных системах, существует стремление достигнуть большей видимости, расширить управление из центра и предъявить более высокие критерии. Эти действия являются не только неэффективными, но и увеличивают вероятность технических аварий, ошибок пользователей и других отказов в работе. Обычные технические сбои вполне естественно возникают в сложных системах. При этом частота сбоев в работе увеличивается пропорционально количеству информационных связей в системе.

Уязвимость программного обеспечения и данных сетецентрической системы. Элементы физической инфраструктуры сетецентрической среды могут быть подвержены высокоэффективному информационно-техническому воздействию. Данное воздействие может быть направлено на блокировку критических информационных ресурсов, важных для проведения операции, ввод ложной информации в сетецентрическую среду, а также в базы данных, внедрения деструктивных программных средств, нарушающих нормальную работу вычислительных систем и средств связи. Кроме того, возможны сценарии ввода в сетецентрическую среду ложных источников информации, которые сформируют ложную ситуационную осведомленность и, в конечном итоге, навяжут противнику свою стратегию действий или полностью перехватят управление его силами и средствами.

Опыт боевых действий последних десятилетий показывает, что в настоящее время для тылового обеспечения действий войск и поддержки сложных боевых систем широко используются коммерческие электронные технические средства. Например, во время операции «Свобода Ираку» значимый в процентном отношении объем информации в интересах группировки западных стран передавался с помощью коммерческих спутников. В вооруженных силах США значительный объем административной информации проходит через гражданский сегмент сети Интернет. Такие общедоступные средства, используемые в военной сфере, могут стать основными объектами информационно-технического воздействия, так как зачастую не обладают высокоразвитыми средствами защиты, характерными для военных систем, являясь при этом важными элементами в сетецентрической среде.

Уязвимость боевой техники от воздействия средств радиоэлектронной борьбы. Высокотехнологические войска и средства оружия критичны к воздействию средств радиоэлектронной борьбы, в частности электромагнитного импульса, способного перегрузить или разрушить на расстоянии многочисленные электронные системы и высокотехнологичные средства, особенно чувствительные к такому воздействию. Уязвимость высокотехнологических систем оружия и связи, используемых в настоящее время в вооруженных силах технологически развитых государств, может побудить террористов, экстремистов и других вероятных противников к активному использованию средств радиоэлектронной борьбы.

Недостаточный учет слабоформализуемых факторов в психологической, культурной и религиозной сфере. Опыт последних военных конфликтов хорошо демонстрирует, что при ведении сетецентрической войны необходимо дополнительно учитывать множество тех факторов, которые в явном виде не могут быть зарегистрированы разведывательными датчиками и формализованы в рамках моделей боевых действий. Так, министр обороны США Р. Гейтс, выступая в Университете национальной обороны в сентябре 2008 г., заявил: «Никогда не игнорируйте психологическое, культурное, политическое и человеческое измерение войны, которое неизбежно имеет трагический, непроизводительный и неопределенный характер. Скептически относитесь к системному анализу, компьютерному моделированию, теориям игр, иначе говоря, доктринам, которые проповедуют противоположные идеи».

Таким образом, к анализу и оценке концепции сетецентрических войн необходимо подходить критически, учитывая как сильные, так и слабые ее стороны. При всей противоречивости взглядов на теорию и практику сетецентрических войн следует отметить, что ее основные положения реализуются в строительстве вооруженных сил США и других технически развитых государств, нашли отражение в оперативных концепциях, боевых уставах и наставлениях и показали свою эффективность в боевых операциях в Ираке, Афганистане, Ливии и Сирии [82].

Вместе с тем теория и практика сетецентрических войн содержит в себе и слабые стороны. Знание слабых сторон этой концепции позволяет выявить уязвимые места высокотехнологичного вероятного противника, ведущего военные действия на основе этой концепции, с тем, чтобы снизить его военно-информационный потенциал, наиболее эффективно применить свои силы и средства вооруженной борьбы и обеспечить достижение целей операций объединенных группировок войск [82].

2.7.2. Возможности ассиметричного противодействия в сетецентрической войне

Глобальное лидерство в экономической, технологической и военной сферах и широкое внедрение в практику вооруженных сил концепции сетецентрической войны заставляют страны и негосударственные субъекты искать новые асимметричные стратегии и тактики ведения вооруженной борьбы, которые позволили бы противостоять заведомо более сильному противнику, ведущему войну на основе сетецентрической концепции.

В настоящее время в вооруженных силах ведущих зарубежных стран «второго эшелона» (Китай, Индия, Пакистан, Иран) резко актуализированы исследования, посвященные возможным асимметричным действиям против современных высокотехнологических армий (прежде всего, США, а также, отчасти, некоторых западноевропейских стран), поскольку стало очевидным, что противостоять им на равных в симметричном военном конфликте с использованием обычных вооружений не представляется возможным [2].

Интересно то, что поиск асимметричных действий (тактики и стратегии) также актуален как для самих США, занимающих позицию бесспорного лидера, так и для государств, имеющих менее технологически оснащенные армии. Это связано с необходимостью превентив-

ного поиска мер, направленных на устранение уязвимостей сетецентрической концепции, и недопущению использования против своих сил и средств асимметричных способов противостояния. Отправной точкой пристального внимания к асимметричным действиям в вооруженных конфликтах служит понимание того обстоятельства, что превосходящая сторона, обладающая значительной военной мощью, еще не может гарантировать обеспечение абсолютной безопасности своей страны [2, 95].

Согласно определению Института национальных стратегических исследований Национального университета обороны США, под «асимметричными» угрозами понимаются «использование фактора неожиданности во всех его оперативных и стратегических измерениях, а также использование оружия такими способами, которые не планируются США» [2].

В соответствии с работой [16] асимметричный подход применительно к сфере национальной безопасности и обороны заключается в реализации собственной стратегии действий, отличных от реализуемых и навязываемых потенциальным противником. Реализация данного подхода позволяет добиться конкретных преимуществ, использовать уязвимые места противника, завоевать инициативу и достичь большей свободы действий.

В работе [203] указывается, что в основе асимметричного подхода лежит навязывание противнику боевых действий в таких условиях, в которых сложно реализовать свое техническое преимущество, например расширении географических границ и длительности конфликта, выборе объектов нападения с учетом не их военного значения, а воздействия на моральное состояние личного состава и гражданского населения противника, при провоцировании несоразмерного применения силы, при активном ведении информационной борьбы. Возможны попытки компенсировать техническое отставание за счет напряжения всех материальных и духовных сил нации, придания войне тотального характера. В технической сфере данный подход выражается в уничтожении личного состава, а также в выводе из строя дорогостоящих и сложных систем вооружения при помощи более дешевых средств. В политическом плане более слабые субъекты будут пытаться балансировать на грани войны и мира, инициировать различные переговоры с целью затягивания времени, а также пытаться заручиться поддержкой авторитетных членов международного сообщества.

В работе [29] указывается, что сущность асимметричного подхода заключается в уходе одной из сторон (стороны, не имеющей до-

статочного количества ресурсов – производственных, интеллектуальных, научных, технологических и т.п.) от фронтального противостояния к концентрации усилий в областях, где удалось выявить уязвимость и слабость в вооружении и организации потенциального противника.

Таким образом, асимметричное противодействие является достаточно рискованным, но тем не менее, единственно возможным эффективным ответом на действия высокотехнологической армии, ведущей войну в соответствии с сетецентрической концепцией [29].

Асимметричный подход может быть как пассивным, так и активным.

К пассивной асимметрии относятся способы военно-технологического развития, которые осуществляются, на первый взгляд, параллельно мировым тенденциям, но за счет отказа от части технологий и концентрации усилий и ресурсов на тех из них, где появляется возможность сократить отставание [29].

Суть активного способа военно-технической асимметрии заключается в формировании развития технологий, направленных на создание оружия, способного либо уничтожать, либо подавлять наиболее опасные средства вооруженной борьбы потенциального противника [29].

Уровень, на котором могут быть реализованы асимметричные угрозы в военном конфликте, может варьироваться от тактического до стратегического, а по временным параметрам угрозы могут быть кратковременными и долгосрочными [95].

Асимметричные угрозы характеризуются значительной степенью неопределенности в отношении потенциальных источников военных и других угроз, форм и способов ведения вооруженной борьбы в будущем [95].

К асимметричным угрозам относят [95]:

- угрозу терроризма;
- информационное противоборство во всех его проявлениях;
- провоцирование несоразмерного применения силы;
- навязывание противником боевых действий в условиях, когда соединениям, частям и подразделениям технологически развитой армии сложно реализовать свое техническое преимущество;
- выбор объектов нападения с учетом воздействия на моральное состояние войск и населения;

- использование противником новых, в том числе инновационных, технологий и средств вооруженной борьбы;
- применение оружия массового поражения.

Такие угрозы способны нейтрализовать или существенно ослабить военные возможности технологически развитого государства и его армии.

В табл. 2.7 и 2.8 приведены уровни относительной опасности и вероятности асимметричных угроз для технологически развитой армии (на примере вооруженных сил США) по данным из работ [95, 179]

Таблица 2.7. Относительные опасность и вероятность асимметричных угроз для технологически развитой армии [95, 179]

Угроза	**Относительная опасность**	**Относительная вероятность**
Использование ядерного или биологического оружия на территории государства	Высшая	Высокая
Наступательные информационные операции против государства	Средняя	Высшая
Применение химического или биологического оружия против воинских группировок на удаленном театре военных действий либо на своей территории	Высокая	Высокая
Использование оружия массового поражения против системы стратегических переброс войск	Высокая	Высокая
Информационная атака (в том числе с применением электромагнитного импульса) против подразделений вооруженных сил	Высокая	Средняя
Принуждение к ведению военных действий в городских условиях, джунглях, горной и другой неблагоприятной местности	Высокая	Высокая
Воспрещение/затруднение стратегических переброс путем применения обычного вооружения	Средняя	Высокая
Новые неожиданные тактические приемы и способы боевого применения сил	Средняя	Высокая
Применение химического оружия на территории государства	Низкая	Средняя

Таблица 2.8. Вероятность использования асимметричных средств государствами или негосударственными субъектами на различных этапах конфликта [95]

Вероятные противники	Средства, приемы и способы	Вероятность использования				
		В мирный период	В период кризиса	При развертывании группировок вооруженных сил	При ведении военных действий	После завершения военного конфликта
Государства	ядерное оружие	наименьшая	наименьшая	высокая	низкая	наиболее высокая
	химическое оружие	наименьшая	низкая	наиболее высокая	высокая	низкая
	биологическое оружие	наименьшая	низкая	наиболее высокая	низкая	высокая
	информационное воздействие	высокая	наиболее высокая	высокая	высокая	высокая
	новые тактические приемы и способы боевого применения	-	-	высокая	наиболее высокая	низкая
	терроризм	высокая	наиболее высокая	высокая	высокая	высокая
Негосударственные субъекты	ядерное оружие	наименьшая	низкая	наиболее высокая	высокая	высокая
	химическое оружие	наименьшая	низкая	наиболее высокая	высокая	высокая
	биологическое оружие	наименьшая	низкая	наиболее высокая	высокая	высокая
	информационное воздействие	наиболее высокая	высокая	высокая	высокая	высокая
	новые тактические приемы и способы боевого применения	-	низкая	высокая	наиболее высокая	низкая
	терроризм	высокая	наиболее высокая	высокая	высокая	низкая

В работах [95, 179] утверждается, что особую опасность для технологически развитых вооруженных сил асимметричные угрозы будут представлять в период стратегических переброс войск (сил), поскольку вся система передислокации обладает уязвимыми звеньями. К ним в первую очередь относят воздушные, морские и сухопутные линии и узлы коммуникаций, а также гражданскую инфраструктуру переброс. В качестве мер по противодействию угрозам подобного рода предусматриваются превентивные наступательные действия, присутствие сил в удаленных районах, совершенствование системы защиты от оружия массового поражения и системы стратегических

переброс, повышение мобильности сил, развитие амфибийно-десантных структур и оборонительных систем, в том числе национальной ПВО и ПРО на ТВД.

В значительной мере росту асимметричных угроз национальной безопасности способствуют широкое распространение и доступность не только и не столько современных технологий, сколько уже готовых технологий двойного назначения, которые можно использовать в военных целях.

Таблица 2.9. Асимметричное противодействие стратегическому развертыванию технологически развитых вооруженных сил [95, 179]

Фазы развертывания	**Возможные объекты воздействия**	**Цель мероприятий**
Подготовка к развертыванию	Центры дислокации боевых подразделений, система обеспечения сил, стационарные пункты управления, гражданские структуры	Устрашение, подрыв единства коалиции
Переброска сил	Средства воздушных, морских и сухопутных стратегических перевозок, линии и узлы коммуникаций – порты погрузки и выгрузки, склады, пункты дислокации и др.	Срыв / затруднение развертывания, снижение темпов переброски
Развертывание в районе кризиса (конфликта)	Компоненты объединенных сил, критически важные элементы инфраструктуры обеспечения сил	Противодействие вторжению

Как показал анализ, проведенный в работе [16], большинство прорывных военных технологий последнего времени, которые используются для модернизации вооруженных сил ведущих зарубежных стран, являются коммерческими и двойными технологиями, а не результатами военных исследований.

К числу основных факторов, определяющих широкое внедрение технологий двойного назначения, можно отнести [16]:

- высокую стоимость военных разработок, при этом их функционал, как правило, дублирует коммерческие продукты;
- невозможность столь же масштабного, как в гражданском секторе, привлечения средств и специалистов к таким разработкам и исследованиям;

- трудности в использовании зарубежных прорывных разработок и привлечении иностранных специалистов к исследованиям;
- высокая конкуренция на рынке вооружений, обусловливающая необходимость снижения стоимости конечного продукта без потери его функциональности.

Однако потенциальная эффективность использования двойных и коммерческих технологий может стать для военных причиной ряда серьезных проблем, поскольку при этом повышается уязвимость систем вооружения [16].

Во-первых, использование коммерческих технологий в военном деле означает, что они будут применяться и в гражданской сфере. При этом документация и модернизированные образцы в гражданской сфере станут доступны раньше, чем они будут внедрены в производство вооружений. Таким образом, существует возможность, что потенциальный противник также получит доступ к новейшим разработкам. Это актуализирует вопросы не только создания, но и использования новых технологий применительно к военным задачам.

Во-вторых, двойное использование коммерческих продуктов ведет к тому, что военные и гражданские пользователи обладают практически идентичными системами. Это создает следующее противоречие. С одной стороны, коммерческие системы разработаны для эксплуатации в гораздо более благоприятных условиях, чем военные, с другой – потенциальный противник имеет доступ к этим технологиям и способен (хотя бы потенциально) создавать аналогичные системы, а также разрабатывать методы борьбы с ними.

В-третьих, любые государства, политические движения и даже отдельные личности в состоянии приобрести эти технологии, минуя продолжительные и дорогостоящие стадии исследований, разработки, производства, опытной эксплуатации и даже не используя промышленный шпионаж.

К числу таких доступных технологий двойного назначения можно отнести информационное оружие, ориентированное на деструктивное воздействие на телекоммуникационную инфоструктуру, на автоматизированные системы управления и на информационные потоки, циркулирующие в них.

Быстрое внедрение перспективных информационных технологий делает возможным неожиданное появление мощного асимметричного информационного оружия у широкого круга потенциальных противников технологически развитых стран. При этом ожидается, что

уровень интенсивности его применения и информационных операций, проводимых противником и в мирное время, повысится с эскалацией кризисной ситуации [16].

При подготовке войны в Ираке администрация США приняла ряд документов, среди которых директивы в интересах обеспечения внутренней безопасности: «Национальная стратегия борьбы с терроризмом» (The National Strategy for Combating Terrorism); «Национальная стратегия по защите киберпространства» (The National Strategy to Secure Cyberspace); «Национальная стратегия физической защиты критической инфраструктуры» (The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets). В них впервые получила официальное признание «полная зависимость инфраструктуры США от информационных систем и сетей» и уязвимость последних [95].

Сделав ставку на высокую компьютеризацию национальных вооруженных сил и ведение сетецентрических войн, Пентагон (The Pentagon) стал испытывать все более мощное давление как со стороны своих потенциальных (таких, например, как Китай), так и действующих (международные террористические организации) противников. Испытав за последние годы несколько достаточно мощных атак на свои компьютерные сети и серверы, руководство Пентагона, оказавшись перед новой угрозой, поручило стратегическому командованию разработать для всех правила и способы ведения кибервойны, а также взять на себя на начальном этапе подготовку специалистов в этой области. В результате в 2008 г. была принята «Национальная военная стратегия по ведению операций в киберпространстве». Главная особенность этого документа состоит в том, что впервые в нем речь идет о переходе от защиты собственных информационных ресурсов и сетей к наступательным операциям в киберпространстве. В целях достижения этой цели предполагается использовать весь спектр сил и средств, в том числе беспилотные летательные аппараты, способные среди прочих задач выводить из строя электрические и энергетические системы [95].

Комментируя этот документ, командующий стратегическим командованием вооруженных сил США в своем выступлении подчеркнул: «Для того чтобы реализовать это намерение, каждый вид наших вооруженных сил должен нанять и дополнительно подготовить достаточное количество квалифицированного персонала, подготовленного к кибервойнам» [95].

В июне 2009 г. министр обороны Соединенных Штатов Р. Гейтс (Robert Michael Gates) объявил о создании (в соответствии с указанием президента) в вооруженных силах страны принципиально новой структуры – Объединенного кибернетического командования United States Cyber Command – (USCYBERCOM). Оно ориентировано на организацию и проведение масштабных наступательных и оборонительных боевых действий в кибернетическом пространстве [95].

Еще одним эффективным средством асимметричного противодействия системе управления и высокотехнологическому вооружению выступает радиоэлектронная борьба, являющаяся видом оперативного (боевого) обеспечения войск (сил).

Под РЭБ (в соответствии с руководящими документами ВС США) понимается совокупность взаимосвязанных по цели, задачам, месту и времени мероприятий и действий войск по выявлению систем и средств управления войсками и оружием противника, их ядерному, огневому поражению, захвату и радиоэлектронному подавлению, а также по радиоэлектронной защите своих систем и средств управления войсками и оружием и противодействию техническим средствам разведки противника [29].

Задачами, которые решаются РЭБ в интересах асимметричного воздействия, могут быть [29]:

- срыв и дезорганизация управления войсками и оружием противника;
- снижение эффективности разведки, а также применения оружия и боевой техники;
- обеспечение устойчивости работы систем и средств управления своими войсками и оружием.

При этом РЭБ включает в себя следующие мероприятия такие как [29]:

1. Радиоэлектронная защита – защита от радиоэлектронного подавления; обеспечение электромагнитной совместимости; защита от самонаводящегося на излучение оружие; защита от ионизирующего излучения и электромагнитного импульса.
2. Радиоэлектронное противодействие – радиоподавление; оптико-электронное подавление; гидроакустическое подавление; радиодезинформация; радиоимитация.
3. Радиоэлектронное обеспечение – поиск, перехват и анализ излучений; опознавание и определение местонахождения радиоэлектронных средств (РЭС) противника; оценка со-

здаваемой ими угрозы для последующего подавления и выдачи целеуказания средствам поражения; управление своими силами. При этом радиоэлектронное обеспечение включает в себя [29]:

- радиоэлектронную разведку (радиоразведку, радиотехническую разведку, радиолокационную разведку);
- оптическую разведку (фоторазведку, оптико-электронную разведку, тепловизионную разведку, инфракрасную разведку, лазерную разведку);
- акустическую разведку;
- гидроакустическую разведку;
- сейсмическую разведку;
- радиационную разведку.

Система РЭБ с методологической точки зрения позволяет практически организовать срыв любой военной операции (при условии наличия технических средств РЭБ) [29].

При наличии у противодействующей стороны средств ВТО возможны два варианта воздействия на системы управления и связи технически развитого противника.

Физический способ. Независимо от предназначения АСУ есть каналы радиосвязи для передачи или приема информации, сбора разведданных и т.д. По запеленгованному источнику производится наведение ВТО, например крылатых ракет воздушного или морского базирования со спутниковой (или инерциальной) навигационной системой наведения, а на конечном участке – с использованием пассивной (радиолокационной или инфракрасной) головки самонаведения (ГСН). В случае режима радиомолчания уничтожение пунктов управления производится ВТО через спутниковую систему навигации, связи и управления с возможным использованием инфракрасной ГСН [29].

Вторым способом является использование комплексов РЭБ. Дислокация пунктов управления всех АСУ вероятного противника может быть заранее выявлена и для вывода из строя или хотя бы временного снижения эффективности функционирования АСУ противника требуется согласованное по времени, пространству и целям массированное воздействие средствами РЭБ на многочисленные взаимоувязанные средства сете- и каналообразования системы управления, приводящее к разрушению системы связи. Именно этот способ наиболее эффективен в большинстве случаев [29].

К числу асимметричных способов противодействия ВТО высокотехнологичного противника можно отнести использование систем

ПРО, а также вывод из строя спутниковой системы навигации и наведения вероятного противника [29].

В рамках подготовки к асимметричному противодействию технологически развитому противнику можно выделить следующие общие пути [29]:

- недопустимость прямого соперничества в создании и развертывании систем и комплексов вооружения, ориентацию на асимметричные средства вооруженного противостояния в ответ на дорогостоящие средства потенциального противника;
- обеспечение противодействия применению ВТО за счет создания интегрированных комплексов ПВО-ПРО;
- создание интегрированных систем и средств разведки, управления и связи, РЭБ и других видов обеспечения в целях организации оперативного взаимодействия разнородных и разноведомственных сил;
- наращивание сил и средств информационных операций в информационно-психологической и информационно-технической сферах.

Нельзя забывать, что асимметричный подход является вынужденной мерой. Безусловно, идя на асимметричные действия надо самым активным образом развивать технологии в широком спектре (хотя бы на уровне фундаментальных и прикладных НИР), виды вооружения и военной техники, связанные с подготовкой к сетецентрическим войнам 6-го поколения.

3. Изменение подходов к строительству Вооруженных сил в условиях внедрения концепции сетецентрической войны

После того, как в вооруженных силах США начала внедряться концепция сетецентрической войны, другие государства также начали искать преимущества в этой модели. Для обозначения данной концепции применяются различные термины (рис. 3.1). НАТО также реформирует свои вооруженные силы в соответствии с принципами сетецентрической войны. В марте 2010 г. начальник ГШ ВС РФ Н.Е. Макаров озвучил, что Россия тоже будет переходить на модель сетецентрического управления войсками и ведения боевых действий. При этом данный принцип управления в ВС РФ получил наименование «Боевые действия в едином информационном пространстве».

Рис. 3.1. Концепции сетецентрических войн, разрабатываемые научными школами ведущих зарубежных стран

С конца 90-х гг. в США и в странах их союзников по идеям и практической реализации концепции сетецентрических войн были посвящены сотни монографий, исследований и статей. Сетецентрическим войнам было посвящено специальное послание Конгрессу США в июле 2001 г. Военно-политические круги США постоянно развивают

эту концепцию, при этом помимо военных организаций в процессе развития концепции принимают участие неправительственные организации, коммерческие структуры и гуманитарные университеты [239].

Стратегическое видение войн будущего военно-политическим руководством США в соответствии с развитием сетецентрической концепции постоянно меняется. Как указано из источников отечественных исследований, США подразделяют своих вероятных противников [239, 240]:

- на державы и военно-политические блоки, вооруженные силы которых способны в полном объеме реализовать передовые военные научно-технические достижения, в том числе основанные на концепции сетецентрических войн;
- на государства, вооруженные силы которых способны частично реализовать передовой военный научно-технический потенциал;
- на неядерные страны с незначительным военным потенциалом;
- на страны, обладающие ядерным оружием сдерживания (устрашения);
- на негосударственные образования, ставящие перед собой ограниченные военно-политические цели и обладающие определенными возможностями для их достижения.

Следовательно, традиционная война вытесняется новой, сетецентрической войной с широким использованием операций, основанных на эффектах информационного противоборства и мобильных боевых подразделений. На ее гибкой основе и формируются текущие задачи военно-промышленного комплекса США, разведсообщества и различных оборонных структур.

Анализ тенденций изменения структуры управления, обеспечения информационной интеграции сил и средств, повышение уровня взаимодействия, а также нацеленность на достижение синергетического эффекта за счет реализации принципов сетецентрической войны становится все более актуальным и приоритетным направлением реформирования вооруженных сил большинства ведущих зарубежных стран и, вероятнее всего, к 2020 г. их вооруженные силы полностью перейдут от централизованно-иерархического к сетецентрическому управлению. Это позволит им обеспечить новые боевые возможности за счет объединения разнообразных боевых платформ в единое информационно-коммуникационное пространство.

При этом в экспертной среде научных школ различных стран существуют различные взгляды на концепцию сетецентрических войн. Например, в работе [43] указывается, что ряд экспертов считают новые сетецентрические принципы управления предназначенными для ведения глобальных войн с управлением из единого центра, а интеграция всех участников боевых действий в единую сеть – это только фантастическая и несбыточная концепция применения группировок «роев» роботов. Другие – что формирование единой (для всех уровней) картины ситуационной осведомленности не нужно боевым формированиям тактического звена, потому что им нужна только тактическая (локальная) информация и т.д.

Основные тенденции изменения принципов строительства вооруженных сил с учетом концепции сетецентрической войны рассмотрены на примере США и дополнены кратким анализом тенденций в вооруженных силах других ведущих зарубежных стран.

3.1. Вооруженные силы США

Начиная с 1990-х гг. XX века, военно-политическим командованием США ведутся мероприятия по внедрению концепции сетецентрической войны в систему управления войсками и силами. Главным принципом этих мероприятий можно считать обеспечение реальной вертикальной и горизонтальной информационной интеграции всех участников боевых действий, а также средств вооружения [43].

3.1.1. Анализ военно-доктринальных документов, стратегических задач и основных тенденций строительства вооруженных сил

Анализ военно-доктринальных документов свидетельствует о том, что военно-политическое руководство США возлагает на свои вооруженные силы решение следующих основных задач [95]:

- сдерживание вероятных противников от создания угроз интересам США, а в случае нападения на США или на их союзников – нанесение им решительного поражения путем коллективных действий под американским руководством;
- осуществление передового присутствия в ключевых регионах мира в целях защиты там американских интересов и

демонстрации готовности США выполнять свои обязательства перед союзниками;

- проведение операций ограниченного масштаба для решения миротворческих задач, эвакуации американских граждан из районов конфликтов, оказания гуманитарной помощи и др.

В стратегии национальной обороны США прямо подчеркивается, что одновременно с обеспечением надежной обороны страны ее вооруженные силы должны иметь возможности для проведения четырех операций сдерживания, двух крупных военных кампаний, одна из которых должна завершиться молниеносной и результативной победой, а также серии менее масштабных специальных операций. Таким образом, политика в области строительства вооруженных сил США в базируется на трех основных положениях [95].

1. Строительство вооруженных сил США должно быть сконцентрировано на решении задач по обеспечению защиты территории США.
2. При планировании строительства вооруженных сил США их структура оптимизируется для участия в двух практически совпадающих по времени крупномасштабных военных конфликтах на различных театрах военных действий (например, Северо-Восточная и Юго-Западная Азия), а также для формирования широкого спектра боевых возможностей вооруженных сил и активного проведения политики передового присутствия.
3. Вооруженные силы США должны быть готовы одновременно с крупномасштабными операциями дополнительно проводить во взаимодействии с союзниками несколько операций меньшего масштаба.

Для обеспечения выполнения первого положения сформировано новое объединенное командование вооруженных сил США в Северной Америке, в зону ответственности которого входят территории США, Канады, Мексики, ряда стран Карибского бассейна и акватории прилегающих морей и океанов в пределах 500-мильной зоны. В соответствии с Единой оперативной концепцией министерства обороны США по обеспечению внутренней безопасности, военному ведомству предписано решение ряда задач по оказанию содействия гражданским властям на территории США и за ее пределами силовыми методами, в том числе превентивного характера [95].

При выполнении второго положения министерство обороны США планирует сконцентрировать внимание на решении задач передового сдерживания в ключевых для американских интересов регионах мира: в Европе, Северо-Восточной Азии, прибрежных районах Восточной Азии, а также на Ближнем Востоке и в Юго-Западной Азии. При этом Пентагон планирует осуществлять строительство своих вооруженных сил с ориентацией на «...быстрое отражение агрессии в нескольких практически совпадающих по времени крупномасштабных вооруженных конфликтах, сохраняя при этом способность по приказу президента страны нанести решительное поражение противнику в одном из них, включая создание условий для оккупации его территории или смены правящего режима» [95].

При обеспечении выполнения третьего положения в соответствии с заключениями американских экспертов считается, что потенциальный региональный противник в крупномасштабном военном конфликте может иметь группировку вооруженных сил, включающую 400-750 тыс. человек личного состава, 2-3 тыс. танков, 2-3 тыс. артиллерийских систем, 500-1000 боевых самолетов, 100-200 боевых кораблей, в том числе до 50 подводных лодок, 100-1000 баллистических ракет оперативно-тактического и тактического назначения [95].

Аналитики Пентагона считают, что операции оперативного уровня в ходе регионального военного конфликта могут иметь четыре этапа:

- сдерживание сил вторжения, отражение наступления противника;
- наращивание боевой мощи в зоне конфликта, ведение боевых действий в основном военно-воздушными и военно-морскими силами, решительный разгром противника;
- обеспечение послевоенной стабильности.

При этом в соответствии с концепцией «Победа – сдерживание – победа» вооруженные силы должны одержать победу в ходе первого этапа, в начальной фазе второго этапа осуществить сдерживающие действия и в последующем также одержать победу. Упомянутая концепция в условиях перехода к сетецентрическим войнам трансформирована в новую концепцию, получившую название «10-30-30» (иногда ее называют «Доктрина Рамсфелда» по имени автора – бывшего министра обороны) [95].

Суть концепции «10-30-30» заключается в том, что после принятия политического решения на применение военной силы войска должны быть в течение 10 дней приведены в боевую готовность и

осуществить перегруппировку в любую точку земного шара, за последующие 30 дней разгромить главные силы противника и лишить его возможности возобновить организованное сопротивление в обозримом будущем, а затем в течение 30 дней восстановить боеспособность и быть готовыми к выполнению новой боевой задачи и переброске в другой регион. Таким образом, положения этой концепции отводят на одну войну 2 месяца и 10 дней, что теоретически позволяет военно-политическому руководству США, опираясь на сеть, состоящую из более 700 мобильных баз по всей планете (рис. 3.2), проводить ежегодно как минимум пять полноценных боевых операций или так называемых экспедиционных войн. При этом ядерное оружие рассматривается в качестве оружия поля боя и становится обычным средством вооруженной борьбы [95].

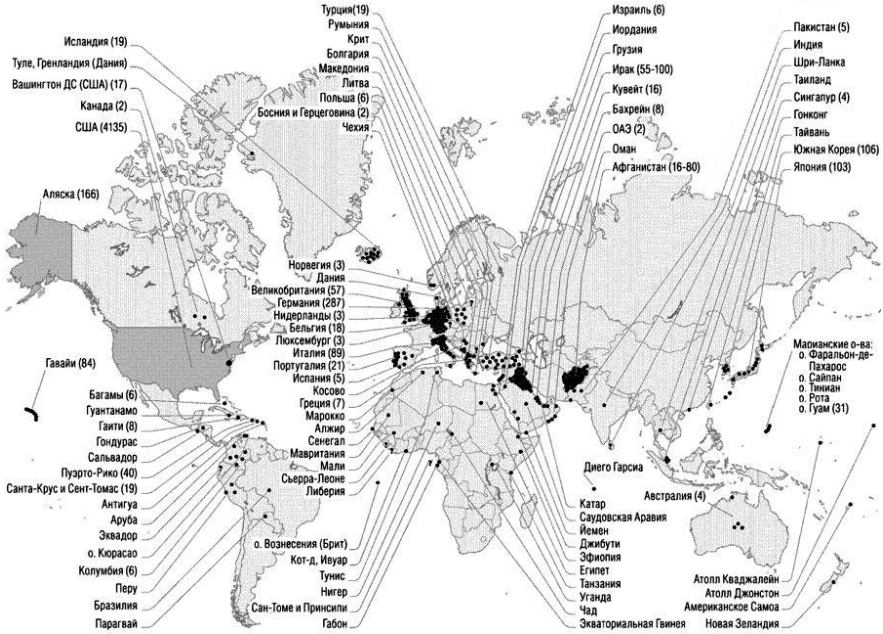


Рис. 3.2. Расположение военных баз ВС США

Всесторонне анализируя характер возможных региональных конфликтов, американское руководство пришло к выводу, что в одном конфликте может принимать участие группировка войск, включающая 5-6 дивизий сухопутных войск, 4-5 авианосных ударных групп, 4-6 бригад морской пехоты, до 10 крыльев тактической авиации, подраз-

деления сил специальных операций, силы и средства боевого обеспечения [95].

Вариант применения ядерного оружия в ходе регионального конфликта вполне вероятен. В оперативно-стратегической концепции «Крупномасштабные военные операции» аналитиками сформулированы базовые принципы и направления строительства вооруженных сил, всестороннего военного превосходства США над любым противником с учетом прогноза развития военно-политической обстановки в различных районах мира. В этом документе определено, что «к крупномасштабным относятся операции против государств или группы государств региона, располагающих значительным военным потенциалом, определенными возможностями по глобальному размаху ведения боевых действий и угрожающих территории и национальной безопасности США». В концепции раскрываются понятия трех основных типов крупномасштабных военных действий – расширенной кампании, ограниченной кампании и одиночной операции. [95].

Расширенная кампания представляет собой боевые действия в нескольких операционных районах в целях нанесения решительного поражения противнику. Такую операцию предполагается вести в случае, если усилия по сдерживанию и меры по нераспространению кризиса окажутся неэффективными.

Основными военными задачами кампании станут [95]:

- нейтрализация сил и средств противника, препятствующих вторжению;
- нарушение работы его систем боевого управления, связи и разведки;
- организация ПВО и ПРО для защиты своих войск и военных объектов;
- завоевание господства в воздухе, на суше и на море с последующим переходом к операции по стабилизации обстановки.

Ограниченная кампания отличается от расширенной меньшими масштабами и продолжительностью. Цели, задачи и характер военных действий в ходе обеих кампаний в основном совпадают – по разработанным планам и сценариям за силовым вторжением следует динамичная «воздушно-наземно-морская наступательная операция».

Расширенная и ограниченная кампании будут начинаться с проведения активной наступательной информационной операции, введения экономических санкций против противника, принятия мер дипломатического характера и создания коалиции под эгидой США.

Одиночная операция является еще более ограниченной по своим масштабам, продолжительности и целям. Ее отличительные характеристики – оперативность, внезапность и переброска войск непосредственно в районы боевых действий путем высадки морских и воздушных десантов.

Указанная оперативно-стратегическая концепция «Крупномасштабные военные операции» разрабатывалась на основе документов министерства обороны («Стратегии национальной обороны» (National Defense Strategy) и «Национальная военная стратегия» (National Military Strategy)) и является базовым документом в серии новых «оперативно-стратегических концепций единых сил» [95].

Одним из таких вновь разработанных документов является концепция «Операция по стабилизации обстановки». Она отражает взгляды военного руководства США на задачи, условия и способы применения американских вооруженных сил для приведения к власти или поддержки лояльных США правящих режимов, а также для обеспечения беспрепятственного продвижения своих национальных интересов.

Основными задачами операции в концепции «Операция по стабилизации обстановки» определены [95]:

- оказание поддержки войскам, ведущим боевые действия;
- установление и поддержание условий для восстановления правопорядка и обеспечения безопасности, как коалиционной группировки войск, так и сочувствующих американцам слоев местного населения;
- организация примирения местных или региональных военных и политических лидеров;
- восстановление социальной и экономической инфраструктуры;
- содействие передаче власти проамерикански настроенным властным структурам.

Концепция «Операция по стабилизации обстановки» допускает четыре варианта развития обстановки, при которых допускается привлечение американских или коалиционных войск для ее стабилизации [95].

1. Правительство союзного или дружественного государства обращается к США или странам коалиции за помощью в случае государственного переворота, восстания или массовых беспорядков.

2. Недружественное государство угрожает жизненно важным интересам США и их союзников в регионе или применяет насилие в отношении собственного населения.
3. Государство выходит из-под контроля США, становится неуправляемым, терпит экономический крах и распадается на отдельные части, власть в которых переходит к самопровозглашенным лидерам и вооруженным формированиям.
4. Деятельность национальной или транснациональной организации, которая серьезно нарушает права человека в какой-либо стране, разрушает жизненный уклад широких слоев населения и дестабилизирует работу законного правительства.

При проведении операций по стабилизации обстановки планируется использовать три основных способа действий [95]:

1. принуждение;
2. пропаганда;
3. стимулирование.

Принудительные действия предполагается предпринимать в форме боевых операций, засад и рейдов против террористов, ликвидации каналов снабжения боевиков продовольствием, замораживания банковских счетов политических и военных лидеров, отказывающихся сотрудничать с американцами. Под пропагандой подразумевается проведение психологических и информационных операций, направленных на убеждение местных лидеров и населения в том, что нормальная мирная жизнь может быть налажена только при тесном сотрудничестве с США. Стимулирование предполагает политические, финансовые и другие виды поощрений в целях установления отношений сотрудничества с местными лидерами [95].

По окончании активного этапа операции приоритетными стабилизационными мероприятиями должны стать [95]:

- полное восстановление правопорядка;
- оказание гуманитарной помощи населению;
- формирование лояльных США новых гражданских властей;
- налаживание работы коммунальных служб, энергоснабжения, неотложной медицинской помощи.

Предполагается, что группировки вооруженных сил США будут содержаться в странах до тех пор, пока условия обстановки не позволят передать эти функции местным органам власти.

Реализация планов по реконфигурации военного присутствия за пределами США изложена в специальной программе «Единая стратегия глобального присутствия и базирования», которая является составной частью военной стратегии и охватывает Западную и Восточную Европу, Ближний Восток, Азиатско-Тихоокеанский регион и Африку. В соответствии с этой программой вооруженные силы США на территории зарубежных государств планируют иметь (с учетом существующих) базы, пункты и объекты пяти типов [95, 207]:

- основные операционные базы с развитой инфраструктурой боевого и тылового обеспечения, обеспечивающие дислокацию крупных группировок сухопутных войск, военно-воздушных сил и военно-морских сил;
- передовые операционные базы, развернутые в непосредственной близости от потенциальных очагов нестабильности и границ государств, препятствующих продвижению национальных интересов США, на которых формирования (контингенты) предусматривается содержать на ротационной основе;
- пункты совместной безопасности, (в том числе с запасами материально-технических средств) на территориях ряда государств с размещением на них немногочисленного персонала вооруженных сил США на постоянной или временной основе;
- пункты заблаговременного складирования, предназначенные для размещения запасов военной техники и имущества с минимальным привлечением обслуживающего персонала;
- объекты морского базирования – специализированные морские платформы и суда-склады с запасами оружия, находящиеся в удаленных районах Мирового океана.

Главный принцип перегруппировки американских войск на зарубежных театрах войны – наращивание сил в стратегически важных районах и на ключевых направлениях, где проходят основные морские коммуникации и имеются значительные месторождения природных, как правило, углеродных, ресурсов. Он направлен на создание высокоманевренных и мобильных формирований экспедиционного типа, размещение которых обеспечит США своевременное и гибкое реагирование на весь спектр угроз в глобальном масштабе, а также установление контроля над стратегически важными источниками энергоресурсов.

Реализуя программу реконфигурации присутствия вооруженных сил США, Пентагон завершил работы по закрытию, реструктуризации и подбору новых мест дислокации баз по всему миру. Суть проводимых мероприятий состоит в том, что, имея, по данным зарубежной печати, 736 военных баз (крупных – 702, средних – 15, мелких – 19), военное ведомство отказывается от объектов с крупной концентрацией сил и средств, находящихся в Германии, Италии, Японии и Турции. Вместе с тем предусматривается сохранение и расширение ряда действующих в настоящее время мест базирования, в том числе в ряде государств Центральной Азии. Разрабатываются планы размещения военных объектов США на территории некоторых стран Центральной и Восточной Европы (Болгария, Польша, Румыния, Чехия), Балтии (Латвия, Литва, Эстония), Кавказа (Азербайджан, Грузия). Практическими шагами в этом направлении являются мероприятия по развертыванию на территориях Болгарии и Румынии подразделений восточно-европейской тактической группы численностью до 5 тыс. человек [95, 207].

Планируется создание принципиально новой системы передового базирования на морских платформах, размещенных в ключевых регионах мира на удалении не менее 45 км от береговой линии. Плавучие базы предполагается эксплуатировать в круглогодичном режиме, а их инфраструктура наряду с приемом военно-транспортных самолетов должна обеспечивать складирование, обслуживание и ремонт вооружения и военной техники, хранение запасов материально-технических средств, размещение личного состава [95].

Одновременно с учетом потребностей обеспечения региональной безопасности предусматривается перераспределить силы и средства в передовых зонах. В целях своевременного и адекватного реагирования на кризисные ситуации и проведения совместных операций объединенных и коалиционных войск (сил) Пентагоном реализуется новый «План объединенных командований», зоны ответственности которых охватывают всю территорию земного шара. При каждом объединенном командовании вооруженных сил США в передовых зонах создаются объединенные оперативные формирования, силы и средства которых должны обеспечивать нанесение с больших расстояний внезапных ударов обычными средствами поражения по стационарным и мобильным целям противника, находящимся по всей глубине его территории [95, 207, 209].

Под эти новые стратегические планы разработан и реализуется специальный проект по финансированию военного строительства

США (без учета средств, выделяемых на проведение конкретных операций типа иракской, афганской, ливийской и т. п.). Динамика военных расходов по годам выглядит следующим образом: 2006 г. – 556,3 млрд долл.; 2007 г. – 625,8 млрд долл.; 2008 г. – 696,2 млрд долл.; 2009 г. – 697,8 млрд долл.; 2010 г. – 722,1 млрд долл. (реально, с учетом дополнительных расходов на чрезвычайные мероприятия – 885,1 млрд долл.); 2011 г. – 738,7 млрд долл.; 2012 г. – 728,4 млрд долл. При этом военные расходы США после 2001 г. (наиболее низкий уровень после окончания холодной войны) возросли в 2010 г. на 81%, и сейчас они составляют 43% мировых военных расходов. Они в шесть раз превышают затраты на вооружение ближайшего соседа по расходам – Китая (источник – Ежегодник Стокгольмского международного института исследований проблем мира СИПРИ-2010 (Stockholm International Peace Research Institute (SIPRI))). США ежегодно тратят на военные нужды в два раза больше, чем остальные 27 стран альянса НАТО, при этом основная часть финансовых средств идет на закупку вооружения и военной техники (ВВТ) и выполнение научно-исследовательских и опытно-конструкторских работ (НИОКР). Затраты США на эти цели приблизительно в пять раз выше, чем у всех европейских союзников, вместе взятых [95].

В целом анализ концептуальных документов США в области национальной безопасности и строительства вооруженных сил позволяет сделать следующие выводы [95].

1. Комплекс документов, определяющих основные направления военной политики США в начале XXI в., переработан практически в полном объеме, существенно обновился и получил дальнейшее развитие. В них подтвержден курс на удержание лидирующего положения страны в мире как военной, так и экономической сверхдержавы, а также на обеспечение свободы действий на международной арене и беспрепятственного доступа в наиболее важные регионы в целях реализации всего спектра национальных интересов. Установки на превентивные действия, содержащиеся в стратегиях и доктринах, характеризуют военную политику и внешнеполитическую деятельность США как наступательную [95].

2. Особенностью документов последних лет является фактическое признание того, что США не смогли в одиночку решить главные проблемы глобальной безопасности, мир перестал быть однополярным, и, исходя из этого, необходимо искать коллективные подходы к решению задач обеспечения безопасности [95].

К угрозам национальной безопасности в стратегиях и доктринах отнесены [95]:

- международный терроризм;
- распространение оружия массового поражения и средств его доставки;
- сохранение конфликтного потенциала в различных регионах мира;
- развитие региональных держав в качестве новых центров влияния;
- усиливающаяся борьба за доступ к мировым ресурсам и энергетическая зависимость США от импорта углеводородного сырья;
- транснациональные проблемы (незаконная торговля оружием и наркотиками, пиратство, угрозы в киберпространстве, неконтролируемые глобальные миграционные процессы).

3. Практически во всех доступных документах их составители исходят из того, что основными задачами вооруженных сил США являются [95]:

- поддержание в готовности к ведению операций на удаленных театрах военных действий и способности к эффективному реагированию на чрезвычайные ситуации, как в пределах своей территории, так и за рубежом;
- предотвращение и сдерживание потенциальных вооруженных конфликтов за рубежом за счет готовности вооруженных сил к участию в ограниченных и широкомасштабных военных операциях;
- предотвращение террористических актов на территории США, защита американского народа и важных (критических) объектов инфраструктуры страны;
- эффективная борьба с терроризмом и распространением оружия массового уничтожения;
- при этом с учетом характера современных угроз и вызовов национальной безопасности вооруженные силы США в средне- и долгосрочной перспективе должны находиться в готовности к ведению военных действий одновременно против двух государств, обладающих боеспособными вооруженными силами.

4. США удалось разработать систему взаимоподчиненных документов по всей вертикали осуществления военной политики: от

формулирования целей применения военной силы в стратегии национальной безопасности до порядка глобального базирования американских войск (сил) и способов ведения конкретных операций в концепциях применения вооруженных сил [95].

5. Поставленная перед вооруженными силами США конечная цель – достижение всеобъемлющего доминирования, способности контролировать любую ситуацию или разгромить любого противника в военном конфликте любого типа и масштаба – провоцирует другие государства на адекватные ответные действия. Более того, создание Соединенными Штатами новых глобальных группировок войск, приближенных к источникам угроз национальным интересам США, затрагивает интересы многих государств мира [95].

В США продолжается динамичное изменение положений военной стратегии и приспособление их к реалиям быстро меняющейся обстановки в мире. Вместе с тем изменения практически не касаются основных политических установок военно-политического руководства, которые по-прежнему направлены на закрепление лидирующей позиции США в мире с использованием всего комплекса средств силовой борьбы. Общая тенденция развития военной идеологии США – обоснование доктрины превентивных действий в глобальном масштабе и поиск путей ее реализации [95].

Главная целевая установка этих документов – адаптировать вооруженные силы США к новым реалиям с учетом меняющегося характера войны, накопленного опыта военных действий за последние годы, стирающейся гранью между войной и миром через повышение боевых возможностей вооруженных сил и их организационную трансформацию. Проводимая США военная политика в первом десятилетии XXI в. свидетельствует о том, что военно-политическое руководство страны основной целью своей военной доктрины считает сохранение лидирующей роли США в мире и создание такой обстановки, в которой, как сказал министр обороны США, «...у потенциальных конкурентов не будет возникать даже мысли о возможности начать состязаться с США в военной области» [95].

В ближайшие годы Пентагон будет концентрировать свои ресурсы на пяти основных направлениях [95]:

- борьбе с терроризмом и распространением оружия массового поражения;
- разведке;

- подготовке к информационной войне (защита информационных систем и коммуникаций США и соответственно, разрушение аналогичных систем противника);
- борьбе за военное превосходство в воздухе (особый упор делается на развитие беспилотных летательных аппаратов);
- развитии военно-космических систем.

Рассмотрим основные изменения в строительстве вооруженных сил США по ее отдельным наиболее важным составляющим.

3.1.2. Ядерные стратегические силы

Начало ядерной программы США датируется 21 октября 1939 г., а первое испытание ядерного оружия проведено 16 июля 1945 г. Первый термоядерный взрыв на атолле Эниветок осуществлен 1 ноября 1952 г. Всего с 1945 г. по настоящее время США произвели 66,5 тыс. атомных бомб и ядерных боеголовок, а в двух правительственных лабораториях – Лос-Аламосской (Los Alamos National Laboratory, LANL) и Ливерморской им. Лоуренса (Lawrence Livermore National Laboratory, LLNL) – было создано в общей сложности около 100 различных типов ядерных зарядов и их модификаций. Всего за истекший период в США проведено 1054 испытания, из которых самый мощный взрыв (15 мегатонн) был произведен 1 марта 1954 г. Последнее испытание отмечено 23 сентября 1992 г. [95].

Максимальное число боеголовок с общим количеством свыше 32 100 боезарядов суммарной мощностью свыше 20 тыс. мегатонн (примерно эквивалентно мощности 1,36 млн бомб, сброшенных на г. Хиросиму в августе 1945 г.) зафиксировано в 1966-1967 гг. [95].

Максимальное расстояние доставки ядерного оружия наземными средствами составило 13 тыс. км, средствами военно-морских сил – 12 тыс. км. Впоследствии, в течение 20 последующих лет, арсенал Пентагона был сокращен на 30%. После окончания холодной войны в конце 1980-х гг. он уменьшился еще на 75% от оставшегося числа. Производство новых боеголовок прекратилось в 1992 г., но модификация имеющихся типов продолжается [95].

На 2009 г. в стратегических наступательных силах в составе ВВС насчитывалось 11 типов ядерного вооружения, в ВМС – 4 типа. С 1968 г. США являются одним из пяти участников договора о нераспространении ядерного оружия (членом ядерного клуба) [95].

За весь производственный цикл (от наработки делящихся оружейных материалов до разработки и выпуска боеприпасов и их утили-

зации) ответственность несет министерство энергетики США. Структурным подразделением министерства энергетики является разведывательный отдел, который осуществляет сбор открытой информации о состоянии энергетических ресурсов иностранных государств. Он тесно сотрудничает с Центральным разведывательным управлением (ЦРУ) (Central Intelligence Agency – CIA), Федеральным бюро расследований (ФБР) (Federal Bureau of Investigation – FBI) и Министерством обороны по вопросам предотвращения действий террористических организаций по хищению ядерного оружия и материалов [95].

Документом, отражающим взгляды военно-политического руководства страны на структуру, развитие и применение ядерного оружия, является «Всесторонний обзор ядерной стратегии США» (Nuclear Posture Review), подписанный президентом 6 апреля 2010 г. В нем говорится, что США не предполагают участия в крупномасштабных конфликтах с применением ядерных сил, и ядерное оружие рассматривается исключительно как инструмент сдерживания. Тем не менее США оставляют за собой право первыми применить ядерное оружие. В соответствии с новой ядерной доктриной главной угрозой для США и международной безопасности представляется не ядерное противостояние держав, а ядерный терроризм со стороны экстремистов и распространение ядерного оружия [95].

В процессе выработки требований к ядерным силам и средствам еще в предыдущем «Всестороннем обзоре ядерной стратегии США», датируемом 2002 г., была проведена классификация угроз, к отражению которых должны быть готовы стратегические силы США. Угрозы, которые рассматриваются и сегодня, были разделены на три категории [95]:

1. непосредственные;
2. потенциальные;
3. непредвиденные.

Непосредственные угрозы представляют собой хорошо известную, постоянно присутствующую опасность. Потенциальные угрозы – возможные, но не представляющие непосредственной опасности. К ним относятся угрозы различного характера, возникновение которых может предполагаться военно-политическим руководством страны и о наличии которых может быть получено своевременное предупреждение [95].

Непредвиденные угрозы представляют собой неожиданную и непредсказуемую опасность, они могут возникнуть как в ближайшее время, так и в перспективе. Примером подобной угрозы в настоящее

время может служить внезапный политический переворот в какой-либо стране, в ходе которого в руки нового руководства, враждебно настроенного к США, попадет ее ядерный арсенал. В качестве другого примера такого рода можно привести неожиданное приобретение враждебной стороной ОМП и средств его доставки [95].

Анализ нового «Обзора ядерной политики США», разработанного по требованию конгресса страны в феврале 2011 г., позволяет констатировать, что взгляды американской администрации на роль мощного потенциала стратегических ядерных сил в защите национальных интересов в последние годы практически не изменились. Однако предусматривается адаптация традиционной стратегии ядерного сдерживания времен холодной войны к новым условиям обстановки, характеризующейся наличием многочисленных потенциальных противников, источников конфликтов и спектром трудно прогнозируемых вариантов развития событий [95].

В обозримой перспективе США намерены сохранить за ядерным оружием только военную функцию, в то время как использование его в качестве средства политического давления будет играть второстепенную роль.

Основными положениями документа «Ядерная стратегия США» являются [95]:

- предотвращение распространения ядерного оружия и ядерного терроризма;
- уменьшение роли ядерного оружия в стратегии национальной безопасности США;
- обеспечение стратегического сдерживания и стабильности при сниженном уровне ядерных сил;
- усиление регионального сдерживания и подтверждение гарантий союзникам и партнерам США;
- поддержание безопасного, надежного и эффективного ядерного арсенала.

В соответствии с требованиями стратегии, изложенной в «Обзоре состояния и перспектив развития ядерных сил США» (Nuclear Posture Review Report), уже в 2012 г. предусматривалась замена ядерной триады периода холодной войны новой стратегической триадой с иными компонентами. В новую триаду предполагается включить [95]:

- ядерные и неядерные стратегические наступательные силы и средства;
- системы активной и пассивной обороны глобального охвата (стратегические оборонительные силы);

- разветвленные инфраструктуры производства, испытаний и боевого применения систем вооружений, обеспечивающие поддержание в боеготовом состоянии вновь создаваемых сил.

Под активной обороной понимаются системы ПРО и ПВО, а под пассивной – меры, направленные на снижение уязвимости вооруженных сил и своевременное предупреждение о внезапном нападении [95].

Объединение стратегических наступательных и оборонительных сил в единое целое направлено, прежде всего, на повышение их боевых возможностей путем развертывания единой глобальной эшелонированной системы противоракетной обороны, предназначенной для перехвата космических и воздушных целей (включая межконтинентальные баллистические ракеты МБР) на любом участке траектории их полета. Вновь создаваемая структура, по мнению авторов стратегии, призвана обеспечить решение следующего круга задач [95]:

- гарантировать безопасность союзников и дружественных стран «надежным вариантом ядерного и безъядерного ответа»;
- сдерживать любого агрессора;
- убедить соперников в бесперспективности гонки вооружений с США.

Специалисты Пентагона полагают, что объединение ядерных и неядерных сил существенно повысит гибкость и оперативность их применения, а также снизит порог применения стратегических наступательных сил, что позволит решать широкий спектр задач – от ядерного сдерживания (устрашения) до внезапного нанесения избирательных высокоточных ударов по наиболее важным объектам в любой точке земного шара. При этом предполагается, что компоненты новой триады будут объединяться в единое целое системой управления, связи и разведки, созданной на основе передовых информационных технологий [95].

В соответствии с Договором о стратегических наступательных вооружениях (СНВ-3), вступившим в силу 5 февраля 2011 г., предусмотрено сокращение ядерных боезарядов до 1550 единиц, межконтинентальных баллистических ракет, баллистических ракет подводных лодок и тяжелых бомбардировщиков – до 700 единиц. Договор рассчитан на 10 лет с возможной пролонгацией по взаимной договоренности сторон на 5 лет. В то же время в первой половине 2011 г. на сайте госдепартамента США были опубликованы данные о том, что по

состоянию на 5 февраля 2011 г. количество стратегических оперативно развернутых ядерных боеголовок составляло 1800 единиц, носителей – 882, а количество развернутых и неразвернутых пусковых установок баллистических ракет – 1124 единицы. Общие запасы США, включая резервы, составляют около 10 350 боезарядов, из которых 5000 оперативно развернутых, в том числе 4216 стратегических и 680 – нестратегических, 315 зарядов находится на хранении и около 5100 в резерве (табл. 3.1) [95].

Таблица 3.1. Ядерные силы США [95]

Силы и средства применения ядерного оружия	**Число развернутых единиц**	**Год начала развертывания**	**Дальность действия, км**	**Тип, число боезарядов, мощность одного боекомплекта, кт**	**Запасы боезарядов**
Стратегические силы					
Бомбардировщики:					
Boeing B-52H Stratofortress	93/56*	1961	16 000	КРВБ 1×5-150	450
Northrop B-2 Spirit	21/16	1994	11 000	УКР 1×5-150 Бомбы 200	400 200**
Итого:	114/72				1050
МБР:					
LGM-30G Minuteman III					
Mk 12	50	1970	13 000	3×170	150
Mk 12A	150	1970	13 000	1×170***	150
LGM-118A	300	1979	13 000	2-3×335	750
MX Peacekeeper	10	1986	13 000	10×310	100
Итого:	510				1150
БР подводных лодок:					
UGM-96A Trident I (C-4)	48	1979	7 400	6×100	288
UGM-133A Trident II (D-5)	288				
Mk 4		1992	Более	6×100	1344
Mk 5		1990	7 400	6×475	384
Итого:	360				2016
Итого в стратегических силах:			Более 7 400		4216

Силы и средства применения ядерного оружия	Число развернутых единиц	Год начала развертывания	Дальность действия, км	Тип, число боезарядов, мощность одного боекомплекта, кт	Запасы боезарядов
Нестратегические силы					
Бомбы B61-3, -4, -10		1979		1×0,3-170	580
КРМБ BGM-109 Tomahawk	320	1984	2500	1×5-150	100
Итого в нестратегических силах:					680
Всего боезарядов:					**4896**

* Первое число означает общее количество бомбардировщиков, второе – количество боеготовых бомбардировщиков, предназначенных для решения задач с применением ядерного и обычного оружия.

** Могут применяться как на бомбардировщиках B-2, так и на бомбардировщиках B-52H.

*** На всех 150 ракетах Minuteman III 90-го космического крыла число боезарядов понижено с трех до одного.

Что касается ядерных бомб, то все 580 единиц находятся в оперативном доступе, и они готовы к установке на различные типы самолетов США и НАТО. Кроме того, более 400 из них размещены на восьми авиабазах в шести европейских странах – участницах альянса (в Бельгии, Германии, Италии, Нидерландах, Турции и Великобритании) и, помимо ракет на подводных лодках, являются единственным типом тактического ядерного оружия США за рубежом [95].

Анализ документов в области ядерной стратегии позволяет предположить, что США намерены отказаться от ранее существовавших концепций сдерживания и устрашения в области применения ядерных сил. Вместе с тем в новых доктринальных документах подчеркнуто право США первыми применять ядерное оружие в соответствии с концепцией превентивных ударов, в первую очередь против враждебных государств, обладающих химическим, биологическим или ядерным оружием. Нанесение упреждающих ударов по этим государствам или террористическим группировкам предусматривается в том случае, когда возникнет угроза применения ими ОМП против США. Такие превентивные действия военные стратеги квалифицируют как активную оборону, а объективность оценки угрозы, как заявил ми-

нистр обороны США, «...особого значения иметь не будет, поскольку Соединенным Штатам не следует дожидаться достоверного подтверждения, чтобы начать действовать первыми и нанести удар по тому, кто угрожает Америке применением ОМП». Необходимость упреждающих ударов обосновывается тем, что терроризм не имеет национальной территории, которую ему нужно было бы защищать от гарантированного ответного уничтожения. Поэтому, скорее всего, единственным решением в войне с ним может стать уничтожение имеющегося у него ОМП еще до начала кризиса, с тем чтобы помешать рассредоточить это оружие или защитить его каким-либо иным способом. К тому же отсутствие сильного противника, по мнению специалистов Пентагона, исключает вероятность ответных ударов на превентивные действия США, а развертывание эффективной системы противоракетной обороны вообще сведет ее к нулю [95].

В дополнение к ядерному оружию в США исследуют возможность создания и использования для нанесения упреждающих ударов обычных средств, в том числе проникающих боеприпасов, сравнимых с ядерными по своей эффективности поражения подземных защищенных объектов. [95].

Главным фактором успеха в возможной войне с ядерной державой считается быстрота нанесения разоружающего удара, т. е. нейтрализация носителей стратегических ядерных сил противника и исключение для него возможности применения тактического ядерного оружия [95].

В развитие упомянутой выше ядерной стратегии в феврале 2011 г. президент США дал указание главе Пентагона переработать всеобъемлющий план модернизации носителей ядерного оружия и ядерного комплекса страны в целом в течение 10 грядущих лет (срок действия договора СНВ-3) [95].

В этом документе отмечается, что США намереваются, следуя установленным договором ограничениям, уменьшить количество оперативно развернутых межконтинентальных баллистических ракет с нынешнего уровня в 450 единиц до 420 и оснастить каждую из них одной боеголовкой. Помимо того, предполагается сохранить 14 находящихся сейчас в строю атомных стратегических подводных лодок, но сократить число пусковых установок на каждой из них с 24 до 20. Количество тяжелых бомбардировщиков, способных нести ядерные заряды, предполагается сократить с 94 до 60. В модернизацию средств доставки боеголовок к целям (объектам) администрация собирается вложить в течение десятилетия 100 млрд долларов [95].

Согласно разделам открытых планово-бюджетных документов, подготовленных Национальным управлением по ядерной безопасности при министерстве энергетики США, в ближайшие 20 лет национальные ядерные лаборатории намерены постоянно вести работу по совершенствованию ядерных боезарядов. Одновременно будут модернизироваться по три типа таких вооружений. Первые на очереди боеголовка W-76, устанавливаемая на баллистических ракетах подводных лодок, бомбы B-61 четырех различных модификаций, а также боеголовки W-78 для МБР наземного базирования [95].

3.1.3. Командование глобальных ударов и интеграции

В течение 2009-2012 гг. Министерство обороны США активизировало деятельность, направленную на практическую реализацию ключевых положений оперативно-стратегической концепции «Глобальный удар» (по некоторым источникам, «Мгновенный глобальный удар» – Prompt Global Strike). Основной целью данной концепции является придание американским вооруженным силам способности высокоточного воздействия на объекты противника в кратчайшие сроки и на большие дальности с использованием набора ударных средств в обычном или ядерном оснащении, а также посредством проведения космических, информационных и специальных операций. Концепция «Глобальный удар» предусматривает одновременный обезоруживающий удар тысячами крылатых ракет по административным и военным центрам, в том числе по шахтным пусковым установкам противника, с ориентировочной интенсивностью пуска до 1000 ракет в сутки [170, 171].

Задачи планирования, подготовки и проведения боевых операций в соответствии с концепцией «Глобальный удар» возложены на командование глобальных ударов и интеграции, созданное в структуре Объединенного стратегического командования. Практическая реализация концепции «Глобальный удар» с применением обычного вооружения может быть ответом на угрозы в таких сферах, как борьба с терроризмом, предотвращение распространения оружия массового поражения, а также недопущение ограничения свободы действий США, в том числе в области оказания ими военно-технической помощи своим союзникам. При этом эксперты Пентагона рассматривают пять возможных вариантов развития военно-политической обстановки, при которых возможно нанесение глобальных ударов обычными средствами [95].

1. *Первый вариант: «Двусторонняя конфронтация, обусловленная действиями государства, сравнимого с США по военному потенциалу, направленными на срыв боевого обеспечения вооруженных сил США и их союзников посредством преднамеренного нарушения функционирования американских космических систем связи и разведки»* [95].

Данный вариант предусматривает обострение военно-политической обстановки в случае преднамеренного уничтожения противником, который обладает возможностями по ведению боевых действий в космическом пространстве, одного из американских военных космических аппаратов. При этом США намерены не только пресечь агрессию, но и избежать дальнейшего перерастания конфликта в полномасштабное вооруженное противостояние. По мнению аналитиков Пентагона, в данном случае конфликт может носить ограниченный характер при реальной угрозе его эскалации до масштабов регионального вооруженного конфликта. Вместе с тем одним из ответных шагов может быть удар по противоспутниковой системе противника в целях предотвращения повторных нападений на орбитальную группировку США [95].

Наиболее оптимальными временными нормативами, по мнению американских экспертов, могут быть следующие [95]:

- принятие решения военно-политическим руководством США на проведение операции – сутки после нанесения противником удара по американским космическим аппаратам;
- перевод сил и средств, планируемых к применению, в высшие степени готовности – в течение 24 ч после принятия решения на проведение операции;
- продолжительность операции – 12 ч;
- оценка эффективности применения ударных средств по целям на территории противника – в течение 12 ч после нанесения удара;
- суммарное время на подготовку и проведение операции – не более 2-х суток с момента агрессии.

2. *Второй вариант: «Действия США по пресечению использования террористами радиоактивных материалов»* [95].

Этот вариант предусматривает незамедлительное принятие США мер в целях пресечения использования международными террористами радиоактивных материалов для изготовления «грязных атомных бомб». Для пресечения использования террористами радиоактив-

ных материалов предусматривается, как правило, применение сил специальных операций, способных захватить и переправить в США эти материалы для их дальнейшего уничтожения. Сведение до минимума сроков проведения операции планируется осуществить за счет организации постоянного дежурства необходимых сил и средств, а также их развертывания в районе планируемого применения одновременно с началом процесса выработки и принятия решения на действия [95].

3. *Третий вариант: «Действия американских вооруженных сил по пресечению применения одной из террористических организаций ОМП против США или их союзников»* [95].

В данном варианте рассматривается возможное развитие обстановки, требующей незамедлительного применения США силы в целях пресечения использования ОМП террористической группировкой, действующей на территории «относительно недружественной страны». Принимая во внимание необходимость оперативного реагирования, вооруженные силы США должны быть готовы к организации и проведению операции по уничтожению ОМП в условиях одностороннего применения силы (без согласия руководства страны, на территории которой находится пункт хранения ОМП) и возможного противодействия со стороны силовых структур отдельных государств региона [95].

4. Четвертый вариант: «Применение вооруженных сил в целях ликвидации лидеров одной или нескольких террористических организаций на территории нейтрального государства» [95].

В качестве исходной обстановки рассматривается ситуация, при которой лидеры террористических организаций в течение ближайших суток планируют встречу в одной из нейтральных стран на удалении более 1500 км от ближайшей передовой базы Вооруженных сил США. Для достижения поставленной цели и уничтожения или нейтрализации террористов предусматривается проведение либо совместной с военным ведомством нейтрального государства силовой операции, либо акции с участием только вооруженных сил США [95].

5. *Пятый вариант: «Применение вооруженных сил по упреждению ракетно-ядерного удара со стороны государства, обладающего ограниченным арсеналом ядерного оружия»* [95].

При этом варианте развития обстановки, по мнению аналитиков Пентагона, требуется немедленное вмешательство вооруженных сил США в целях пресечения ракетно-ядерного нападения со стороны государства, обладающего ограниченным арсеналом ядерного оружия. В качестве наиболее целесообразного способа нейтрализации этой

угрозы (ядерного шантажа) рассматривается внезапное применение МБР, баллистических ракет, подводных лодок (БРПЛ), крылатых ракет воздушного базирования в комплексе с возможностями региональной и национальной противоракетной обороны [95].

Эксперты Пентагона отмечают общие черты, характерные для всех вариантов действий вооруженных сил в рамках реализации концепции «Глобальный удар неядерными средствами», которыми являются [95]:

- минимальные временные затраты на оценку обстановки, принятие решения и подготовку ударных систем к боевому применению;
- предпочтение в применении сил специальных операций во всех вариантах использования вооруженных сил;
- широкое использование территории и воздушного пространства дружественных США государств;
- решающая роль фактора внезапности в достижении поставленных целей во всех без исключения вариантах.

Таким образом, в перспективе вооруженные силы США за счет развития высокоточного оружия и сопряжения его с глобальной информационной системой разведки и целеуказания планируют задействовать только неядерные силы для достижения текущих стратегических задач, а ядерные силы использовать только как оружие устрашения.

3.1.4. Командование боевых действий в киберпространстве

Военно-политическое руководство США первым начало рассматривать кибернетическое пространство как новую сферу ведения боевых действий наряду с наземной, морской и воздушно-космической сферами.

В мае 2009 г. аппаратом Белого дома в кооперации с комиссией по вопросам кибербезопасности Центра стратегических и международных исследований была подготовлена концепция «Информационное превосходство», впоследствии использованная в документе о стратегии развития ВС США «Единая перспектива – 2020». Основными принципами новой стратегии комплексной кибербезопасности в США являются следующие положения [95, 282]:

- создание условий для дальнейшего развития киберпространства с акцентом на совершенствование и расширение широкополосных сетей;
- распределение ответственности за кибербезопасность с одновременным тесным взаимодействием между федеральными ведомствами, местными властями и частным бизнесом;
- создание эффективной скоординированной системы распределения информации и реагирования на инциденты;
- поощрение и финансирование внедрения инновационных разработок в области кибербезопасности;
- совершенствование подготовки специалистов по кибербезопасности, которые должны владеть инструментами оборонительного и наступательного назначения.

Приказом министра обороны от 23 июня 2009 г. в США сформировано новое командование боевых действий в киберпространстве USCYBERCOM, которое находится в структуре объединенного стратегического командования США USSTRATCOM, подчинено директору АНБ и является основным органом управления боевыми действиями в киберпространстве ВС США. Данный шаг направлен на создание национальной системы координации, контроля и управления процессами планирования, подготовки и проведения операций в киберпространстве [281, 282].

Основное предназначение USCYBERCOM – координация защиты компьютерных сетей США и организация наступательных операций в кибернетическом пространстве. По сообщениям американских СМИ, комментирующих обоснование высшим военным руководством страны своих решений, активизация таких действий вызвана необходимостью противодействия попыткам, в частности со стороны КНР, атаковать компьютерные сети Пентагона, нарушить электроэнергетическую систему США и сорвать программы разработки перспективных систем вооружения (упоминается программа F-35) [95].

Ключевыми задачами командования USCYBERCOM в киберпространстве являются [281, 282]:

- обеспечение защиты информационных сетей министерства обороны США и национального разведывательного сообщества;
- координация взаимодействия профильных структур министерства обороны США в сфере кибербезопасности;

- представление интересов министерства обороны США по вопросам кибербезопасности на национальном уровне;
- оказание содействия и участие в общенациональных мероприятиях по обеспечению безопасности в киберпространстве, проводимых под руководством других федеральных ведомств США;
- оперативное управление выделенными видами ВС США силами и средствами ведения боевых действий в киберпространстве;
- координация планирования, разработка и ведение разведывательных, оборонительных и наступательных операций в киберпространстве.

Поставленные задачи командование USCYBERCOM решает во взаимодействии с агенством национальной безопасности (АНБ) (National Security Agency – NSA) и управлением информационных систем (УИС) министерства обороны США. Указанные органы министерства обороны в рамках решения задач обеспечения кибербезопасности и ведения боевых действий в киберпространстве отвечают за своевременное предоставление для USCYBERCOM разведывательной информации АНБ и технической поддержки УИС [281].

В организационно-штатной структуре USCYBERCOM использовалась модель объединенного боевого командования, включающая в себя киберкомандования родов вооруженных сил, что, по мнению высшего военного руководства США, позволяет наиболее эффективно задействовать возможности всех видов вооруженных сил США и учитывать их интересы при ведении общевойсковых операций [282]. Управление выделенными в оперативное подчинение командованию USCYBERCOM силами и средствами осуществляется через входящий в структуру командования центр совместных операций в киберпространстве. Он отвечает за непосредственное решение возложенных на командование задач, в том числе за координацию планирования, разработку и ведение совместных операций в киберпространстве во взаимодействии с другими объединенными командованиями, профильными структурами министерства обороны, а также специализированными структурами других федеральных министерств и ведомств [281].

В оперативном подчинении командования USCYBERCOM находятся следующие специальные командования и формирования основных видов и компонентов ВС США [281, 282]:

- командование боевых действий в киберпространстве сухопутных войск;

- командование боевых действий в киберпространстве ВМС – 10-й оперативный флот ВМС;
- 24-я воздушная армия (воздушная армия боевых действий в киберпространстве) ВВС;
- командование боевых действий в киберпространстве морской пехоты;
- командование боевых действий в киберпространстве береговой охраны США.

Общая численность командования USCYBERCOM на начало 2012 г. составила около 1 тыс. человек. Бюджет USCYBERCOM на 2011 г. превысил 150 млн долл.[281].

3.1.5. Сухопутные войска

По планам командования США в период до 2025 г. в американских сухопутных войсках произойдут коренные преобразования, которые затронут все стороны их применения: планирование, организационную структуру, техническое оснащение, обучение и подготовку, стратегию, оперативное искусство и тактику, организацию обеспечения боевых действий и др. В связи с развитием технологических возможностей США, одними из наиболее важных аспектов указанных преобразований являются выработка и своевременная корректировка требований, которые предъявляются к средствам вооруженной борьбы как традиционного, так и нелетального характера [95].

В сухопутных войсках ведется формирование инфраструктуры, предоставляющей возможности совместного использования информационных ресурсов, как в рамках вида вооруженных сил, так и за счет сетевого обмена информацией между всеми видами ВС согласно концепции сетецентричности. Так, построение перспективной глобальной информационной структуры сухопутных войск США, получившей название LandWarNet, рассматривается руководством этого вида вооруженных сил в качестве базовой основы перехода к сетецентрическому принципу боевого управления. Концепция LandWarNet должна обеспечить на основе совместного использования информационных ресурсов и надежного сетевого взаимодействия высокую степень согласованности и синхронизации действий широко рассредоточенных на ТВД боевых и обеспечивающих формирований всех видов вооруженных сил. При этом командование сухопутных войск США выделило 17 направлений перспективного строительства, определенных в качестве базовых для достижения подавляющего превосходства над лю-

бым противником. Спектр этих направлений достаточно обширен – от индивидуальной подготовки и экипировки военнослужащих, способных вести боевые действия в единой сетецентрической среде, до создания подразделений, формируемых по модульному принципу для решения соответствующих задач. Реализация таких планов позволит преобразовать сухопутные войска традиционной структуры в силы нового типа, гарантирующие превосходство над любым противником [107].

Развитие СВ США в настоящее время осуществляется в соответствии с программой «Армия 21», разработанной в рамках концепции строительства ВС США «Единые силы» (Joint Force 2020). Эта программа нацелена на проведение реорганизации «тяжелых» (механизированных и бронетанковых) соединений, составляющих основу СВ, с целью создания более гибких формирований, способных противостоять любому противнику. Реализация положений данной программы началась в середине 1996 г. на базе 4-й механизированной дивизии, оснащенной новейшими образцами вооружения, военной, специальной техники (ВВСТ). Она прошла дальнейшую проверку в ходе батальонных, бригадных и дивизионных экспериментальных учений под общим наименованием «Таск Форс – 21» (Task Force XXI). По их результатам в 2002 г. было создано первое компьютерное соединение («Division XXI») СВ [29].

Основным содержанием оптимизации организационно-штатной структуры сухопутных войск является перевод их на бригадную структуру модульного типа [95].

В рамках данных мероприятий формируются бригады модульного типа. При этом на базе дивизионных и корпусных штабов создаются новые модульные органы управления. Каждый такой модуль способен не только обеспечить оперативное управление действиями нескольких (до шести) боевых бригад и бригад обеспечения, но и взять на себя функции штаба объединенного оперативного формирования в различных по масштабу и интенсивности операциях с участием вооруженных сил США [95].

Главной особенностью строительства СВ является то, что в целях подготовки наземных формирований к ведению боевых действий в условиях неопределенного будущего руководством СВ разработана и успешно осуществлена программа «Force XXI». Важнейшее место в ней отводится достижению всеобъемлющего превосходства СВ над любым противником во всех сферах боевого пространства за счет применения новейших образцов ВВСТ в соответствии с новыми опе-

ративными концепциями. Особенностью является тот факт, что в основе реализации программы «Force XXI» лежит четко организованный процесс проведения экспериментов, касающихся обучения личного состава, обеспечения боевой готовности, изменения подходов к управлению войсками и их техническому оснащению, а также к совершенствованию организационно-штатной структуры [29].

В рамках программы «Force XXI» планируется реализовать ряд концепций, основными из которых являются «Force XXI» и «Армия будущего». Они должны осуществляться в рамках боевых лабораторий, войсковых экспериментальных учений, демонстраций концепций передовых технологий и преследовать следующую основную цель – повысить боевые возможности СВ будущего за счет перспективных образцов ВВСТ [29, 42].

Оснащение сухопутных войск высокоточным оружием и их технологическая модернизация позволят США обеспечить наступательно-оборонительный характер боевых действий (сражений). Характерными чертами применения сухопутных группировок могут быть [95]:

- сближение боевых и небоевых форм действий;
- сочетание наступательных, оборонительных и поддерживающих действий;
- стремление к упреждению противника в темпе и интенсивности ведения боевых действий за счет возрастания мобильности, точности поражения целей и информационного превосходства;
- освоение и применение наземными группировками тактических приемов сил специальных операций;
- увеличение степени рассредоточения подразделений (частей) на поле боя и глубины боевого порядка (оперативного построения);
- появление новых элементов боевого порядка (оперативного построения), в том числе противодесантных вертолетных резервов, группировок сил и средств информационной борьбы, разведки и РЭБ, воздушных эшелонов различного назначения;
- появление новых форм применения средств поражения, в том числе массированного огневого удара с применением высокоточного оружия, совместное использование средств радиоэлектронного подавления и огневого поражения, рей-

довые действия воздушно-наземных тактических групп и аэромобильных десантов и др.

Основной способ разгрома противника – удар по уязвимым местам группировки с целью лишить его способности к продолжению боевых действий. Главный удар в наступлении предполагается наносить по объектам, определяющим тактическую (оперативную) устойчивость группировки противника [95].

3.1.6. Силы разведки и радиоэлектронной борьбы

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 вв. 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 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 противника [95].

К настоящему времени аналитиками Пентагона отмечается, что в современных условиях именно РЭБ является основой информационной войны на военном уровне, а развитие теории информационных операций является базой для ведения такой войны [95].

Ключевые концепции строительства сухопутных войск США XXI в. нового типа и задачи РЭБ по подавлению систем боевого управления противника определены рядом основных документов комитета начальников штабов вооруженных сил страны и командования сухопутных войск США [95]:

- меморандум Joint Vision 2020 (2000);
- стратегия – The Army Transformation Strategy (2001);
- уставы КНШ JP 3-13.1, JP 3-51;
- уставы сухопутных войск FM 3-0, FM 2-19.301/ST, FM 2-19.401/ST, PM2-40.1/8T и др.

Способы, методы и приемы ведения радиоэлектронной борьбы, предусмотренные новыми концепциями, проверяются в ходе крупных учений и локальных конфликтов и в последующем находят свое отражение в руководящих документах [95].

Для реализации положений выдвинутых концепций проводятся организационные и технические мероприятия [95]:

- создаются новые организационные структуры в вооруженных силах и органах их управления;
- создаются единые структурно упорядоченные системы РЭБ соединений и объединений во всех видах вооруженных сил, а в перспективе – в масштабе видов;
- развернут обширный круг научно-исследовательских и опытно-конструкторских работ по созданию новых средств РЭБ, а также совершенствованию существующих.

Подразделения и части разведки и РЭБ нового типа, действуя в информационных операциях в составе сил борьбы с системами боевого управления, будут способны добывать, быстро обрабатывать, хранить и распределять информацию, а также в масштабе времени, близком к реальному, воздействовать на противника, привлекая для этого штатные силы разведки и РЭБ наземного и воздушного базирования, а также средства разведки и РЭБ, забрасываемые на его территорию, в первую очередь роботизированные [95].

Целями радиоэлектронной борьбы в операциях сухопутных войск нового типа наряду с дезорганизацией систем боевого управления противника станет лишение его возможности использовать информацию о своих войсках [95].

Содержание РЭБ в ВС США расширено за счет включения в него мероприятий по оперативной маскировке, в том числе комплексному противодействию техническим средствам разведки противника, огневому и ядерному поражению его радиоэлектронных средств и их захвату диверсионными силами [95].

Мероприятия РЭБ составляют основу активно внедряемой в вооруженных силах США концепции «Борьба с системами боевого управления». Суть ее 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» [95].

Радиоэлектронная борьба в информационных операциях планируется в комплексе с другими элементами оперативного планирования, а ведущими исполнителями в этой области являются офицеры РЭБ оперативного штаба [95].

Долгосрочное планирование возлагается на управление планирования объединенного штаба, под руководством которого готовится операция [95].

Краткосрочное планирование РЭБ, как и оперативное руководство ее ведением, осуществляется оперативными отделами (отделениями) в штабах объединений (соединений). Координация задач радиоэлектронной атаки и радиоэлектронной защиты, согласование действий со штабами формирований других видов вооруженных сил, разрешение конфликтных ситуаций при использовании радиоэлектронных систем и средств возлагается на управление (отдел) боевого управления, связи и автоматизации [95].

Все мероприятия радиоэлектронной борьбы в информационной операции коалиции многонациональных сил объединяются единым планом. При этом устанавливается общий порядок обмена информацией об объектах воздействия и применяемых силах и средствах РЭБ, сопряжения систем связи и боевого управления, указываются общие для всех правила кодирования и засекречивания информации [95].

В сухопутных войсках США ряд мероприятий по организации и ведению радиоэлектронной борьбы в интересах информационных операций выполняет командование разведки и безопасности INSCOM (Intelligence and Security Command), оперативно подчиненное заместителю начальника штаба армии по разведке (Army Deputy Chief of Staff for Intelligence) [95].

Командование INSCOM является основным органом оперативно-стратегического звена управления сухопутных войск США, отвечающим за ведение разведки и радиоэлектронной борьбы, обеспечение безопасности и проведение информационных операций. Его штаб размещен в Форт-Бельвуар, штат Виргиния. Общая численность командования к началу 2011 г. составляла приблизительно 12,5 тыс. человек личного состава, в том числе около 3 тыс. – гражданские специалисты [95].

На это командование возлагаются следующие задачи [95]:

- организация разведки, контрразведки и радиоэлектронной борьбы;
- ведение стратегической радио- и радиотехнической разведки;
- руководство подразделениями криптологической службы;
- осуществление агентурной разведки и контрразведки;

- проведение мероприятий по обеспечению безопасности в масштабе сухопутных войск.

Кроме того, оно занимается разработкой обобщенной разведывательной оценки состояния вооруженных сил вероятных противников для руководства сухопутных войск, оказанием технического содействия и оперативной помощи командованию сухопутных войск в организации и ведении разведки и РЭБ, фоторазведкой в интересах сухопутных войск, а также обеспечением решения задач, поставленных перед разведывательным сообществом.

На основе опыта войн и вооруженных конфликтов, в которых участвовали части и подразделения разведки и радиоэлектронной борьбы, была разработана новая доктринальная концепция разведывательного обеспечения операций вооруженных сил США XXI в. Intelligence XXI Concept.

В ней определены основные принципы ведения разведки и РЭБ в операциях сухопутных войск [95]:

- непрерывное руководство организацией и ведением разведки и радиоэлектронной войны соответствующими органами управления сухопутных войск;
- согласование по цели, месту и времени задач частей и подразделений военной разведки в соответствии с замыслом операции и решениями соответствующих командующих компонентами сухопутных войск объединенных сил США;
- охват всего спектра задач военной разведки и РЭБ путем своевременного распределения сил и средств и осуществление контроля за эффективностью ведения разведки и радиоэлектронной войны в операции;
- разведывательное обеспечение действий войск на протяжении всех этапов операции, начиная с подготовки к проведению и после ее завершения;
- обеспечение своевременной обработки, анализа, уточнения и распределения разведывательной информации;
- доведение разведывательной информации до штабов войск, средств поражения и радиоэлектронной войны;
- обеспечение подготовки и проведения информационных операций сухопутных войск и объединенных сил США.

В связи с трансформацией вооруженных сил США и переходом их к модульному принципу построения боевых и обеспечивающих формирований в настоящее время, судя по материалам открытых источников, бригады военной разведки предполагается передавать в

оперативное подчинение штабу компонента сухопутных войск объединенного оперативного формирования в зоне ответственности. Выделяемые частями военной разведки подразделения планируется применять в интересах разведывательного и информационного обеспечения действий формирований оперативно-тактического и тактического уровней.

3.1.7. Военно-морские силы

Принятая в США в начале 2008 г. новая «Скоординированная стратегия морской мощи XXI века» (A Cooperative Strategy for 21st Century Seapower) определила роль всех морских компонентов (силы флота, морской пехоты и БОХР) в урегулировании кризисов, ведении (и предотвращении) войн и вооруженных конфликтов всех уровней в условиях непростой современной международной обстановки и растущей экономической напряженности. На ее основе были выработаны основные направления и концепции оперативного применения морских сил [43].

Наряду с традиционными установками на обеспечение передового присутствия и демонстрацию силы, стратегического сдерживания и силового давления, поддержания господства на море и гарантированной свободы мореплавания, морская стратегия выдвинула в число основных новые концепции [43]:

- обеспечения коллективной безопасности на море (TSC – Theater Security Cooperation);
- глобального сотрудничества морских сил (Global Maritime Partnership).

Эти концепции предусматривают расширение и углубление сотрудничества с морскими силами всех союзных государств и стран-партнеров в области обеспечения безопасности в Мировом океане, повышения возможностей морской составляющей системы противоракетной обороны, организации эффективного и устойчивого оперативного взаимодействия ВМС США и их союзников в составе объединенных и коалиционных формирований в любых регионах мира. В конечном итоге предполагается даже формирование международного флота 1000-корабельного состава. Успешная реализация вышеуказанных концепций возможна, по мнению западных военных экспертов, лишь на базе создания интегрированной структуры, или, как ее называют на западе, функциональной концепции «Единая сеть сил ВМС» (FORCE-

net), объединяющей системы боевого управления силами флота, оружием и обеспечивающими средствами [43].

«Единая сеть сил ВМС» разрабатывается в рамках формирования «Единой сети вооруженных сил» и связана с аналогичными структурами других видов вооруженных сил, что позволит сформировать единое информационно-коммуникационное пространство, в котором компоненты ВМС, ВВС, СВ и сил космического базирования, составляющие объединенные группировки или оперативные формирования войск (сил) на ТВД, будут способны вести согласованные боевые действия как наступательного, так и оборонительного характера. Выполнение всех предусмотренных концепцией мероприятий позволит достичь недосягаемых ранее возможностей по добыванию, обработке, обобщению, распределению и защите информации в интересах любых объединенных или коалиционных формирований военно-морских сил [43].

Концепция «Единая сеть сил ВМС» (FORCEnet) пришла на смену существовавшей раннее концепции «Информационные технологии XXl века» (IT21 – lnformation Technology for 21-st Century) и предполагает интеграцию всех участников операции (боевых действий), систем управления и разведки, боевых платформ (надводных кораблей, подводных лодок, самолетов и т. д.), а также комплексов и средств вооружения в единую взаимосвязанную структуру рассредоточенных боевых сил, способных проводить успешные операции в конфликтах любого уровня и масштаба. Ведущееся в настоящее время обновление самолетного и вертолетного парка, поступление на вооружение палубной авиации новейшего радиоэлектронного оборудования и высокоточного оружия нового поколения позволят существенно повысить ударные возможности авиации флота. В результате, по расчетам специалистов, силами авианосных и экспедиционных (с авиагруппой авиации морской пехоты) ударных групп может быть нанесен удар по нескольким сотням целей одновременно [43, 95].

В настоящее время в океанских стратегических районах и морских зонах, прилегающих к территории России, сохраняется постоянное присутствие групп кораблей США и их союзников. Здесь развернуты три оперативных флота ВМС США (5-й, 6-й и 7-й) в составе 3-х авианосных ударных групп (АУГ – 120–160 палубных истребителей-штурмовиков, а также до 36 носителей крылатых ракет морского базирования (КРМБ) Tomahawk с боезапасом более 700 крылатых ракет). Готовность к их применению составляет не более часа. В угрожаемый период и в начальный период военных действий группировка может

быть увеличена более чем в 3 раза и включать до девяти АУГ (360 ударных самолетов) и до 80 носителей КРМБ Tomahawk с боезапасом свыше 2 тыс. КРМБ [269].

Мощными средствами воздействия на береговые объекты противника в ВМС США являются корабельные ударные группы (КУГ). Как правило, они включают в свой состав крейсеры и эсминцы УРО, а также корабли охранения. Подобные группировки предназначены для нанесения ударов по целям на дальностях до 2,5 тыс. км. Каждая КУГ способна нести 120-190 крылатых ракет [269].

К 2030 г. ВМС США будут иметь в своем составе до 400 боевых кораблей, среди них до 50% кораблей – носителей КРМБ и до 12 авианосцев. Подобные группировки в гипотетическом военном конфликте могут представлять реальную угрозу для 60-65% важных объектов военно-промышленного потенциала Российской Федерации на 80% территории европейской части страны, Сибири и Дальнего Востока [269].

Авианосная многоцелевая группа (АМГ) включает в себя многоцелевой авианосец, авиакрыло, 6-8 кораблей охранения, оснащенных сильным противолодочным, противокорабельным и зенитным ракетным оружием. В состав АМГ могут включаться 1-2 многоцелевые подводные лодки и транспорты снабжения. Развитая система универсальной обороны этого соединения обеспечивает его высокую боевую устойчивость [269].

3.2. Объединенные вооруженные силы блока НАТО

Анализ работ [43, 50, 206, 207, 208, 283] показал, что переход к концепции сетецентрических войн главного члена НАТО – США определил развитие и внедрение данной концепции в вооруженных силах других членов альянса. В настоящее время в НАТО реализуется концепция «Комплексные сетевые возможности» (NNEC – НАТО Network Enabled Capabi1ities), предназначенная для решения вопросов организации взаимодействия высокотехнологичных формирований национальных вооруженных сил в современных и будущих вооруженных конфликтах. Основные положения новой концепции были отражены еще в 2005 г. в документе «Defense Requirements Review».

Главной целью реализации концепции «Комплексные сетевые возможности» НАТО является внедрение перспективных информаци-

онных технологий в военную сферу для противодействия современным вызовам и угрозам национальной и коалиционной безопасности. Проводимые в настоящее время мероприятия осуществляются в трех ключевых областях [43]:

- развертывание современных систем связи и передачи данных;
- разработка перспективных систем обработки, анализа и распределения информации, использующих унифицированные инструментарии ее обработки и форматы передачи;
- формирование современной когнитивной сферы, затрагивающей вопросы реформирования и оптимизации организационных структур органов управления, обработки и анализа информации, а также подготовку личного состава и пересмотр уставных и доктринальных документов.

Реализация новой концепции НАТО позволит осуществлять эффективное информационно-разведывательное обеспечение операций всего возможного спектра, начиная от миротворческих операций и операций по установлению мира до крупномасштабных боевых действий высокой интенсивности. Вместе с тем военные специалисты НАТО подчеркивают, что концепция NNEC – это не только интеграция систем управления и связи, но и возможность повысить уровень взаимодействия всех участников операции (боевых действий), в том числе и средств поражения, органов и пунктов материально-технического обеспечения и др. (табл. 3.2) [43].

Для оптимизации проводимых мероприятий сформирован специальный консорциум NCOIC, призванный обеспечить единство протоколов обработки и представления информации и оказать поддержку промышленности в выполнении требований по достижению необходимого уровня взаимодействия и интеграции перспективных систем и комплексов в реализации сетецентрических принципов управления формированиями. Консорциум пополняется новыми членами. Если в 2004 г. в его состав входили только 15 компаний, то сейчас их число увеличилось до 96, представляющих 32 страны, 26 из которых являются членами НАТО. Консорциум тесно взаимодействует с Агенством по оборонным информационным системам Пентагона DISA – (Defense Information Systems Agency), а в состав его руководства входят представители министерства обороны, разведывательного сообщества, министерства внутренней безопасности и ряда других ведомств США [43].

Таблица 3.2. Оценки повышения эффективности разведывательного обеспечения современных и будущих операций коалиционных сил НАТО [50]

№ п/п	Возможности системы разведки коалиционных сил на ТВД			
	Критерии оценки	Значение критериев		
		Существующие	Пороговые	Ожидаемые
1	Доведение информации от средств радиолокационной разведки с возможностью селекции движущихся целей до потребителей на ТВД	Менее 1 мин	Не более 10 с	Не более 5 с
2	Доведение данных видовой разведки до потребителей	Менее 20 мин	Не более 5 мин	Не более 2 мин
3	Доведение обобщенной информации об обстановке на поле боя на основе данных видовой и радиолокационной разведки с возможностью селекции движущихся целей	Не менее 30 мин	Не более 20 мин	Не более 5 мин
4	Предоставление командирам всех звеньев управления доступа к потокам разведывательной информации для формирования единой картины обстановки на поле боя	--	Не более 5 мин	Не более 1 мин
5	Перенацеливание средств разведки коалиционных сил	Не менее 30 мин	Не более 10 мин	Не более 2 мин
6	Идентификация средства в поле видимости	Не менее 30 мин	Не более 12 мин	Не более 3 мин
7	Передача данных целеуказания любому средству поражения на ТВД	Не менее 30 мин	Не более 5 мин	Не более 2 мин

№ п/п	Возможности системы разведки коалиционных сил на ТВД			
	Критерии оценки	Значение критериев		
		Существующие	Пороговые	Ожидаемые
8	Возможность интеграции нового средства разведки к уже функционирующей системе боевого управления, связи и разведки на поле боя	Несколько месяцев	Не более 1 недели	Не более 1 дня

Для осуществления рационального строительства вооруженных сил в условиях перехода к концепции сетецентрической войны в НАТО в 2010 г. была принята стратегическая концепция «Активное участие, современная оборона» (Active Engagement, Modern Defence), которая представляет собой три важнейшие задачи блока – коллективную оборону, кризисное регулирование и безопасность на основе сотрудничества.

Ключевые положения новой стратегической концепции НАТО остались прежними, и в соответствии с ними в области безопасности блок будет проводить политику с позиции силы. Однако теперь прямое военное столкновение НАТО с Россией считается маловероятным. Вместе с тем в случае развязывания войны в Европе альянс, в соответствии с новой стратегией, не должен допустить потери своей территории [207].

В документе отмечается, что угрозы безопасности НАТО, как военного, так и невоенного характера, в обозримом будущем сохранятся. Они обусловлены, в первую очередь, наличием очагов нестабильности на Евроатлантическом пространстве, а также возможностью возникновения кризисов регионального масштаба за пределами зоны ответственности НАТО. Этнические и религиозные конфликты, с которыми сталкиваются некоторые государства Европы и прилегающих к ней регионов, территориальные споры, болезненные политические и экономические реформы, нарушение прав человека, распад государств – все это может привести к кризису локального, а при определенных условиях регионального, масштаба и перерастанию его в вооруженный конфликт, вероятность вовлечения в который соседних стран – членов НАТО весьма высока [207].

Основной формой применения вооруженных сил НАТО в крупномасштабном конфликте остается стратегическая операция с привлечением всех видов вооруженных сил. Характер операций на

каждом стратегическом направлении будет зависеть от военно-политических целей, преследуемых блоком, и физико-географических особенностей ТВД [207].

Такое изменение стратегии потребовало коренной перестройки всей военной структуры блока. Создаются многонациональные войсковые формирования, а национальные ВС вырабатывают единый подход к военному планированию, приобретению вооружения и военной техники, оперативной и боевой подготовке. На стратегическом уровне ведется реорганизация национальных министерств обороны, пересматриваются подходы к стратегическому планированию, меняется военно-промышленная политика государств, создаются новые высшие объединенные органы военного управления и коренным образом обновляются функции старых. На оперативном уровне пересмотрены задачи объединенных командований, реформируется система объединенного планирования, изменяется отраслевая структура военно-промышленной базы стран-членов. На тактическом уровне внедряются новые формы и способы ведения боевых и других действий, которые приводятся в соответствие с концепцией сетецентрических войн [207, 208].

К глобальной организационной реформе своей военной структуры НАТО приступил еще в 2002 г. Необходимость преобразований была продиктована следующими факторами [207]:

- *изменением характера и спектра угроз.* Переход к концепции сетецентрической войны, преобладание ограниченных локальных военных конфликтов, возрастание активности международных террористических организаций, рост международной преступности обусловил актуальность изменения военной структуры НАТО, так как для нейтрализации этих новых угроз она была совершенно не приспособлена;
- *возникновением новых задач, связанных с урегулированием кризисных ситуаций в зоне ответственности альянса, а также за ее пределами, что раньше было прерогативой ООН*. Теперь руководство альянса считает возможным проводить военные операции, а также сопутствующие действия невоенного характера и в случаях, не предусмотренных ст. 5 о коллективной обороне Североатлантического договора. Правда, в отличие от ситуаций, связанных с выполнением союзнических обязательств, сила в таких случаях будет применяться не автоматически. В случаях, требующих применения или угрозы применения военной силы,

спектр операций, как по характеру, так и по масштабу, может быть очень широк: от обеспечения санкций или режима эмбарго, установленного международными организациями, до боевых действий в целях принуждения к миру. Предполагается, что операции по урегулированию кризисов вряд ли по степени напряженности будут уступать действиям в рамках коллективной обороны. Следовательно, войска к ним надо готовить соответствующим образом, обучать, оснащать и вооружать. Без реформы структуры НАТО эта задача не может быть решена;

- *в рамках операций, организуемых под руководством НАТО, войска должны проводить эвакуацию гражданского населения и сотрудников международных организаций, осуществлять поисково-спасательные работы, оказывать помощь пострадавшим во время стихийных бедствий*;
- *стремлением снизить затраты на содержание громоздких военных структур НАТО;*
- *политикой США, направленной на уравнивание вкладов союзников в оборонный сектор НАТО.*

Главная цель реформ структуры НАТО – создать структуру вооруженных сил, позволяющую быстро и без особых затрат перестраиваться под новые задачи и условия. В этом направлении в настоящее время достигнуты определенные успехи:

1. Во-первых, в результате реорганизации новая структура управления выглядит следующим образом [207].

На стратегическом уровне созданы два органа управления. Стратегическое командование (СК) (Strategic Command) объединенных вооруженных сил НАТО в Европе будет преобразовано в АСО Allied Command Operations – стратегическое командование НАТО по операциям, а СК объединенных вооруженных сил НАТО на Атлантике станет базой для формирования командования стратегических исследований (КСИ). Оно не должно иметь оперативных функций, т.е. не будет управлять войсками, а займется разработкой концепций строительства и применения объединенных вооруженных сил альянса, исследованием форм и способов ведения военных действий в различных условиях, выработкой военно-технической политики блока [207].

Показательно, что штаб-квартира командования стратегических исследований расположена в г. Норфолке (восточное побережье Америки) по соседству с объединенным командованием единых сил ВС США, на которое возложены аналогичные задачи: концептуальная

проработка стратегии реформ американских вооруженных сил, проверка теории в ходе экспериментов и учений, а также внедрение новшеств в войска.

На оперативно-стратегическом уровне созданы три коалиционных органа управления: объединенные командования (ОК) «Север», «Юг» и «Запад». Первые два формируются на базе существующих региональных командований в Европе и имеют сухопутные границы. Зоны их ответственности в совокупности составляют зону ответственности стратегического командования операций ОВС НАТО. ОК «Запад» создается на базе атлантического регионального командования «Юго-восток». На него возложены функции по разработке планов применения объединенных военно-морских сил (ОВМС) НАТО и управлению ими в зоне Иберийской Атлантики [207].

Все другие командно-штабные структуры оперативно-стратегического уровня, функционирующие на Атлантике, будут упразднены, а вновь созданные подчинены СКО ОВС НАТО. В случае обострения обстановки в оперативное подчинение соответствующего стратегического командования будет передаваться командование ударного флота НАТО на Атлантике [207].

На оперативном уровне – видовые командования объединенных ВВС и ВМС «Север» и «Юг» будут сохранены, а субрегиональные упразднены. В результате в состав объединенных командований «Север» и «Юг» войдут по три видовых командования: объединенных сухопутных войск (ОСВ), ОВВС и ОВМС. В мирное время ОК «Запад» подчиненных видовых командований иметь не будет.

Директивные документы альянса устанавливают зоны ответственности только для коалиционных командований стратегического и оперативно-стратегического уровней. Видовые командования выполняют поставленные задачи в пределах границ соответствующих объединенных командований.

2. Во-вторых, будет упразднена громоздкая трехкомпонентная структура вооруженных сил НАТО, состоявшая из сил реагирования, главных оборонительных сил и войск усиления. Произошли серьезные изменения и в классификации вооруженных сил альянса. Теперь они различаются по степени готовности к применению, по предназначению и по подчиненности коалиционным командованиям.

Структурно ВС Североатлантического союза состоят из объединенных и национальных вооруженных сил. Последние могут выделяться в распоряжение соответствующих командований ОВС НАТО в соответствии с блоковым механизмом, а также соглашениями по ко-

ординации и сотрудничеству, предусматривающими передачу сил и средств в соответствии с национальными возможностями и сценариями развития обстановки [207].

По способности к развертыванию ОВС альянса подразделяются [207]:

- на силы территориального применения;
- на силы универсального применения.

Силы территориального применения (СТП) формируются преимущественно за счет национальных ВС и предназначены для решения задач коллективной обороны территории государств НАТО. Они могут привлекаться и к операциям по урегулированию кризисных ситуаций вне зоны ответственности блока, если эти операции проводятся в непосредственной близости от мест постоянной дислокации СТП. В обычных условиях силы территориального применения находятся в местах постоянной дислокации – необходимости в полном их развертывании нет. При этом СТП должны сохранять способность своевременно реагировать на угрозу территориальной целостности стран – членов альянса [207].

Силы универсального применения (СУП) предназначены для ведения как крупномасштабных военных действий, так и операций по урегулированию кризисных ситуаций. Их основу составляют многонациональные формирования, способные в течение продолжительного времени вести активные военные действия, в том числе и на удаленных от Европы ТВД. Входящие в боевой состав СУП формирования в мирное время сведены в единый комплект, что позволяет им быстро реагировать на угрозы безопасности альянса [207].

Силы универсального применения – наиболее боеготовые и мобильные в НАТО. С 2010 г. в состав сухопутного компонента этих сил входит девять оперативно-тактических объединений, сформированных на базе многонациональных и национальных армейских корпусов и их органов управления. Шесть из них должны находиться в высокой степени готовности к применению, три – в пониженной. В составе морского компонента сил универсального применения уже имеется три штаба морского базирования высокой степени готовности, способные управлять группировками сил флота альянса оперативно-тактического уровня [207].

Силы универсального применения будут способны вести одновременно до трех операций (две – оперативно-тактического и одна меньшего масштаба) продолжительностью до двух лет. В таких операциях с самого начала предполагается использовать силы высокой го-

товности, а силы пониженной готовности будут обеспечивать их плановую ротацию (контингентов сухопутных войск и ВМС – через каждые полгода, а ВВС – через три месяца) [207].

Военно-воздушных сил блока реорганизация коснулась незначительно. По оценкам руководства НАТО, они в настоящее время могут, в соответствии с требованиями альянса, вести военные действия любого характера и масштаба [207].

3. В-третьих, осуществляя общее сокращение своих ОВС, альянс на саммите в Праге принял решение создать силы первоочередного задействования численностью более 20 тыс. военнослужащих. Это высокомобильные формирования, состоящие из сухопутного (бригадного состава), воздушного (две-три эскадрильи боевой авиации) и морского (одна-две авианосные ударные группы) компонентов. Силы специального задействования предназначены для решения широкого круга задач, включая операции по борьбе с терроризмом. Они позволят осуществлять глобальный контроль за военно-политической обстановкой в мире и оперативно реагировать на внезапно возникающие кризисы. Эти силы должны осуществлять развертывание в любой точке земного шара в течение 5–30 суток. Находиться они будут поочередно в подчинении объединенных командований «Север», «Юг» и «Запад» [207].

Таким образом, НАТО, внедряя концепцию сетецентрической войны, с одной стороны, ведет сокращения числа штабов и органов управления, а с другой стороны – параллельно создает более гибкие и эффективные объединенные оперативные формирования на многонациональной основе. При этом главное внимание альянс уделяет специальным силам, (десантным) и авианосным ударным группам, расширению возможностей ВВС, как при нанесении дальних ударов, так и при обеспечении наземных операций, усилению маневренных сухопутных соединений, способных вести наступательные действия.

3.3. Вооруженные силы Израиля

Все без малого 60 лет своего существования Израиль находится в состоянии войны. Не случайно его вооруженные силы считаются своеобразным полигоном, на котором апробируются новейшие стратегические идеи и военные технологии. В ходе многочисленных, разных по масштабу вооруженных конфликтов армия страны приобрела богатейший опыт, который аккумулирован в военной доктрине. Для Израиля сетецентрические войны являются не абстрактными конфликтами

будущего, а фактически современным этапом стратегии применения компактных вооруженных сил, оснащенных современными информационными системами самого высокого уровня.

До недавнего времени строительство национальных вооруженных сил шло в соответствии с военной доктриной, принципы которой были разработаны еще создателями государства Израиль, в частности первым премьер-министром страны Д. Бен-Гурионом. Основные ее положения были следующими [210].

1. Израиль должен превосходить любой противостоящий ему блок арабских государств качеством вооружений, а также уровнем боевой подготовки военнослужащих.
2. Небольшие регулярные вооруженные силы должны быть обеспечены необходимым числом резервистов, которые ежегодно проходят боевую подготовку и в случае войны могут быстро пополнить свои подразделения.
3. Армия должна гарантированно одержать победу в широкомасштабной обычной войне, в которой задействованы мотопехотные, танковые и авиационные соединения, включающие в себя тысячи единиц боевой техники.

В военном строительстве Израиль достиг впечатляющих результатов – ударная мощь его армии (армия обороны Израиля – ЦАХАЛ) не уступает, а по ряду показателей превосходит суммарную военную мощь европейских стран НАТО; мобилизационные ресурсы Израиля выше мобилизационных ресурсов такого государства, как Германия; израильская военная промышленность – один из крупнейших в мире производителей и экспортеров высокотехнологичных вооружений. Вместе с тем содержание такой армии является экономически довольно обременительным. Военные расходы составляют значительную часть ВВП. К тому же население Израиля выросло с 600 тыс. до 7 млн чел., и нынешний ежегодный призыв новобранцев в соответствии с Законом о всеобщей воинской обязанности просто превышает потребности армии [210].

О необходимости кардинального реформирования вооруженных сил заговорили еще на рубеже 80–90-х гг. прошлого века. Генератором новых идей был генерал Д. Шомрон, занимавший с 1987 по 1991 г. пост начальника Генштаба ЦАХАЛа. Он автор сейчас широко используемого термина «маленькая умная армия». Д. Шомрон предлагал радикально обновить, сделать более эффективными средства ведения войны и одновременно сократить армию и военные расходы. Тогда эта идея не получила поддержки [210].

На рубеже третьего тысячелетия Израиль столкнулся с новыми угрозами. Это, прежде всего, международный, в частности палестинский, терроризм и стремление враждебных Израилю режимов тем или иным способом заполучить оружие массового поражения. Известно, например, что Иран, открыто провозгласивший своей целью уничтожение еврейского государства, близок к созданию ядерной бомбы [210].

Эти угрозы вынудили руководство страны пересмотреть доктрину национальной безопасности и начать глобальную реформу армии Израиля – ЦАХАЛа. Основные направления, по которым будут произведены наиболее радикальные реформы - это разведка, активные действия в киберпространстве, оснащение вооруженных сил современным вооружением (прежде всего, высокоточным оружием и системами ПВО). Все реформы пройдут на фоне серьезных бюджетных сокращений. Планируется увольнение части военнослужащих, сокращение нескольких эскадрилий и танковых частей. При резко снижаемом количестве и продолжительности полевых учений уделяется особое внимание технологическому оснащению боевых частей. Программа сокращений сделает армию количественно меньше, но качественно лучше.

Цель реформы – подготовить вооруженные силы к будущим конфликтам в соответствии с концепцией сетецентрической войны. При этом предполагается, что вооруженным силам Израиля, прежде всего, придется иметь дело с мятеж-войной, в которой будут участвовать разрозненные террористические группы, скрывающиеся в населенных пунктах с многочисленным, сочувствующим террористам населением. Такие группы способны нанести тяжелый урон противнику, особенно если в их руках окажется оружие массового поражения. Другой тип вероятной войны – столкновение с географически удаленными государствами (прежде всего, Ираном), стремящимися завладеть ядерным оружием и средствами его доставки [210].

Современные войсковые операции имеют ту особенность, что в них совместно под единым командованием действуют относительно небольшие пехотные, танковые и авиационные части, оснащенные высокотехнологичным оружием и средствами связи. Надо отметить, что эффективность войсковой интеграции была продемонстрирована еще в ходе начавшейся в 2000 г. палестинской интифады. Столкнувшись тогда с невозможностью по гуманитарным соображениям проводить массированные войсковые операции в палестинских городах, служивших базами для террористов, израильское командование избрало путь

точечных ударов по базам боевиков с использованием интегрированных сухопутных и авиационных подразделений, вооруженных высокотехнологичным оружием. В связи с этим одной из задач реформы является максимальная интеграция различных военных структур.

В соответствии с программой реформирования масштабное перевооружение пройдет в ВВС, которое получило самые большие средства из бюджета на приобретение новой техники. ВВС было выделено более миллиарда долларов, из них 200 млн на доведение хорошо показавших себя в операциях по ликвидации террористов ударных вертолетов Apache до уровня противотанковых Apache Longbow.

Так же реформирование пройдет в военной разведке, которая получила финансирование в объеме 600–700 млн долл. на совершенствование системы сбора информации. Ведется модернизация системы распределения информации и доведения ее до низового командного состава – так называемой системы «sensor-to-shooter». Планируется запуск новых космических аппаратов оптико-электронной разведки и связи, а также приобретение большого количества БПЛА самого различного назначения (разведки, ударных, связи и ретрансляции). Предусмотрено создание системы «Цифровая сухопутная армия» для единого управления всеми тремя родами войск [210].

Масштабы и темпы военной реформы заметно возросли в 2004 г, когда должность начальника генштаба занял генерал Д. Халуца. В своем плане реорганизации армии Д. Халуц предусматривал сокращение оборонного бюджета, а также укрепления израильских ВВС как стратегической доминанты за счет сокращения сухопутных войск. Произойдет интеграция, по крайней мере, четырех родов войск: пехотных, танковых войск, войск связи, тылового командования. Будут расформированы службы тылового командования и ликвидировано Управление планирования (с передачей его функций аппарату заместителя начальника генштаба). Все эти сокращения позволят перебросить значительные средства на оснащение армии высокотехнологичным оружием и повышение уровня боевой подготовки [210].

В соответствии с прежней моделью управления войсками генеральный штаб осуществлял непосредственное руководство сухопутными войсками и ВМС, тогда как, например, ВВС управляло командование и штаб ВВС. Теперь на базе сухопутных войск будет сформировано отдельное командование сил наземного базирования, а генштаб займется стратегическим планированием, управлением и координацией действий как наземных и военно-морских, так и военно-воздушных сил. В состав командования сил наземного базирования войдут броне-

танковые войска, войска связи, инженерные войска, войска ПВО, тыла, а также ряд ключевых управленческих органов: управление личного состава армии, управление стратегических вооружений и управление стратегического планирования. Тем самым значительно сократится число звеньев управления войсками, что повысит оперативность принятия решений и их качество. За счет совмещения, ранее дублировавших друг друга штабных и тыловых структур, произойдет заметное сокращение аппарата. Освободившиеся материальные ресурсы пойдут на укрепление боевых частей и соединений [210].

Реформа затронет и условия прохождения службы. За счет уменьшения срока пребывания военнообязанных в резерве число резервистов сократится на 60 тыс. чел. Срок действительной службы будет постепенно снижен с нынешних трех лет до одного года восьми месяцев, что приведет к сокращению численности личного состава регулярной армии. За период с 2005 по 2008 г. значительные сокращения прошли в войсках тылового обеспечения – из них уволены почти три тысячи офицеров и сержантов сверхсрочников. Это стало возможным благодаря передаче ряда функций тылового обеспечения, таких как продовольственное и вещевое снабжение войск, ремонт автомобильной, ряда категорий броне- и авиационной техники, гражданским фирмам на конкурсной основе [210].

В процессе реформы не планируется переход к полностью профессиональным вооруженным силам, так как армия в Израиле считается одним из главных государственных институтов, и престиж военной службы весьма высок, а потому отказ от призыва может быть негативно воспринят обществом. Однако планируется увеличить кадровый состав боевых частей и значительно поднять уровень их оснащенности новейшим вооружением, средствами связи и управления. Особое внимание уделяется улучшению качества и увеличению численного состава разведывательных и специальных подразделений израильской армии, авиации и флота. На их основе в будущем планируется создание единых разведывательно-диверсионных мобильных сил быстрого реагирования, способных превентивными ударами влиять на исход войн и вооруженных конфликтов. При этом значительная роль отводится современным системам связи и управления, являющимся средством интеграции всех организационных структур армии. Уже сейчас портативные компьютеры, оборудованные средствами радиосвязи, стали стандартным элементом оснащения израильского бойца [210].

Наряду с ВВС и разведкой быстрыми темпами будет развиваться ВМФ, ранее не игравший в ЦАХАЛе заметной роли. Включение в его состав трех подводных лодок типа Dolphin и приобретение в Германии еще двух подлодок этого класса, способных нести крылатые ракеты морского базирования большой дальности и выполнять автономные плавания в любую точку Мирового океана, превратили израильский ВМФ в стратегический вид вооруженных сил [210].

Для защиты войск и населения Израиля от ракетных ударов создана и непрерывно развивается многоуровневая система ПРО, получившая название «Хома». В ее состав входят система обнаружения и оповещения на основе радиолокационных станций Green Pine, противоракетный комплекс «Хец» для борьбы с баллистическими ракетами, высокоэнергетический лазер «THEL» для поражения ракетных систем залпового огня, современные БПЛА с повышенным временем патрулирования (до двух суток) для обнаружения и оповещения о нападении, а также ударные БПЛА – носители противоракет [210].

Особое внимание уделяется развитию систем космической связи и разведки, функционирующих в интересах информационного обеспечения всех звеньев управления. По этой причине военные космические программы в Израиле выделены в отдельное приоритетное направление совершенствования боевых средств, а в главном штабе ВВС создано управление космических войск. Оно, в частности, отвечает за разработку и пуск космических аппаратов разведки, спутниковой связи, а также за сбор и обработку данных, поступающих от космических средств [210].

Фактически в результате реформирования ЦАХАЛ в максимальной степени стал соответствовать армии, воплощающей основные принципы сетецентрической войны.

3.4. Вооруженные силы Китайской Народной Республики

Руководство вооруженных сил Китая внимательно следит за всеми шагами США в области совершенствования своей «военной машины», а также внедрения новых технологий в военную сферу. Более того, китайские теоретики рассматривают вооруженные силы США в качестве эталона в области осуществления информационного обмена и применения новых информационных технологий [43, 177].

Изучая американский опыт, военное руководство Китая начало разработку доктрины применения новых информационных технологий в военной сфере. Более того, в вооруженных силах Китая формируется новая сетецентрическая архитектура построения боевых формирований, способных эффективно выполнять поставленные задачи в конфликтах ограниченного масштаба. Объясняется это уверенностью китайских военных специалистов в том, что успеха в современных и будущих операциях XXI в. можно будет достичь только при условии предоставления всем участникам боевых действий (операций) возможности использовать данные интегрированной системы боевого управления, связи, компьютерной техники, разведки и наблюдения C4ISR. В документах народной освободительной армии Китая (НОАК) концепция сетецентрической войны получила наименование «Интегрированная и электронная война» (Integrated Network-E1ectronic Warfare). Данная концепция предусматривает проведение как наступательных, так и оборонительных действий. Вместе с тем американские военные аналитики отмечают превалирование в ней первых над вторыми. В частности, в рамках реализации концепции осуществляется разработка лазерного оружия для борьбы с космическими аппаратами вероятного противника, а также собственных навигационных систем космического базирования, прорабатываются вопросы создания интегрированных систем управления, связи и разведки, которые должны позволить применять баллистические ракеты в неядерном оснащении для борьбы с авианосными группировками ВМС США [43].

Высшее командование НОАК активно внедряет новые принципы управления, проверяет их на полевых учениях, а также осуществляет закупку новой техники, содержащей самые инновационные технологические решения. Более того, новые информационные технологии внедряются и в старые образцы боевой техники, что позволит адаптировать и привести их к необходимому уровню информационного взаимодействия.

Возможно, наиболее ярким отражением долгосрочных планов военного руководства Китая в отношении создания интегрированной системы боевого управления, связи, компьютерной техники, разведки и наблюдения является высказывание бывшего начальника генерального штаба ВС Китая (1992-1995 г.) генерала Джан Ваньнянь (Zhang Wannian). Он отмечал, что «система боевого управления и связи должна быть интегрирована и связана единой сетью для повышения эффективности боевых формирований, а также что этот процесс должен сопровождаться одновременным снижением количества уровней

управления» [43, 180]. Генерал, изучая опыт ВС США, указывал, что «процесс «цифровизации» и объединения сетей позволяет снизить количество уровней управления с пяти до трех». Он также предположил, что ВС Китая смогут рассчитывать на такой же эффект, объединив свои органы управления и участников боевых действий в единую сеть.

Теория военного искусства в Китае фокусируется на исследовании войны в пяти сферах. Пять сфер боевого пространства включают в себя: землю, море (в том числе и подводное пространство), воздушное, космическое и электромагнитное пространство (некоторые китайские эксперты вместо электромагнитного пространства выделяют информационное пространство или сферу) [43, 181]. Именно внедрение перспективных информационных технологий в военное дело позволит не просто повысить эффективность систем боевого управления, связи, вычислительной техники и разведки во всех сферах боевого пространства [43, 182], но и полностью пересмотреть устоявшиеся взгляды на традиционные уровни системы боевого управления и связи [43, 183]. Также существует мнение, что вооруженные силы должны сами структурироваться вокруг «неявных возможностей информации» [43, 184]. Это означает, что революция в военном деле должна наступить уже после внедрения перспективных информационных систем и привести к реформированию ВС с изменением организационно-штатных структур формирований, а также форм и способов их применения.

Среди сфер боевого пространства китайские эксперты особое внимание уделяют космосу, утверждая, что ВС КНР должны быть готовы к ведению там полноценных боевых действий, а контроль за космосом позволит достичь невиданной до этого мощи вооруженных сил и выиграть как информационные войны, так и обычные сражения. Генерал-майор Джан Лин (Zhang Ling) утверждал, что воздействие в космической сфере может быть осуществлено как «мягким» воздействием против информационных систем космического базирования, так и за счет физического уничтожения космических аппаратов противника [43, 185]. Уточняя формы воздействия, он подчеркивал, что «в космосе на удалении 120 км от земной поверхности нет разграничения по территориальным и государственным признакам, поэтому воздействие должно носить глобальный характер». Другие китайские исследователи Сунн Юнсинь и Го Ичжин (Song Yongxin и Guo Yizhing) делали похожие заявления. Они соглашались, что война в космосе будет неотъемлемой частью информационной войны и что контроль косми-

ческого пространства позволит получить преимущества и перехватить инициативу в будущих сражениях [43, 186].

Обсуждая применение перспективных информационных технологий в военной сфере, китайские эксперты отмечают довольно распространенное заблуждение, а именно – снижение значимости человеческого фактора. По их мнению, наоборот, никакая на данный момент и ближнесрочную перспективу самая современная система (хотя подобные разработки ведутся полным ходом) не заменит человеческий мозг. В настоящее время действительно можно говорить о снижении человеческого участия, но только при решении некоторых задач, а вот от участия человека в принятии решения на поражение еще очень долго никто не откажется. Таким образом, внедрение информационных технологий, по мнению китайских военных экспертов, нисколько не умаляет значение оператора, наоборот, необходимо прилагать серьезные усилия, чтобы командиры (да и весь личный состав) получали необходимые знания и опыт в работе с современными информационными системами.

Внедрение перспективных информационных технологий в военную сферу, а также переход к новым принципам управления войсками и силами позволят в будущем получить не только преимущества в управляемости частей и подразделений на поле боя, а также в ведении разведки, но и окажет положительное влияние на боевые возможности формирований.

Так, Синь Цинь (Xin Qin) в своей книге «Война в информационном веке» отмечал, что современные информационные решения важны для повышения эффективности системы боевого управления и связи, а также помогут повысить маневренность и, в конечном счете, боевые возможности формирований [43, 187]. Более того, в работах еще 1994 г. китайские авторы соглашались, что информационные технологии являются ключевым связующим звеном для интеграции не только систем боевого управления, связи, но и всех участников военных (боевых) действий [43, 188].

На проводимых практически во всех военных округах учениях военные специалисты Китая осуществляли моделирование продолжительных боевых действий и исследовали работу центров и пунктов управления. В одном из таких сценариев они специально смоделировали высоко цифровизированную группировку войск противника, которая противостояла и успешно разгромила формирования НОАК, имеющие существенные ограничения в системе боевого управления, связи, вычислительной техники, разведки и наблюдении

C4ISR [43, 189]. Проводимые учения были призваны показать дивизионному командованию эффект от интегрированной в единую сеть систем разведки и боевого управления. Такие интегрированные системы позволяли войскам противника с высокой точностью поражать силы НОАК еще в местах их сосредоточения до момента развертывания в боевые порядки. По результатам учений военным руководством Китая было принято решение о необходимости цифровизации и объединения в единую сеть всей системы боевого управления и связи вооруженных сил [43, 190].

В настоящее время у Китая имеются средства боевого управления, связи, компьютерной техники, разведки и наблюдения C4ISR национального (стратегического) и регионального (оперативного) уровняей [43].

Автоматизированная система боевого управления и связи уровня военных действий воплощена в системе «Цюй Дянь» (Qu Dian). По мнению американских экспертов, это несколько избыточная и сложная система уровня военного округа и ниже, связывающая генеральный штаб и главные штабы видов ВС, службы и рода войск со штабами региональных (окружных) командований. Китай начал развертывание системы «Цюй Дянь» по юго-восточной границе еще в 1990 г. Сейчас эта система способна обеспечивать эффективные действия объединенных группировок наземного, воздушного и морского базирования. По данным европейских спецслужб, принцип ее работы похож на принцип функционирования американской объединенной системы распределения тактической информации JTIDS (Joint Tactical Information Distribution System), используемой США и союзниками для связи и обмена разведывательной информацией между самолетами, кораблями и наземными формированиями союзных войск в военное время. В настоящее время наземная подсистема «Цюй Дянь» в юго-восточном Китае ориентирована на обеспечение операций (боевых действий) в возможном конфликте с Тайванем. Она обеспечивает связью войска Нанкинского (Nanjing) и Гуаньчжоуского (Guangzhou) военных округов и включает в себя объединенный оперативный центр боевого управления, связи, вычислительной техники, разведки и наблюдения Joint Operation C4I Centre (JOC), способный своевременно передавать приказы и команды по всей цепочке управления и обеспечивать разведывательной информацией органы принятия решения национального уровня и уровня округа. Объединенный оперативный центр имеет прямые каналы связи с центрами боевого управления, связи, вычислительной техники, разведки и наблюдения C4ISR

Нанкинского и Гуаньчжоуского военных округов, штабами ВМС, кораблями в Восточном море, разведывательным центром подводных сил и др. Система также позволяет командованию округа формировать и отображать единую картину оперативной обстановки, объединять и коррелировать разведывательные данные от средств наземной, воздушной, морской и космической разведок и осуществлять дальнейшее их доведение до подчиненных формирований. Задействуемая аппаратура способна осуществлять контроль за большим количеством разнообразных средств разведки, включая спутники ОЭР и РЛР, самолеты ДРЛО, РЭР, РЭБ, разведывательные корабли, наземные станции разведки и др. [43, 199].

В состав системы боевого управления «Цюй Дянь» помимо наземной подсистемы входят связные космические аппараты, получившие наименование «Фэн Хо-1» (FengHuo-1-FH-1). Первый спутник связи был запущен в 2000 г., второй – в 2003 г. Пентагон характеризует систему как закрытую, помехозащищенную, с возможностью передачи больших объемов информации. Частотный диапазон аппаратуры космических аппаратов обеспечивает функционирование в С-диапазоне и УВЧ-диапазоне [43].

В ближайшие несколько лет Китай получит и перспективную космическую систему разведки для обеспечения действия боевых формирований. Так, по данным ежегодного доклада Military power of the people's republic of China 2009, подготовленного министерством обороны США, Китай осуществляет развертывание перспективных КА видовой разведки серий «Чжиюань-2» (Ziyuan-2), Яогань-1 (Yaogan-1) и 2, «Хайян-1В» (Haiyang-1B), CBERS-1 и -2, а также космической группировки КА наблюдения за земной поверхностью, формируемой по программе «Хуаньцзин» (Huanjing). В составе группировки «Хуаньцзин» планируется иметь 11 КА ИК- и радиолокационной разведки (РЛС с синтезированием апертуры). В скором времени можно ожидать появления у Китая собственных спутников фоторазведки высокой разрешающей способности, а также средств наблюдения за морскими акваториями и др. [43, 200].

Глобальное военное противостояние между США и КНР сегодня военно-политическим руководством Китая признается маловероятным, а вот конфликты ограниченного масштаба считаются неизбежными, и их наличие связывается с растущей конкуренцией за источники сырья и сферы влияния. Не случайно среди возможных причин возникновения войн (защита социалистического строя, борьба с гегемонией США, территориальные споры и пр.) в китайской военной

доктрине появилась новая – топливно-сырьевой кризис. Число конфликтов ограниченного масштаба, как считают в Китае, будет расти, и расцениваются они как полезное и даже прогрессивное явление, поскольку позволяют разрешать противоречия на раннем этапе, когда в боевые действия еще не вовлечено большое число участников [204, 211].

Классификацию военных конфликтов китайские специалисты проводят по следующим параметрам (рис. 3.3):

- тип противоречий;
- масштаб конфликта;
- применяемые средства вооруженной борьбы;
- характер политических целей;
- географические особенности ТВД и характер действий сторон.

Цели ведущих стран в конфликтах, которые в период до 2015–2020 гг. по оценкам Пекина будут носить ограниченный, локальный характер, предполагаются следующие [204]:

- защита территориальной целостности (борьба с разного рода сепаратистскими движениями);
- отстаивание спорных территорий и других интересов в том или ином регионе мира и т. п.

Поскольку во всех этих случаях речь не идет об угрозе самому существованию государства или его жизненным интересам, то перерастание конфликтов такого рода в крупномасштабные и тем более в глобальные маловероятно. Вооруженные силы КНР в локальных конфликтах будут стремиться не к полному разгрому противника, а к реализации поставленных руководством страны политических целей и задач. В обозримом будущем, по мнению китайских аналитиков, локальные войны вряд ли выйдут за рамки среднего и малого масштаба. Охватываемый ими театр военных действий на суше будет в основном ограничен оперативной глубиной, т. е. одним или двумя большими военными округами [204, 211].

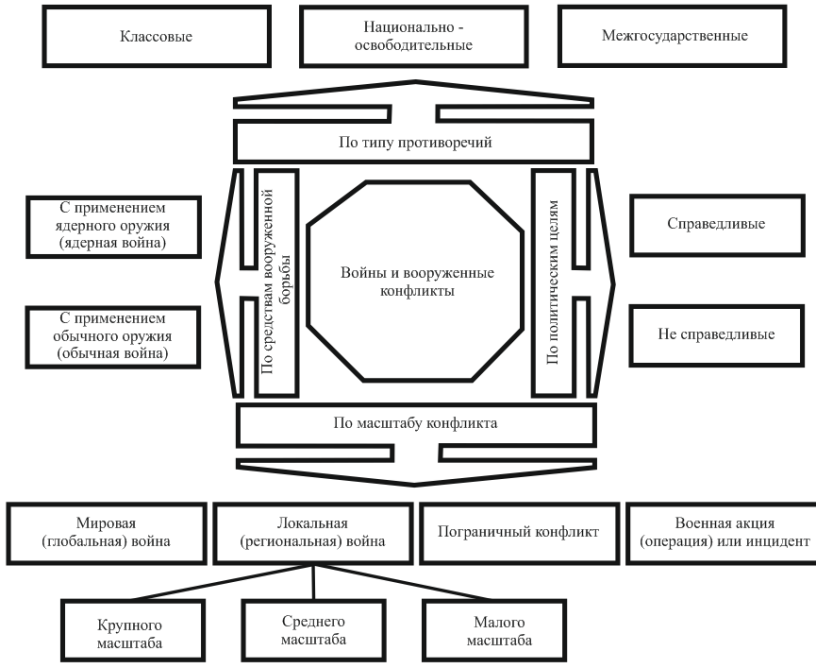


Рис. 3.3. Классификация военных конфликтов

Локальная война среднего масштаба – это, по китайской классификации, военный конфликт, в который с обеих сторон вовлечено от 500 тыс. до 1 млн чел. Примером его может служить война между Китаем и Вьетнамом 1979 г., в которой участвовало около 700 тыс. чел. [204, 211].

Малая локальная война – это военный конфликт, в котором общая численность войск не превышает 500 тыс. Типичным примером такой войны считается пограничный конфликт, наподобие разгоревшегося в 1962 г. между Китаем и Индией. В нем участвовало с обеих сторон не более 70 тыс. чел.

В китайской классификации будущих конфликтов по средствам вооруженной борьбы особое место отводится так называемым обычным высокотехнологичным войнам, т. е. войнам, в которых широко применяются высокотехнологичные средства и, прежде всего, высокоточное оружие в обычном снаряжении (без применения ядерных боеголовок) [211, 212]. Именно этот вид войн, как считают в Китае, будет основным в рассматриваемый период, и страна должна к ним готовиться.

Если говорить о целях возможных локальных войн, то они, согласно воззрениям китайских политиков, могут быть следующими:

- отражение вооруженной агрессии;
- наказание противника (восстановление справедливости и ликвидация угрозы со стороны соседних стран);
- разрешение пограничного конфликта;
- разрешение споров за морские границы и островные территории.

Прогноз военно-стратегической обстановки до 2020 г. заставил военное руководство Китая пойти на глубокое реформирование армии. Здесь точкой отсчета служит 1985 г., когда было принято решение переориентировать военное строительство с подготовки к мировой (обычной или ядерной) на локальные войны.

В настоящее время своей главной задачей военно-политическое руководство Китая видит в подготовке армии к ведению небольших по масштабам, но интенсивных и скоротечных боевых действий в пограничных районах. В соответствии с военной доктриной КНР основной стратегией ВС будет активная оборона, т. е. проведение оборонительных операций и овладение инициативой после ударов противника [211].

При этом Китай готовит свои ВС к проведению наступательных операций для перехвата инициативы, в том числе и при любом сценарии развития ситуации с Тайванем и нанесении решительного поражения, как ВС Тайваня, так и его возможным союзникам, в том числе и США.

В настоящее время Китай активно занимается преобразованием своих ВС «из армии количественного состава в армию качественного превосходства». Согласно плану реорганизации все ветви вооруженных сил будут входить в объединенное военное командование. Ведется реорганизация существующей административной системы и системы оперативного командования армией с целью повышения их эффективности. Как полагают аналитики [304], сейчас в действующей окружной системе командование различных уровней остается достаточно изолированным, что усложняет централизованное управление большими группами войск и препятствует эффективному использованию современных систем вооружений. Объявленной военной реформой предусмотрены преобразования в семи военных округах. В настоящее время их основная задача – проведение крупномасштабных наземных операций, которые уже считаются маловероятными. В этой связи численность данных крупных воинских объединений, вероятно,

будет сокращена. Особый упор будет сделан на развитие ВМС как гарантию надежной защиты геополитических интересов Китая практически во всей акватории Тихого океана. По завершении реформы, к 2020 г., ВС КНР будут способны вести все виды войн против любого противника [204, 211, 214, 304].

Реализация планов преобразования НОАК будет осуществляться в соответствии со следующими установками [211]:

- рост боевых возможностей ВС, в первую очередь, за счет переоснащения их перспективным, высокотехнологичным оружием до уровня, позволяющего вести локальные войны любого масштаба;
- доведение оперативных, огневых, маневренных и разведывательных возможностей ВС до уровня ведущих стран;
- сокращение общей численности ВС (прежде всего, за счет уменьшения числа пехотных дивизий и увеличения относительного веса ВВС и ВМС);
- сохранение сухопутных войск как самого многочисленного вида ВС, предназначенного для решения основных задач по разгрому противника;
- сохранение воинской обязанности как основного принципа комплектования;
- приоритетное оснащение войск высокоточным оружием, автоматизированными системами управления (завершение развертывания единой АСУ ВС) и современными средствами связи и разведки;
- упор в подготовке ВВС к действиям оперативного и оперативно-стратегического масштаба, которые могут проводиться как в тесном взаимодействии с формированиями других видов ВС, так и в рамках самостоятельной воздушной наступательной операции;
- создание эффективной в условиях информационной войны системы управления войсками и оружием;
- совершенствование всех трех составляющих ядерной триады и, прежде всего, стратегических вооружений наземного базирования;
- обретение способности вести разновидовыми группировками всесторонне обеспеченные военные действия ограниченного масштаба за пределами национальной территории;
- повышение способности оперативных формирований к огневому поражению, особенно на больших дальностях, в

первую очередь, за счет быстрого роста числа соединений, оснащенных реактивными системами залпового огня крупного калибра, тактическими и оперативно-тактическими ракетами;
- сохранение мобилизационной базы масштабного развертывания ВС в случае возникновения глобального военного конфликта;
- развитие флота до уровня, позволяющего вести действия оперативного масштаба в океанской зоне в пределах Тихоокеанского ТВД.

Реформа ВС Китая, повторяя в главных чертах реформы, которые проводят западные страны, имеет ряд существенных особенностей. Ее, в частности, отличает долгосрочность планирования (до 2050 г.) и глобальность замысла – к середине XXI столетия страна «должна иметь вооруженные силы, достойные великой державы», способные «победить в любой войне любого противника». Отличает китайские реформы и ориентация на приоритетное развитие ВМС. Это обусловлено стремлением Китая распространить свой суверенитет на Тайвань, а также тем фактом, что экономическое процветание страны зависит от доступа к морским ресурсам и коммуникациям [204, 211, 214].

Необходимо также отметить, что китайское руководство попрежнему относит США к числу своих главных противников и не исключает возможности вооруженного столкновения с ним в большем или меньшем масштаба. Потому в ходе реформ настойчиво предпринимаются попытки найти пути так называемого асимметричного строительства ВС, с тем чтобы уже в ближайшем будущем армия могла адекватно ответить на возможные действия США. Основной упор ассиметричного строительства делается на развитие средств и способов информационной войны. Информационную войну китайские официальные документы определяют как «переход от механизированной войны индустриального общества к войне решений и стиля управления, войне знания и войне интеллекта». В рамках этой доктрины китайские ВС развивают концепцию сетевых сил – воинских подразделений численностью до батальона, укомплектованных высококлассными специалистами, владеющими передовыми компьютерными технологиями [204, 211, 214].

В настоящее время продолжается переоснащение войск наиболее перспективными, высокотехнологичными системами оружия. Руководствуясь новой стратегической доктриной, ВС Китая в течение

ближайших 15 лет планируют развернуть пять больших современных систем вооружений [211].

1. Система вооружений стратегического устрашения и сдерживания (ядерного возмездия).
2. Система стратегической разведки раннего предупреждения и оповещения о возможном нападении.
3. Система противовоздушной и противокосмической обороны (планируется создать орбитальную космическую группировку ПРО, наладить производство высокоточных боевых систем дальнего радиуса действия и поставить на вооружение оперативно-тактические ракеты высокой точности).
4. Система борьбы с авианосными ударными группами. Основной упор здесь делается на строительство авианосцев среднего водоизмещения и многоцелевых ударных подводных лодок, которые станут основой мощного подводного флота, способного вести успешную борьбу с авианосными ударными группами противника в акваториях, прилегающих к Китаю, и зонах его экономических интересов.
5. Система нападения и защиты в киберпространстве.

В последние годы, по некоторым данным, производство вооружения в КНР выросло в несколько раз. НОАК стремительно перевооружается, при этом сокращается количество личного состава. Вместо людской массы ставка сделана на высокотехнологичное современное вооружение. Оборонный бюджет КНР – второй по величине после США. Страна усиленно занялась развитием оборонно-промышленного комплекса. Возникли десятки конструкторских и специализированных научных бюро, строились предприятия ОПК. Компартия поставила задачу из категории догоняющих – перейти в мировые лидеры производителей вооружения. Самый быстрый способ осуществить этот переход – это покупка технологий, копирование и промышленный шпионаж. Особенностью китайского ОПК является большое количество прототипов и вариантов вооружения и военной техники. При этом если ранее это были копии в основном российского вооружения, то сейчас это – вооружение полностью китайской разработки. В настоящее время высокоточное оружие, управляемые снаряды, средства связи, навигации, автоматизированные системы управления огнем – все это китайцы проектируют и производят самостоятельно [205].

Китай активно наращивает экспорт вооружения и уже вышел на пятое место в мире по экспорту вооружения и военной техники. При этом продолжается уверенное наращивание объема продаж. Ки-

тайское вооружение отличает невысокая, по сравнению с аналогами, цена. Небогатые страны охотно покупают дешевое китайское оружие. В основном это страны Азии, Ближнего Востока и Африки, причем в последнее время к ним прибавилась Латинская Америка [205].

В Китае досконально изучают всю информацию об экспериментальных учениях и опыте применения формирований в вооруженных конфликтах, отслеживают любые материалы, связанные с внедрением перспективных информационных технологий в военное дело и уставные документы по принципам реализации новых сетецентрических концепций. При этом особое внимание уделяется организации объединенных действий и повышению эффективности группировок.

Например, сотрудники национального военного университета науки и техники (PLA's National Defense University of Science and Technology г. Чанша) занимаются исследованием влияния информационных технологий на повышение боевых возможностей формирований, а также вопросами их внедрения в войска и системы оружия. В других китайских военных учебных заведениях также проводятся изыскания по подобной тематике.

Некоторое время назад в морском инженерном институте НОАК была опубликована работа по анализу путей более эффективного применения систем боевого управления, связи, компьютерной техники, разведки и наблюдения в боевых условиях. В военно-морской академии (Navy Command Academy) китайские офицеры активно исследуют новые возможности применения систем C4ISR для обеспечения наступательных действий НОАК. Одним из основных оперативных вызовов Китаю со стороны американской военной машины является превосходство США в воздухе и в том числе благодаря авианосным ударным группам. В связи с этим в одной из работ военно-морской академии КНР рассматривался вопрос интеграции средств управления, связи, разведки и баллистических ракет в неядерном оснащении для поражения авианосных группировок противника. Такое комбинированное применение средств летального (кинетического) и нелетального поражения должно позволить НОАК эффективно преодолевать систему ПРО противника и наносить удары по авианосным группировкам и базам ВМС. В то же время американские морские офицеры скептически относятся к идее военного руководства КНР применять баллистические ракеты для поражения развернутых авианосных ударных групп (АУГ) в районах предназначения. Они обосновывают это тем, что Китай не имеет необходимых космических средств обнаружения АУГ в Мировом океане, кроме того, головные

части их ракет не могут маневрировать. Вместе с тем китайские специалисты считают идею применения баллистических ракет с неядерным оснащением для поражения авианосных группировок довольно привлекательной и перспективной [43, 192, 193].

Более того, в инженерном училище ракетных войск (Second Artillery Engineering College) проводились исследования на предмет усложнения траектории движения боеголовок для осуществления самостоятельного поиска, захвата и поражения цели, в роли которой выступала авианосная ударная группа АУГ [43, 194]. Исследования показали, что обеспечение ИК-наведения боеголовок на конечном участке траектории позволяет увеличить возможный радиус и точность поражения.

Для Китая, который не имеет хорошего ракетного вооружения большой дальности для борьбы с морскими целями и подходящих воздушных носителей, такой способ применения баллистических ракет с неядерным оснащением имеет смысл. По мнению офицеров академии ракетных войск (Second Artillery Command Academy), такие системы крайне необходимы хотя бы потому, что баллистическими ракетами может производиться пуск по любому объекту (цели) на Земном шаре, в то время как на проведение такого же удара средствами стратегической авиации или крылатыми ракетами может потребоваться от нескольких часов до нескольких дней. Управляемое ракетное вооружение может стать козырной картой в достижении победы в высокотехнологичной войне. Необходимым условием реализации подобной концепции является не только комплексное использование мер противодействия, в том числе и применение ложных головных частей, обеспечение точными данными целеуказания, но и обязательное задействование космических средств разведки, связи и управления, что и предусмотрено перспективной сетецентрической концепцией [43, 195, 196, 198].

Обсуждая потенциальные угрозы для США со стороны таких систем, американский конгрессмен Б. Шаффер отметил, что наличие баллистических ракет высокой точности, а также техническая возможность наблюдать за ВС США из космоса теоретически может позволить Китаю осуществлять атаки авианосных ударных группировок, как в портах, так и в открытом океане. Кроме того, такие возможности по интеграции систем боевого управления и связи достигнуты Китаем именно благодаря развертыванию группировки связных космических аппаратов, а также перспективных средств разведки и наблюдения [43].

Рис. 3.4. Дальность действия баллистических ракет ВС Китая

Реализация сетецентрической концепции в Китае вызывает у американских экспертов серьезную озабоченность. «Неважно, как они скопируют и адаптируют под свои нужды нашу концепцию сетецентрической войны, важно, что они в разы повысят инвестиции в разработку перспективных средств разведки и ВТО», – отмечают американские специалисты. Итогом реализации концепции сетецентрических войн в НОАК станет технологический прорыв, который обеспечит китайцам необходимый уровень ситуационной осведомленности и понимания обстановки на поле боя (в боевом пространстве). Вследствие этого американские группировки будут вскрыты, а это (при наличии необходимых средств высокоточного оружия дальнего действия) равносильно их поражению. В технологической сетецентрической гонке обе стороны (США и Китай) могут довести уровень применения перспективных информационных средств и систем до логического завершения, когда столкновение двух высокотехнологичных ВС нивелирует само технологическое преимущество, что значительно повысит значимость человеческого фактора и собственно профессионализма [43].

Проводя оценку военного потенциала Китая, ученые и стратеги США оживленно обсуждают вопрос, сможет ли Китай создать угрозу безопасности США и их региональным интересам в Восточной Азии в ближайшие несколько десятилетий. Основной упор делается на сравнении будущих военных возможностей Китая по сравнению с воз-

можностями США и других стран Восточной Азии. Многие специалисты США считают, что Китай может стать «почти равным соперником» США в военной области, однако необходимо иметь в виду следующие факторы [204].

1. Вооруженные силы США размещены на нескольких потенциальных театрах военных действий и не имеют там достаточной плотности для одновременного ведения успешных военных действий.

2. Важным фактором является география потенциального военного конфликта с Китаем. Наличие баз США на Окинаве и в Японии облегчает действия американских вооруженных сил. Но даже при оптимально благоприятных политических условиях переброска американских войск из этих районов займет время. Помимо этого, заранее трудно предположить, сколько времени уйдет на координацию с политической точки зрения и достижение консенсуса между США и Японией относительно того, как этот союз должен отвечать на подобные кризисы.

3.5. Вооруженные силы других государств

В *Австралии* осуществляется разработка новых средств разведки, внедряются перспективные информационные технологии, проводятся испытания беспилотных и роботизированных комплексов и систем для того, чтобы сделать свои немногочисленные вооруженные силы более эффективными. Проводится тестирование перспективных сетевых средств связи и передачи данных, которые должны позволить одному оператору осуществлять управление группировкой робототехнических средств, способных также выходить из сети и действовать автономно в целях решения разведывательных задач или нанесения поражения по выявленным объектам и целям [43].

Во *Франции* подобные мероприятия реализуются в рамках концепции, получившей наименование «Информационно-центрическая война» (Guerre Infocentre), которая в большей степени акцентирует внимание на информационных потоках, а не на самих сетях, как принято у американцев. Первоначально эта концепция реализовывалась в рамках программы «Перспективная воздушно-наземная система боевого управления», она позволяет объединить разнообразные боевые платформы для осуществления мероприятий объединенного огневого поражения целей.

Германия также работает над созданием перспективной системы оснащения и вооружения личного состава Infanterist der Zuknft,

позволяющей реализовать новые принципы управления и связи между боевыми формированиями и вышестоящими органами управления. Проводимые работы включают в себя разработку перспективных средств разведки, персональных компьютерных систем, военных систем управления и связи типа «тактический интернет», позволяющих организовать взаимодействие между аналоговыми средствами связи и цифровыми системами передачи данных [43, 207].

В *Великобритании* формируется собственная глобальная информационная инфраструктура, представляющая собой единую информационно-управляющую сеть, со специализированными системами обеспечения безопасности и единым семейством программного инструментария. В будущем возможности формируемой информационной инфраструктуры планируется расширить и для организации взаимодействия и обеспечения доступа к информационным ресурсам вооруженных сил союзников: США, Канады, Новой Зеландии и Австралии [43].

4. Развитие вооружений, средств, систем и комплексов военного назначения в условиях перехода к концепции сетецентрической войны

Достижения современной науки, техники и промышленности в области создания и производства высокоточных ракет различных классов и назначения, информационных систем и средств военной радиоэлектроники являются той основой, на которой строится вся система вооружения современной армии. Все это, в свою очередь, обусловливает и характер сетецентрической войны, и способы ее ведения, и основы строительства вооруженных сил. Опыт истории свидетельствует о том, что по мере развития науки и техники неуклонно развиваются и средства вооруженной борьбы, военная техника в целом, повышается их роль в войне. При этом именно развитие средств борьбы неизбежно обусловливает изменение способов ведения военных действий. Отличительная особенность развития средств вооруженной борьбы в современных условиях состоит в появлении качественно новых видов оружия и военной техники, в их быстрой информатизации, что резко увеличило боевые возможности последних, привело к коренной ломке организационных форм вооруженных сил и способов ведения военных действий всех масштабов. Именно за счет развития средств вооруженной борьбы произошел переворот в военной стратегии и военном искусстве в целом [289].

4.1. Общие тенденции развития вооружения, военной техники и военных технологий в условиях перехода к концепции сетецентрической войны

4.1.1. Общие тенденции развития вооружения и военной техники

Анализ наиболее резонансных локальных войн и военных конфликтов, происходивших после второй мировой войны, показал, что разрушительная мощь ядерного оружия не исключила военные конфликты, и поэтому потребность в обычных средствах вооруженной борьбы не снижается. Как отмечают зарубежные эксперты, в результа-

те информационно-технической революции плавный, постепенный эволюционный процесс разработки и модернизации ВВТ начал уступать место их скачкообразному обновлению. Это явление отражает динамику прогресса в целом, увеличения в геометрической прогрессии объема знаний, а также интенсивного экономического развития, основанного на внедрении новых технологий [203].

В результате информационно-технической революции создаются новые военные технологии, в результате чего на их основе создается и в больших количествах поступает в войска не просто новое оружие, а целые боевые системы, объединяющие средства поражения, РЭП, управления, связи, разведки, наблюдения и навигации. Высокоточные ракеты, бомбы и снаряды со сложнейшими системами наведения дополняются оружием, действующим на новых физических принципах: боевыми лазерами, ускорителями массы, генераторами различных полей. Появились средства информационного воздействия на автоматизированные системы управления и компьютерные сети, которые по своей разрушительной мощи и эффектам применения можно сопоставить с применением ядерного оружия [203].

По оценкам зарубежных исследователей, современное высокоточное оружие, применение которого обеспечивается воздушно-космическими средствами разведки, связи и навигации, постепенно превращается в решающий фактор вооруженной борьбы и победы в войне. Это связано со следующими факторами, обобщенными в работе [203].

Во-первых, массированный и внезапный удар высокоточными средствами поражения по объектам системы государственного и военного управления, промышленности, энергетики, транспорта, вооруженных сил менее развитого в технологическом отношении противника может решительным образом изменить дальнейший ход войны.

Во-вторых, если ядерное оружие рассматривается как средство сдерживания, которое в идеале не должно быть применено никогда, то обычные высокоточные средства поражения могут использоваться в конфликтах любого масштаба и любой интенсивности. Сторона, обладающая только ядерными силами, будет лишена этой возможности и в случае агрессии столкнется с необходимостью выбора момента, когда уже не останется надежд на мирное завершение конфликта, но еще сохранится потенциал для нанесения удара возмездия. В условиях мощного информационного воздействия на органы государственного и военного управления, момент для принятия такого решения может быть упущен.

В-третьих, появление ВТО, оружия на новых физических принципах, средств информационно-технического воздействия на автоматизированные системы управления и компьютерные сети позволяет переносить боевые действия в сферы, где применение традиционных средств было невозможным или малоэффективным: труднодоступные районы суши и Мирового океана, подводная среда, верхние слои атмосферы, космос, киберпространство. Благодаря этому США получили возможность начать работы по созданию глобальной системы ПРО, включающей наземный, морской, а в перспективе воздушный и космический компоненты [203].

Отдельные специалисты справедливо считают, что развертывание подобной системы, способной обеспечить гарантированный перехват множества баллистических ракет, запущенных в течение нескольких часов по объектам на территории США и Западной Европы, сопряжено с серьезными техническими проблемами, решения которых еще не существует. Однако, если речь идет об ответном ударе, число ракет и боевых зарядов, которым теоретически должна противодействовать американская система ПРО, может сократиться на порядок. В этих условиях США если и не гарантируют себя от ответного удара полностью, то в значительной степени смогут снизить его мощь. Следовательно, ядерное оружие не всегда сможет выполнить свою сдерживающую функцию, особенно если его устойчивость не будет обеспечена собственными силами общего назначения. Кроме того, средства ПРО могут использоваться для уничтожения космических систем противника, составляющих основу современных систем разведки, связи и навигации.

Продолжится развитие беспилотных летательных аппаратов, дистанционно управляемых катеров и сверхмалых подводных лодок, малогабаритных самодвижущихся машин, способных выполнять по команде оператора и с опорой на искусственный интеллект боевые задачи в опасных для человека условиях. Возможно появление боевых роботов, в том числе и сверхмалых, а также биокибернетических систем – различных животных (птицы, крысы, морские млекопитающие) с вживленными электронными датчиками и стимуляторами активности отделов головного мозга [203].

Качественно повысится мобильность войск (сил), главным образом за счет массового внедрения широкофюзеляжных авиалайнеров, быстроходных морских судов, создания гибридных летательных аппаратов большой грузоподъемности, объединяющих лучшие характери-

стики самолетов и вертолетов или самолетов и катеров (экранопланы) [203].

Эксперты по вопросам кибербезопасности считают, что по мере насыщения государственных и военных систем управления, элементов критической инфраструктуры и собственно вооруженных сил сложными аппаратно-техническими электронными компонентами повышается не только их эффективность, но и уязвимость. Выявление критически значимых элементов и их вывод из строя при помощи относительно примитивных аппаратно-программных средств могут вызвать каскадные и системные эффекты, совокупный ущерб от которых сопоставим с результатами применения стратегического оружия. При этом низкая стоимость разработки и приобретения подобных средств делает их доступными для отсталых стран, не имеющих современной научно-технической и производственной базы, а также террористических организаций. Вышеуказанное актуализирует разработку современных комплексов обеспечения безопасности критической инфраструктуры государства в информационном пространстве [203].

Развитие сети Интернет и ее глубокое проникновение во все социально-экономические сферы общественной жизни делает государства уязвимыми к проведению через сеть специальных информационных операций, направленных на дестабилизацию ситуации, дискредитацию государственных институтов и смену власти. В связи с этим ожидается дальнейшее увеличение спроса на оружие, боевую и специальную технику, предназначенную для противодействия терроризму, организованной преступности, пресечения массовых беспорядков, охраны границ, обеспечения гражданской обороны, ликвидации последствий техногенных катастроф и стихийных бедствий [203].

Увеличение удельного веса высокотехнологичных образцов в общем потенциале ВВТ современных армий требует качественно нового подхода к подготовке кадров, поэтому ВС передовых стран будут комплектовать силы постоянной готовности и резерв преимущественно профессиональными военнослужащими. Профессионализация передовых армий, высокие моральные издержки от потерь в личном составе стимулировали создание индивидуальной экипировки солдата будущего, повышающей эффективность и безопасность действий военнослужащего на поле боя за счет расширения возможностей по получению упреждающей информации о противнике и окружающей среде, улучшения координации действий в составе подразделения, увеличения точности и огневой мощи личного оружия, оснащения качественно новыми средствами маскировки и защиты от поражающих

факторов, диагностирования в реальном масштабе времени психофизического состояния каждого военнослужащего [203].

Не утратят актуальности и военные исследования в сфере биологии и медицины. Различные террористические и экстремистские организации не оставят попыток получить в свое распоряжение биологических агентов, при помощи которых можно сравнительно легко отравить воздух, воду, продукты, различные предметы. В развитых странах основное внимание будет уделено не созданию смертельно опасных боевых препаратов, а качественно новым разработкам с целью выведения бактерий и вирусов, поражающих людей, животных и растения с определенным генотипом. Не прекращаются работы по конструированию микроорганизмов, временно лишающих противника работоспособности, уничтожающих запасы продовольствия и даже горюче-смазочных материалов. Увеличится потребность в компактных средствах экспресс-диагностики, позволяющих в реальном масштабе времени выявлять возбудителей опасных заболеваний и их носителей, а также в новых вакцинах, антибиотиках и других медицинских препаратах [203].

Активные работы ведутся в сфере манипулирования человеческим сознанием при помощи определенных приемов подачи информации, воздействия на организм химических веществ, биологических агентов и различного рода излучений [203].

Дальнейшее развитие получит так называемое оружие нелетального действия. К нему можно отнести [203]:

- аэрозоли, ленты и порошки из электропроводящих материалов, ускорители элементарных частиц, выводящие из строя электротехнические устройства, в том числе вызывающие короткие замыкания в электрических цепях;
- клеящие или сверхскользкие вещества для блокирования взлетно-посадочных полос, мостов, тоннелей, участков дорог;
- генераторы электромагнитных и акустических полей, вещества со специфическим запахом для рассеивания толпы или удержания ее на безопасном расстоянии;
- лазеры для временного ослепления и термического воздействия;
- оглушающие, ослепляющие и травматические боеприпасы для снижения сопутствующих потерь.

Принятие на вооружение подобных образцов вызвано не гуманными соображениями, а стремлением избежать обвинений в не-

пропорциональном применении силы. Более того, некоторые средства нелетального действия оказываются эффективнее, чем традиционное оружие. Например, последствия попадания авиабомбы во взлетно-посадочную полосу аэродрома можно устранить за несколько часов, но, чтобы возобновить эксплуатацию этой же ВПП после распыления над ней специального клея, может не хватить и суток [203].

Увеличение доли высокотехнологических средств поражения ведет к значительному росту сложности военного производства. В результате наращивание, а тем более организация производства высокотехнологичных средств вооруженной борьбы с нуля, в условиях военного конфликта становятся невозможными, поэтому эти средства должны разрабатываться, выпускаться в необходимых количествах и поступать в войска в мирное время [203].

4.1.2. Общие тенденции развития военных технологий

Основу модернизации вооружения и военной техники составляют военные технологии, под которыми понимается совокупность знаний и документированных данных о типовых формах (способах или методах) военной деятельности [13, 14].

В соответствии с работой [14] три технологии относятся к основным видам военной деятельности и шесть – к обеспечивающим.

Технологии основных видов военной деятельности обеспечивают [14]:

1. поражение живой силы, военных объектов, объектов инфраструктуры, вооружения, военной и специальной техники;
2. защиту войск, военных объектов, объектов инфраструктуры, вооружения, военной и специальной техники;
3. мобильность, маневр силами и средствами, перемещение и доставку к цели средств поражения и информационных средств.

Технологии обеспечивающих видов военной деятельности лежат в основе [14]:

1. разведки и освещения обстановки;
2. навигации и целеуказания;
3. управления войсками (силами) и боевыми средствами (оружием);

4. обеспечения действий и жизнедеятельности личного состава в штатных и экстремальных условиях;
5. эксплуатации и восстановления вооружения, военной и специальной техники;
6. обеспечения развития и применения вооружения, военной и специальной техники.

Проведенный анализ основных общемировых тенденций развития базовых военных технологий показывает, что для совершенствования систем вооружения и военной техники на современном этапе важнейшее значение имеют информационные технологии, технологии микроэлектроники и новых материалов, био- и нанотехнологии.

Рассмотрим основные общемировые тенденции развития базовых военных технологий на основе материалов работы [14].

1. *Технологии поражения живой силы, военных объектов, объектов инфраструктуры, вооружения, военной и специальной техники.*

Основной тенденцией развития данной технологии является переход от кинетического воздействия на объекты поражения к энерго-информационному во всех сферах (космос, воздух, суша, море, подводное и подземное пространство) и на любой дальности с использованием различных способов преодоления активной и пассивной защиты [14].

Указанная тенденция обусловлена достижениями в следующих областях [14]:

- мощные источники излучения (лазерного, радиочастотного, акустического);
- системы формирования, наведения и удержания излучения на цели;
- сверхмощные взрывчатые вещества, в том числе малочувствительные, и их компоновка в средствах поражения с учетом специфики решаемых задач;
- технологии информационного и нелетального воздействия на системы вооружения, объекты инфраструктуры и живую силу противника;
- гиперзвуковые средства поражения и средства их доставки.

2. *Технологии защиты войск, военных объектов, объектов инфраструктуры, вооружения и военной техники*.

Основной тенденцией развития данной технологии является переход от пассивных «окопных» средств защиты (броня, фортификационные сооружения, сильно заглубленные и подводные объекты

и др.) к активным способам противодействия поражающим факторам, основанным на повышении мобильности вооружения и военной техники и применении интеллектуальных (адаптивных) систем защиты [14].

Указанная тенденция обусловлена достижениями в следующих областях, а именно [14]:

- технологии активного противодействия средствам ВТО (лазерные и радиочастотные комплексы, средства постановки уводящих помех, высокоскоростные кинетические средства защиты, «умные обшивки» и др.);
- многофункциональные, управляемые, мульти- и гипермультиспектральные маскировочные средства, «активные» системы подавления вибрации;
- многофункциональные композиционные материалы на основе нанокерамики, интерметаллидов, сверхвысокомолекулярных полимеров, обеспечивающие повышение эффективности защиты личного состава и бронетехники в 1,6 раза при снижении массы защитных элементов в 2 раза.

3. ***Технологии обеспечения мобильности, маневра силами и средствами перемещения и доставки к цели средств поражения (подавления) и информационных средств.***

Основной тенденцией развития данных технологий является переход от традиционных платформ оружия и доставки средств поражения к применению более мобильных, действующих во всех сферах (космос, воздух, суша, море, подводное и подземные пространства) унифицированных (модульных) технических систем обеспечения маневренности и доставки поражающего фактора (в том числе информационных средств и систем подавления) к цели [14].

Особая роль в перспективе отводится освоению гиперзвуковых скоростей перемещения в пространстве, использованию нетрадиционных и комбинированных способов обеспечения мобильности (экранопланы, дирижабли, воздушно-космические системы, самолеты-амфибии, самолеты-подводные лодки и др.), миниатюризации и роботизации [14].

Указанная тенденция обусловлена достижениями в следующих областях, а именно [14]:

- высокоэффективные двигательные установки различных типов;
- технологии автоматизации подвижных средств наземного, морского, воздушного и космического базирования;

- высокоэнергетические ракетные топлива и топлива к торпедному вооружению, в том числе на основе нано- и ультрадисперсных компонентов;
- нетрадиционные источники питания, обеспечивающие энергонезависимость средств перемещения и доставки поражающего фактора к цели;
- интеллектуальные адаптивные системы управления и связи;
- облегченные высокопрочные материалы и гибридные конструкционные материалы с программируемыми свойствами (умной структурой), реагирующие на воздействие окружающей среды.

4. ***Технологии разведки и освещения обстановки.***

Основной тенденцией развития данных технологий является переход от использования отдельных средств разведки и наблюдения, основанных на накоплении данных за определенное время, к созданию интегрированных общевидовых и межвидовых разведывательно-информационных систем, обеспечивающих получение от космических, воздушных, наземных, морских и специальных средств и обработку разведданных о стратегической и оперативно-тактической обстановке в реальном масштабе времени. При этом происходит расширение зон разведки, повышение точности определения координат подвижных объектов и оперативности добывания и доведения разведывательной информации [14].

Указанная тенденция обусловлена достижениями в следующих областях, а именно [14]:

- много- и гиперспектральные средства разведки и наблюдения;
- миниатюризация, комплексирование и цифровизация датчиков;
- технические средства обеспечения безопасности и скрытности;
- проведение специальных операций (мероприятий);
- технологии геоинформационного обеспечения сил и средств разведки различных уровней;
- технологии интеграции и слияния данных (Data Fusion);
- технологии обработки «Больших Данных» (Big Data);
- системы доступа к новым информационным источникам, в том числе ведения разведки в информационно-управляющих компьютерных системах;

- высоконадежные беспроводные средства связи и передачи кодированных данных.

5. ***Технологии навигации и целеуказания.***

Основной тенденцией развития данных технологий является переход от использования автономных навигационных систем среднего класса точности определения координат к применению высокоточных интегрированных автономно-спутниковых навигационных систем на основе комплексирования инерциальных навигационных систем со средствами спутниковой навигации и локальных навигационных систем. Расширяется применение нетрадиционных способов навигации и целеуказания (навигация и целеуказание по аномальному гравитационному и магнитному полям Земли, относительная навигация по локальным радионавигационным полям и др.).

Указанная тенденция обусловлена достижениями в следующих областях, а именно [14]:

- высокоточные автономные навигационные системы наземного, воздушного и морского базирования;
- технологии приема и обработки в навигационной аппаратуре потребителей всех сигналов Глобальной навигационной спутниковой системы (ГЛОНАСС), доступных сигналов GPS, Галилео (Galileo) и Бэйдоу (BeiDou), а также различных (существующих и разрабатываемых) функциональных дополнений;
- локальные навигационные системы;
- навигационные устройства, функционирующие по геофизическим полям;
- цифровые карты местности, реализующие трехмерное позиционирование объектов.

6. ***Технологии управления войсками и оружием.***

Основной тенденцией развития данных технологий является переход от централизованного иерархического управления к распределенному сетецентрическому управлению на основе интеграции интеллектуальных объектов (сети датчиков, исполнительных узлов и штабов) в едином информационном пространстве [14].

Указанная тенденция обусловлена достижениями в следующих областях, а именно [14]:

- средства цифровой связи и коммутации, засекречивания гарантированной стойкости;

- сопряжение средств разведки, навигации, опознавания с информационно-управляющими системами межвидового применения;
- межвидовые информационно-управляющие системы с интеграцией функций разведки, РЭБ, опознавания и топогеодезического обеспечения;
- спутниковая связь во всех звеньях управления.

7. ***Технологии обеспечения действий и жизнедеятельности личного состава в штатных и экстремальных условиях.***

Основной тенденцией развития данной технологии является переход от традиционного снаряжения военнослужащих к многофункциональной сверхлегкой и эргономичной экипировке, обеспечивающей значительное повышение автономности действий. Особая роль отводится разведывательно-информационной обеспеченности отдельного военнослужащего. Принимаются меры по информационной и эмоционально-психологической разгрузке операторов в человеко-машинных автоматизированных системах управления войсками и оружием.

Указанная тенденция обусловлена достижениями в следующих областях, а именно [14]:

- компактные источники электроэнергии на молекулярных топливных ячейках;
- миниатюрные средства обеспечения разведданными, связи, жизне- и энергообеспечения;
- сверхлегкие бронематериалы на основе армированных керамических композитов, гибких металлосодержащих графитов и алмазных покрытий, многослойных полимерных и силикатных наноматериалов;
- интеллектуальные системы индивидуальной защиты и маскировки;
- экзоскилетные системы физической разгрузки военнослужащих;
- перспективные технологии и средства дистанционной диагностики, оказания помощи, эвакуации и спасения;
- эргономичные интеллектуальные и адаптивные средства отображения информации.

8. ***Технологии эксплуатации и восстановление вооружения, военной и специальной техники.***

Основной тенденцией развития данных технологий является переход от эксплуатации вооружения и военной техники по норматив-

ным срокам к системам эксплуатации и ремонта по фактическому техническому состоянию на основе встроенных и дистанционных систем диагностики и интегрированной логистической поддержки жизненного цикла [14].

Указанная тенденция обусловлена достижениями в следующих областях, а именно [14]:

- методы и средства автоматизации технического диагностирования и контроля, в том числе встроенных, прогнозирования неисправностей и отказов ВВТ, поддержки принятия решений командирами и техническими службами о применении (ремонте по состоянию) ВВТ;
- методы и технические средства, обеспечивающие качественное восстановление исправности (работоспособности), продление ресурса (сроков службы) ВВТ;
- информационная поддержка жизненного цикла вооружения и военной техники (ИПИ-технологии);
- композиционные и интеллектуальные материалы, в том числе на основе нанотехнологий, обладающие повышенными эксплуатационными характеристиками (высокая жесткость и прочность, небольшая плотность и удельная масса, высокая температурная, коррозионная и радиационная стойкости, возможность получения материала с заданными свойствами для решения конкретной технической проблемы).

9. ***Технологии обеспечения развития и применения вооружения, военной и специальной техники.***

Основной тенденцией развития данных технологий является переход от традиционного программно-целевого планирования (ПЦП) развития системы вооружения к усовершенствованной методологии сквозного ПЦП, охватывающей полный инновационный цикл формирования перспективного облика системы вооружения, в рамках которого обеспечивается взаимная увязка по срокам и содержанию системных проектов, по развитию межвидовых и видовых систем вооружения, работ по обоснованию структурно-функционального облика перспективных образцов и исследований по созданию научно-технического задела. При этом основной упор делается на создание и обеспечение разработки ВВТ с использованием отечественных материалов и современной электронной компонентной базы, а также электронных модулей для применения в экстремальных условиях воздействия факторов различной физической природы [14].

Указанная тенденция обусловлена достижениями в следующих областях, а именно [14]:

- автоматизированные системы поддержки принятия решений и экспертные системы;
- методы адаптивного управления различными процессами и интеллектуального анализа данных;
- новая электронная компонентная база, стойкая к воздействию внешних факторов различной физической природы;
- электронные модули с уменьшенными размерами и массогабаритными характеристиками;
- вычислительные средства и системы передачи данных повышенного быстродействия и пропускной способности.

В обобщенном виде тенденции развития базовых военных технологий представлены в табл. 4.1 по данным работы [14].

Таблица 4.1. Обобщенная характеристика тенденций развития базовых военных технологий

№ п/п	Базовые военные технологии	Тенденции развития	
		2008 год	2025 год
1	Поражение живой силы, военных объектов, объектов инфраструктуры, ВВСТ	Кинетическое воздействие на объекты поражения	Энергоинформационное воздействие во всех сферах (космос, воздух, суша, море, подводное пространство) и на любой дальности.
2	Защита войск, военных объектов, объектов инфраструктуры, ВВСТ	Пассивные («окопные») средства защиты (броня, фортификационные сооружения, заглубленные и подводные объекты и д.р.)	Активные способы противодействия поражающим факторам. Повышение мобильности ВВСТ и применение интеллектуальных (умных, адаптивных) систем защиты
3	Обеспечение мобильности, маневра силами и средствами, перемещения и доставки к цели средств поражения (подавления) и информационных средств	Традиционные платформы оружия и доставки средств поражения	Мобильные, в том числе безэкипажные, технические системы обеспечения маневренности и доставки поражающего фактора к цели

№ п/п	Базовые военные технологии	Тенденции развития	
		2008 год	2025 год
4	Разведка и освещение обстановки	Отдельные средства разведки и наблюдения, основанные на накоплении данных за определенное время	Интегрированные общевидовые и разведывательно-информационные системы. Получение и обработка разведданных в реальном масштабе времени
5	Навигация и целеуказание	Автономные навигационные системы среднего класса точности определения координат	Высокоточные интегрированные спутниковые навигационные системы. Комплексирование навигационных систем со средствами спутниковой навигации и локальными навигационными системами
6	Управление войсками и оружием	Централизованное иерархическое управление	Распределенное сетецентрическое управление. Интеграция интеллектуальных объектов (сети датчиков, исполнительных узлов и штабов) в едином информационном пространстве
7	Обеспечение действий и деятельности личного состава в штатных и экстремальных условиях	Традиционное снаряжение военнослужащих	Многофункциональная сверхлегкая и эргономичная экипировка. Повышение автономности действий
8	Эксплуатация и восстановление ВВСТ	Эксплуатация ВВСТ по нормативным срокам	Системы эксплуатации и ремонта по фактическому техническому состоянию. Применение встроенных и дистанционных систем диагностики

Окончание табл.4.1

№ п/п	Базовые военные технологии	Тенденции развития	
		2008 год	2025 год
9	Обеспечение развития и применения ВВСТ	Традиционное программно-целевое планирование развития системы вооружения	Методология сквозного ПЦП, охватывающая полный инновационный цикл формирования перспективного облика системы вооружения

Рассматривая США как наиболее технически развитую державу, по которой имеются сведения о перспективах развития вооружений (в отличие, например, от Китая), можно констатировать, что в США в ближайшей перспективе заканчиваются испытания результатов завершенных научных программ по следующим направлениям[29]:

- сверхскоростным ударным гиперзвуковым стратосферным и заатмосферным летательным аппаратам, против которых пока не существует эффективных средств ПВО, например, Х-37В (поступление на вооружение в 2020 г.), способного пребывать на орбите до 9 месяцев и поражать наземные, воздушные и космические цели с использованием лазерного оружия;
- микроволновому, кинетическому и лазерному оружию. Сегодня прототипы этого оружия проходят лабораторные испытания в США и Израиле, и их появление в арсеналах возможно уже в течение следующего десятилетия.

На стадии фундаментальных научных разработок (это среднесрочные будущие военные технологии), т.е. еще до этапа НИОКР, находятся следующие направления [29]:

- дистанционно управляемые автоматизированные устройства, имитирующие физическую, речевую и даже интеллектуальную деятельность человека – роботы-пехотинцы, роботы-разведчики;
- минироботы и киборги, т.е. сочетание живого существа и механизма, в т.ч. киборги-насекомые (пчелы, бабочки и т.п.), создаваемые путем вживления в их организм сверхминиатюрных наноэлектронных передатчиков;
- генно-инженерное оружие;
- дистанционное воздействие на ионосферу Земли радиоволнами сверхвысокочастотного диапазона и создание искусственных протяженных плазменных образований (амери-

канская программа HAARP – High Frequency Active Auroral Research Program «Программа исследования полярных сияний высокочастотным воздействием»).

В рамках этой программы уже получены результаты, позволяющие говорить о реальном создании систем геофизического оружия, способного нарушать радиосвязь и радиолокацию, выводить из строя бортовую электронную аппаратуру космических аппаратов, ракет, самолетов и т.п. [10, 29].

В перспективе технологические возможности США могут привести к появлению новых боевых систем [95]:

- ударных беспилотных летательных аппаратов и их самолетов-носителей (воздушных авианосцев);
- кораблей-арсеналов;
- дистанционно управляемых пусковых установок ракет большой дальности;
- роботизированных систем боевого и иного назначения;
- средств разведки и органов ведения информационной войны;
- ударных сил, способных вести борьбу с космическими объектами и поражать из космоса наземные цели;
- новых видов специального оружия.

Развитие средств вооруженной борьбы приведет к тому, что космическое пространство и информационная сфера могут стать самостоятельными ТВД.

Рассмотрим более подробно современное состояние и основные тенденции в развитии отдельных видов вооружения и военной техники. С учетом того, что именно США и странам НАТО принадлежит приоритет в разработке наиболее перспективных образцов вооружения, основная часть нижеприведенного обзора посвящена анализу средств вооружения именно их вооруженных сил. Однако на основании представленного обзора можно сделать общие выводы о том, в каком именно направлении развиваются средства вооружения, и можно не сомневаться, что в ближайшее время и в других технологически развитых странах появятся подобные типы оружия.

4.2. Системы управления, связи и разведывательного обеспечения (на примере систем ВС США)

Информационные технологии в области систем управления и связи являются теми достижениями, которые легли в основу концепции сетецентрической войны, взаимоувязав силы и средства различных уровней управления в единую систему систем и переведя вооруженную борьбу на принципиально новый уровень.

4.2.1. Единое информационное пространство

Концепция единого информационного пространства предполагает создание глобальной информационной среды, обеспечивающей комплексную обработку сведений в реальном масштабе времени о противнике, своих войсках и окружающей местности в интересах поддержки принятия решений по созданию группировок войск (сил) оптимального (для достижения поставленных целей) состава и их эффективного применения в различных условиях обстановки. Наличие единой информационной среды должно обеспечить эффективное взаимодействие всех участвующих в операции органов управления и войск (сил), которые условно можно разделить на три основные группы элементов [206]:

- добывающие;
- информационно-управляющие;
- исполнительные.

Добывающие элементы включают в себя силы и средства разведки, призванные осуществлять сбор, предварительную обработку и доведение разведывательных сведений до информационно-управляющих и исполнительных элементов.

Информационно-управляющие элементы представляют собой коалиционные и национальные органы и пункты управления, автоматизированные системы управления и связи, обеспечивающие их функционирование, а также территориально распределенные базы данных оперативной, разведывательной и другой необходимой информации (топогеодезической, геопространственной, фоноцелевой, гидрометеорологической и т. п.), предоставляемой пользователям в масштабе времени, близком к реальному.

Исполнительными элементами являются системы оружия и воинские формирования, задействуемые в операциях и решающие задачи по поражению (уничтожению) живой силы и объектов противника [206].

Сетецентрические системы управления призваны обеспечить функционирование единого и надежного информационного пространства, в котором в реальном времени решаются комплексные задачи сбора, накопления и интеллектуальной переработки многоканальных потоков сложно структурированных данных. Цель – формирование единой картины событий и обеспечение превосходящего качества управления большими системами разнопрофильных многокомпонентных систем подвижных и стационарных объектов, гарантирующего достижение поставленных целей с минимальными потерями [162].

В документальном виде принципы объединения сил и средств в единое информационное пространство, являющееся основой сетецентрической среды, нашли отражение в виде соответствующих объединенных функциональных концепций (ОФК) (JFC – Joint Functional Concepts) и объединенных интегрирующих концепций (ОИК) (JIC – Joint Integrating Concepts), принятых в ВС США, в том числе следующие [319]:

- концепция «Командование и оперативное управление»;
- концепция «Единое информационно-коммуникационное пространство»;
- концепция «Объединенное командование и оперативное управление»;
- концепция «Сетецентрическое операционное пространство».

Наличие этих концепций обусловлено многогранностью процессов командования и оперативного управления и их прикладным значением для структуры вооруженных сил, а также комплексным характером решаемых задач в информационную эпоху [319].

Концепция «Командование и оперативное управление» определяет формы и способы деятельности командира (командующего) объединенными войсками (силами) по организации командования и оперативного управления. В соответствии с ее положениями возможности командира (командующего) объединенными войсками (силами) по обеспечению бесшовности и мобильности командования и оперативного управления характеризуются способностью к быстрой структурно-функциональной адаптации во всем спектре военных действий. Эта структурно-функциональная адаптация будет обеспечиваться

наличием единого информационного пространства и устойчивой, безопасной коммуникационной сети, находящейся в его распоряжении [319].

Концепция «Единое информационно-коммуникационное пространство» – это концепция, основанная на использовании информации, а также превосходстве в принятии решений. Эта концепция определяет формы и способы деятельности объединенных войск (сил) в полносвязном сетевом пространстве. Ее положениями предусматривается кардинальное повышение эффективности и результативности решения задач за счет расширения возможностей по использованию коллективных знаний и наличия гарантированной коммуникации между всеми компонентами.

Единое информационно-коммуникационное пространство – неотъемлемый компонент успешного внедрения организационных решений в области управления объединенными войсками (силами) в информационную эпоху. Возможности по формированию единого информационного пространства обусловлены особенностями происходящей в настоящее время информационно-технической революции. Техническими аспектами революционных изменений являются расширение объемов циркулирующей в сетях информации и предоставление к ней доступа независимо от пространственно-временного нахождения абонентов, а также качественные межведомственные и внутриведомственные взаимосвязи на основе использования перспективных телекоммуникационных технологий [319].

Важнейший принцип, заложенный в саму идею построения единого информационного пространства, – обеспечение универсальной возможности взаимодействия на основе функциональной совместимости информационно-коммуникационных систем различных звеньев управления [319].

При этом военные ученые США и НАТО акцентируют внимание на том, что техническая среда единого информационного пространства, в которой осуществляется командование и оперативное управление, безусловно, имеет важное значение, однако по мере возможности, во избежание подмены функций должностных лиц, принимающих решения, эта среда должна быть использована лишь для помощи в реализации функций командования и оперативного управления, а не для необдуманной адаптации командования и оперативного управления к среде [319].

С практической точки зрения формирование единого информационного пространства предусматривает объединение локальных,

территориальных и глобальных сетей с целью охвата системами и средствами передачи информации наземного, морского и воздушного пространства. В конечном итоге создание единого информационного пространства постулируется как главное условие обеспечения информационного превосходства над противником. Под этим понимается превосходство в сборе, обработке и распределении информации, что приводит к превосходству в скорости и обоснованности принятия решений и их дальнейшей реализации.

Фактически единое информационное пространство формирует общую виртуальную среду, объединяющую любые источники информации, системы оружия и органы управления всех уровней, реализуя, таким образом, один из основополагающих принципов концепции «Единое информационно-коммуникационное пространство» – совместную выработку и принятие решений по управлению рассредоточенными в пространстве боевыми и вспомогательными формированиями объединенных войск (сил) [319].

Научно-технологические принципы построения систем управления ВС США и ОВС НАТО первоначально основывались на архитектуре клиент-сервис. Однако позже произошел отказ от такого принципа доступа к информации в пользу сервис-ориентированной архитектуры SOA (Service-Oriented Architecture) [318].

Использование сервис-ориентированной архитектуры SOA дает возможность реализовать информационные потребности за счет использования модели «размещение и интеллектуальное извлечение по запросу». Информационный обмен в едином информационном пространстве будет обеспечивать сервисы обеспечения безопасности информации, поиска услуг, управления корпоративными услугами, межмашинного обмена, обнаружения пользователей и устройств, посредничества и каталога метаданных. Эти и другие специализированные сервисы, входящие в SOA, физически могут храниться и выполняться на различных серверах, включенных в сеть, обеспечивая формирование адаптивной распределенной вычислительной среды. По своему функциональному назначению в SOA сервисы могут быть поставщиками или потребителями услуг. Кроме того, они могут инициализировать выполнение других сервисов и/или осуществлять обмен данными с ними [318].

Принципиальным отличием архитектуры SOA от архитектуры клиент-сервер является наличие каталога услуг, который обеспечивает их учет и возможность поиска, предоставляя возможность обмена данными между территориально разнесенными сервисами без необхо-

димости настройки жесткой адресации в сети. При этом сервисы-поставщики предоставляют услуги, в формализованном виде публикуют информацию об их наличии, способе получения и месте расположения в каталоге услуг, в котором накапливаются сведения обо всех имеющихся сервисах для их последующего поиска. Такое построение позволяет сервисам-потребителям находить требуемые услуги в сети и осуществлять инициализацию соответствующих сервисов-поставщиков [318].

Изменение технологического подхода к построению единого информационного пространства позволяет сместить акцент решения проблемы информационного обеспечения с источника информации, чьей задачей являлось определение как можно большего количества потенциально заинтересованных потребителей, в сторону потребителя, информационные потребности которого реализуются посредством определения потенциальных источников этой информации. Внедрение сервис-ориентированных архитектур будет осуществляться с использованием стандартов и технологии открытой архитектуры и программно-аппаратных средств коммерческого назначения в целях сокращения расходов и снижения зависимости от конкретных производителей [319].

При этом особого внимания заслуживает одна специфическая особенность – строгая ориентированность на применение коммерческих стандартов в системах связи и информационного обеспечения военного назначения [319].

Структура и содержание программ по формированию единого информационного пространства показывают, что они направлены на формирование технической и логической инфраструктуры, предоставляющей возможности совместного использования информационных ресурсов как в рамках вида ВС, так и за счет сетевого обмена информацией между всеми видами ВС США, а также с другими участниками операции [319].

В настоящее время в США создание единого информационного пространства лежит в плоскости завершения строительства единой информационно-коммуникационной инфраструктуры министерства обороны США, получившей наименование «Глобальная информационная сеть» – GIG (Global Information Grid) Минобороны США. Сеть GIG является основой глобальной оборонной единой цифровой сети оборонной информационной системы DISN (Defense Information Systems Network) и предназначена для информационного обеспечения всех элементов системы национальной безопасности страны, в том

числе и вооруженных сил. Она объединяет взаимосвязанные распределенные вычислительные системы коллективного пользования, локальные вычислительные сети, системы связи, базы данных, системы компьютерной и сетевой безопасности, средства обучения пользователей, а также другие элементы, предназначенные для централизованного удовлетворения всех информационно-технических потребностей системы управления войсками и органов административного управления [319].

В НАТО для обеспечения комплексной обработки данных о своих войсках предполагается объединить по принципу полной организационно-технической и программно-лингвистической совместимости следующие автоматизированные системы [206]:

- автоматизированную систему управления AC2S;
- автоматизированную систему сбора и отображения данных о местоположении своих войск (сил) FFT/BFT (Friendly Force Tracking/Blue Force Tracking (Systems));
- автоматизированную систему связи (обмена данными) и информационного обеспечения CIS (Communication Interface System).

Дальнейшую интеграцию автоматизированных информационно-управляющих систем альянса планируется осуществить в рамках программы A4ISR, которая предусматривает объединение вышеуказанных групп систем обработки данных о противнике и своих войсках для формирования командной и аналитической основы единого информационного пространства блока. При этом эти автоматизированные информационно-управляющие системы, функционируя в комплексе с геоинформационными (GIS) и навигационными системами (GPS), образуют систему систем SoS (System of Systems) или блок систем FoS (Federation of Systems) [206].

4.2.2. Системы и сети связи

4.2.2.1. Общие тенденции развития систем и сетей связи

Системы и сети связи являются технической и технологической основой объединения сил и средств на основе единого информационного пространства.

Одним из ключевых направлений повышения боевых возможностей вооруженных сил США является формирование интегрированного информационного пространства на основе новейших информационных технологий. Минимизация длительности цикла принятия решения, увеличение производительности вычислительных систем и эффективное распределение информационного потока между аппаратными ресурсами посредством унифицированного сетевого оборудования позволят достичь максимального уровня ситуационной осведомленности и управляемости критическими процессами [107].

Анализ работ [95, 107, 108, 272, 273, 320, 321, 322, 323, 324, 325, 327] позволил сформировать следующие тенденции развития систем связи:

- широкое использование коммерческих протоколов и технологий в составе военных и специальных систем связи, прежде всего, протоколов IP и MPLS (Internet Protocol and Multiprotocol label switching);
- конвергенция отдельных сетей и систем связи в единое информационное пространство на основе концепции NGN;
- построение транспортных сетей связи на основе высокоскоростных оптических каналов связи с использованием технологий DWDM (Dense Wavelength Division Multiplexing), а также с использованием спутниковых систем связи с лазерными межспутниковыми каналами;
- широкое использование спутниковых систем связи на ТВД во всех звеньях управления, в том числе и за счет аренды ресурса у гражданских операторов спутниковой связи;
- использование в тактическом звене управления технологий адаптивных мобильных радиосетей Mesh/MANET-сетей (Mobile Ad hos Network), сопрягающих всех абонентов на ТВД;
- использование методов обработки Big Data, а также облачных и Grid-технологий для организации распределенного хранения и обработки больших массивов данных, поступающих от сенсорных средств сетецентрической среды.

Министерством обороны США развиваются две основные программы:

- система командования, управления, связи, вычислительной техники и разведки для участника боевых действий C4IFTW (Command, Control, Communications, Computers, and Intelligence for the Warrior);

- программа создания оборонной информационной инфраструктуры DII (Defense Information Infrastructure).

Программа C4IFTW предусматривает разработку концептуальных принципов и плана достижения глобального взаимодействия между участниками боевых действий, что позволит им выполнять любую задачу в любое время в любом месте, быстро устанавливать надежную и безопасную засекреченную связь и при этом иметь систему, приемлемую по стоимости. Основной задачей C4IFTW является формирование среды, которая позволяла бы эффективно поддерживать связь и управление в операциях, проводимых несколькими видами ВС, либо с участием союзных войск с тем, чтобы участники боевых действий имели средства, позволяющие выполнять боевые задачи в любой точке земного шара. Она концентрирует внимание на вопросах обеспечения стандартной бесшовной стыковки сетей, что гарантирует возможность взаимодействия и объединения усилий. Концепция C4IFTW определяет облик глобальной системы связи и управления на период после 2010 г., которая полностью обеспечит потребности участника боевых действий в информации, необходимой для поиска и уничтожения противника.

Программа DII направлена на решение следующих основных задач:

- обеспечение услуг сквозной информационной поддержки, позволяющих осуществлять сбор, создание, хранение, отображение и распределение информации в масштабах министерства обороны;
- удовлетворение требований к услугам, связанным с информационным обеспечением, при выполнении министерством обороны боевых задач;
- предоставление пользователям широкого спектра услуг посредством прозрачных механизмов;
- повышение надежности и безопасности обработки информации и передачи в соответствии с требованиями, определяемыми выполняемой боевой задачей и экономически реализуемыми;
- обеспечение безопасности, секретности и живучести обработки информации и передачи в соответствии с требованиями, определяемыми выполняемой боевой задачей и экономически реализуемыми.

Реализация этих инициатив предусматривает создание и развитие глобальной единой телекоммуникационной среды, которая должна

обеспечить информационные потребности военного командования США в XXI веке. К числу сетей, играющих наиболее важную роль в этой телекоммуникационной среде, относятся следующие.

4.2.2.2. Сеть DISN

Сеть DISN (Defense Information Systems Network) – оборонная интегрированная система передачи данных. Главная цель сети DISN – обеспечить высокую степень интеграции услуг, предоставляемых отдельным пользователям, в локальных и глобальных сетях. Предполагается, что пользователи будут регулярно обмениваться информацией в виде речи, данных и изображений, используя одни и те же терминалы в течение отдельного сеанса. Сеть предоставляет услуги по передаче всех видов информации (речи, данных, видео, мультимедиа) и интегрирует все системы связи министерства обороны США (рис. 4.1).

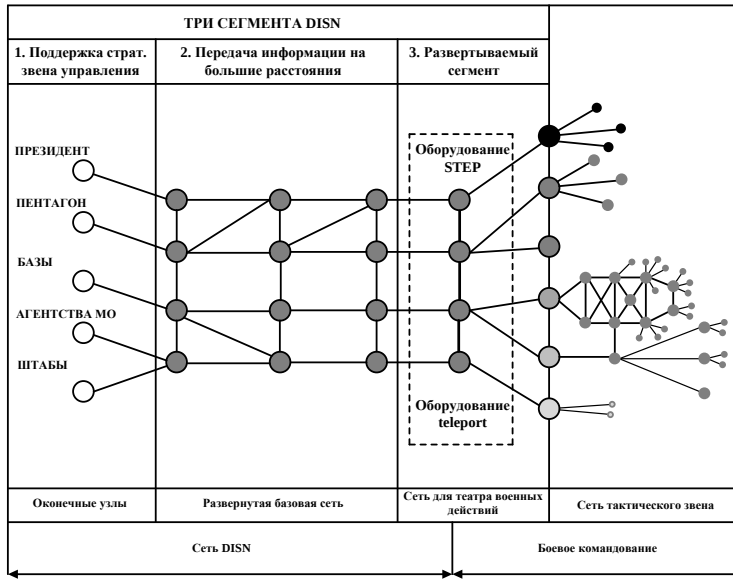


Рис. 4.1. Сеть DISN

В настоящее время основу DISN составляют оптические транспортные сети на основе технологии SONET, использующие коммутацию каналов по стандарту TDM. В сети коммутации каналов се-

годня работают следующие основные военные сети связи Пентагона (рис. 4.1) [321]:

1. телефонная сеть DSN (Defense Switched Network);
2. закрытая коммутируемая сеть DRSN (Defense Red Switched Network);
3. сеть видеоконференцсвязи DVS (DISN VIDEO).

Кроме того, ресурсы DISN используют четыре закрытые сети JWICS, AFSCN, NIPRNet и SIPRNet, которые используют выделенные магистральные каналы [321]:

- объединенную глобальную сеть разведывательных коммуникаций JWICS (Joint Worldwide Intelligence Communications System) – для передачи секретной информации по протоколам TCP/IP;
- сеть управления спутниками AFSCN (Air Force Satellite Control Network);
- NIPRNet (Non-classified Internet Protocol Router Network) – сеть, используемую для обмена несекретной, но важной служебной информацией между внутренними пользователями;
- SIPRNet (Secret Internet Protocol Router Network) – систему взаимосвязанных компьютерных сетей, используемых МО для передачи секретной информации по протоколам TCP/IP.

При этом сети JWICS и AFSCN построены на базе коммутаторов ATM (техника ATM в настоящее время не производится) [321].

В 2006 г. в военном ведомстве США решили перейти от коммутации каналов к коммутации пакетов: был принят план Joint Vision 2020 – на текущие 15 лет, в котором объявлена смена парадигмы сети DISN – переход к IP-протоколу. Предполагается, что IP-протокол станет единственным средством общения между транспортным уровнем и приложениями (рис.4.2), а протоколом сигнализации станет протокол SIP.

Ввиду того, что у стандартного протокола SIP имеются определенные сложности с обеспечением секретности и обслуживанием приоритетных вызовов, что важно для военных применений, по заказу МО США разработали защищенный протокол AS-SIP. Протокол AS-SIP получился очень громоздким. Если обыкновенный SIP использует 11 стандартов RFC, то AS-SIP требует учета почти 200 стандартов RFC. Кроме того, сам протокол AS-SIP еще далек от совершенства – в версию AS-SIP, обнародованную в июле 2013 г., уже внесено более 50

исправлений по сравнению с исходной версией, подготовленной полугодом ранее. Переход от сети SONET с коммутацией каналов к коммутации IP-пакетов и протоколу SIP (или к AS-SIP) требует использования новых программных коммутаторов SoftSwitch, которые будут функционировать в соответствии с концепцией NGN. При этом в качестве поставщиков этих коммутаторов выступают Avaya, Jupiter и другие производители [321, 322].

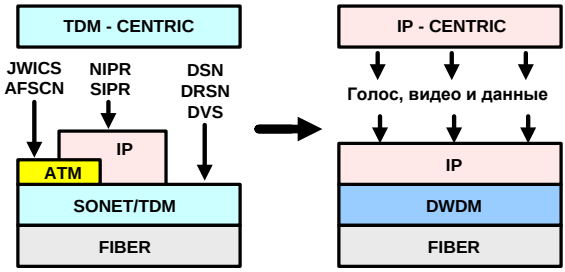


Рис. 4.2. Эволюция сети DISN [321]

Фактически сеть DISN является базовой телекоммуникационной инфраструктурой, к которую подключаются другие сети (спутниковые, сети тактического звена и др.), а также на основе, которой строятся другие информационно-управляющие сети (такие как GIG) или сети обмена информацией (такие как NIPRNet, JWICS).

Более полная информация о построении и технологических особенностях функционирования сети DISN приведена в работах [108, 321, 322].

4.2.2.3. Сеть GIG

Сеть GIG (Global Information Grid) – Глобальная информационно-управленческая сеть минобороны США. GIG строится в том числе и на основе связных ресурсов DISN и предназначена для информационного обеспечения всех элементов системы национальной безопасности страны, включая вооруженные силы. Она объединяет взаимосвязанные распределенные вычислительные системы коллективного пользования, локальные вычислительные сети, системы связи, базы данных, системы компьютерной и сетевой безопасности, средства обучения пользователей, а также другие элементы, предназначенные для централизованного удовлетворения всех информационно-

технических потребностей системы управления войсками и органов административного управления [319].

GIG поддерживает обработку для обеспечения оперативных задач, действий и функций разведорганов министерства обороны США, АНБ и других органов разведывательного сообщества. Она предоставляет возможность контакта всем оперативным пунктам дислокации – авиабазам, гарнизонам, военно-морским базам. GIG обеспечивает интерфейсы для коалиционных, союзных и не принадлежащих министерству обороны США пользователей и систем. Информационные технологии в виде автоматизированных и информационных систем, не входящих в GIG, являются автономными, самодостаточными либо информационными системами, которые не предназначены или не могут быть подсоединены к этой информационно-управляющей сети [325].

Сеть обмена данными GIG представляет собой объединенную цифровую сеть на основе протокола IPv6, построенную по принципу «Все по IP» и использующую как собственные каналы связи, так и каналы связи региональных и национальных операторов связи. В качестве базового протокола для обмена данными в GIG используется IP/MPLS, а сама сеть строится в соответствии с концепцией NGN с широким использованием программных коммутаторов SoftSwitch производства Avaya, Jupiter и других производителей [322]. При этом ядром GIG является глобальная высокоскоростная опорная сеть GIG-BE (Global Information Grid-Bandwidth Expansion). GIG-BE – это мировая оптическая сеть SONET с каналами 10 Гбит/с, обслуживающая порядка 100 операционных вычислительных центров по всему земному шару [318, 324].

Первая версия GIG-системы (GIG v. l), представленная в январе 2000 г., была построена как структура, которая объединяла существовавшие в то время системы с иерархическим принципом построения (platform-centric). В этой связи формально GIG определялась как множество глобально объединенных по принципу «точка-точка» информационных, а также автоматизированных и коммуникационных систем, связанных с ними процессов сбора, отправки, распределения и управления информацией по требованию участников военных операций, политического руководства и обеспечивающих структур. Она была ориентирована на обслуживание штабов объединенных оперативных формирований и, в основном, ограничивалась стратегическим и оперативным уровнями [325].

Разработка архитектуры GIG второй версии (GIG v. 2) была обнародована в ноябре 2002 г. Новая архитектура была ориентирована на создание сетецентрической среды в соответствии с концепцией сетецентрических войн NCW (Network-Centric Warfare). Архитектура GIG v. 2 состоит из пяти блоков для стратегического, оперативного, тактического и комбинированного применения американскими и союзническими ВС в операциях и конфликтах различного масштаба и назначения. Включение тактического уровня в состав GIG v. 2 отражает стремление реализовать то положение, что информационное превосходство становится важным слагаемым на всех уровнях управления и особенно по отношению к боевым возможностям перспективных систем тактического звена. Основой этого информационного превосходства становятся Grid-системы, то есть распределенные инфраструктуры для суперкомпьютерных приложений. Вычислительную основу GIG составляют 18 центров корпоративных вычислений министерства обороны США, 5 региональных информационных центров и 10 центров региональной обработки данных сухопутных войск. Создание Grid-системы распределенных вычислений в составе GIG стал возможен за счет использования в качестве ядра GIG высокоскоростной оптической системы связи GIG-BE. Использование Grid-технологий позволило создать управляющую и прикладную инфраструктуру для предоставления широкого класса информационных сервисов в интересах военных пользователей [325].

Глобальная информационная Grid-система в составе GIG – это инфраструктура координированной распределенной обработки информации и хранения гетерогенных информационных ресурсов с гибкой политикой управления, непрерывного доступа к ресурсам и вычислительным мощностям с обеспечением безопасности, распараллеливания обмена данными, эффективного и экономного использования процессорной нагрузки. Она образует так называемую «инфраструктуру базовых возможностей» для своевременного, безопасного и повсеместного доступа пользователей к информации для выработки, принятия решений и оптимизации их исполнения (рис. 4.3.) [325].

Наличие Grid-инфраструктуры позволило реализовать программу перехода от объединенной глобальной системы оперативного управления GCCS-J (Global Command and Control-Joint) к объединенной системе командования и оперативного управления JC2 (Joint Command and Control System). Переход к последней выполняется посредством переложения программного обеспечения GCCS-J на корпоративные сервисы сетевой связности NCES (Net Centric Enterprise

Services), что является одной из основных составляющей корпоративных сервисов GES (GIG Enterprise Services) для GIG в интересах командования и оперативного управления стратегического уровня [325].

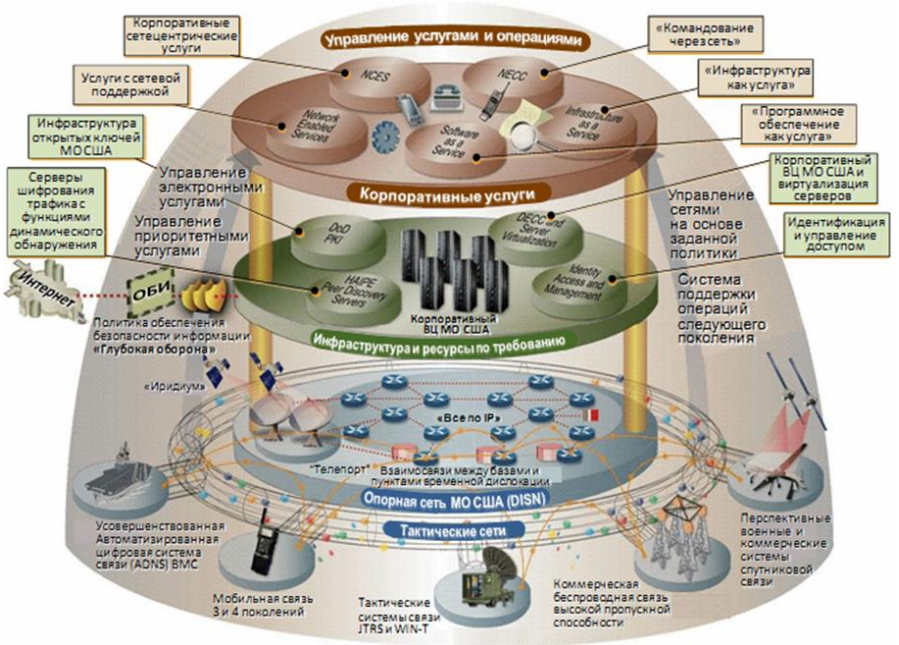


Рис. 4.3. Общая структура информационного пространства на основе GIG [273]

С целью расширения диапазона досягаемости и повышения сетевой связности GIG для нее были разработаны дополнительные программы, связанные с включением в сеть спутниковых систем связи через систему телепортов, включения в сеть тактических радиосетей. Кроме того, для повышения качества принятия решений пользователи GIG получили возможность объединяться в виртуальные группы коллегиального сотрудничества [325].

В 2011 г. министерство обороны США приступило к переходу GIG на новую версию – GIG v. 3. Необходимость модернизации статьи обусловлена тем, что основным глобальным связывающим звеном между серверами GIG вне ТВД и участниками боевых действий является спутниковая группировка. Однако, как показали результаты войны в Ираке и Ливии, она зачастую не справляется с передачей больших объемов данных в условиях боевых действий. Развитие сети GIG

при переходе к версии GIG v. 3 будет вестись в соответствии с шестью ключевыми программами (рис 4.4) [323].

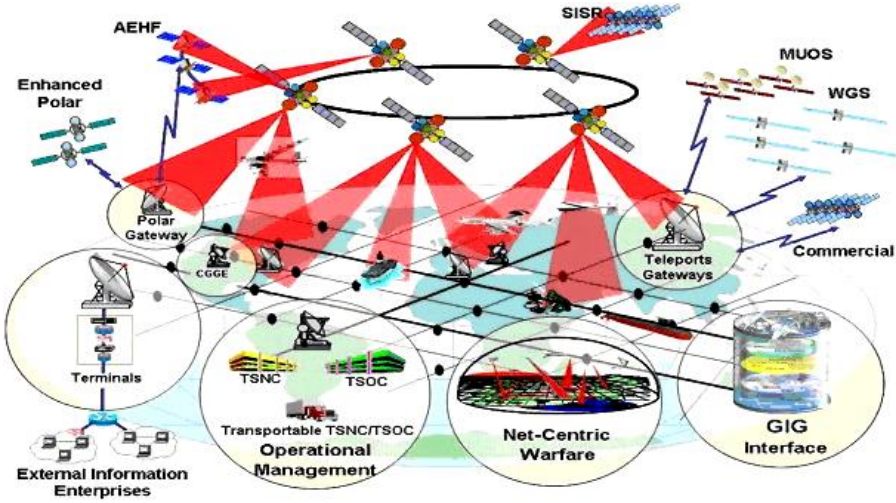


Рис. 4.4. Общая схема сети GIG [323]

Программа 1 – формирование высокоскоростного наземного компонента GIG на основе волоконно-оптических линий связи с технологией DWDM, получившая название DISN-Core [323].

Программа 2 – формирование космического сегмента GIG. Эта программа включает строительство перспективной объединенной системы спутниковой связи, базовыми компонентами которой станут несколько группировок космических аппаратов связи.

Программа 3 – система «телепортов». Под «телепортом» американские специалисты понимают телекоммуникационный пункт сбора и распределения информации, который объединяет наземный и космический сегменты GIG и обеспечивает боевые подразделения широкополосным, мультимедийным и глобальным доступом к DISN [323].

Программа 4 – разработка тактического радиосегмента GIG. Программа предполагает разработку широкополосных радиостанций нового поколения, структура и функциональные возможности которых реализуются на основе концепции программируемого радио SDR (Software Defined Radio), и удовлетворяет новым, повышенным требованиям АНБ США к системам шифрования сигналов [323].

Программа 5 – предусматривает разработку унифицированного комплекса сетевых сервисов корпоративного информационного обслуживания NCES (Net-Centric Enterprise Service). Комплекс предназначен для обеспечения любого пользователя, имеющего доступ к GIG, стандартным набором информационных услуг по своевременному и безопасному доступу к необходимой информации высокого качества [323].

Программа 6 – обеспечение информационной безопасности в GIG. Ее ключевым элементом является программа модернизации криптографических средств защиты CMP (Crypto Modernization Program), которая предполагает создание новых методов и способов засекречивания и защиты информационных ресурсов [323].

Более полная информация о построении и технологических особенностях функционирования сети GIG приведена в работах [108, 322, 323, 324, 325].

4.2.2.4. Сеть NIPRNet

Сеть NIPRNet (Non-classified IP Router Network) – наложенная сеть, используемая для обмена несекретной информацией между «внутренними» абонентами ВС США, а также для обеспечения доступа абонентов к глобальной сети Интернет [88]. NIPRNet состоит из IP-узлов в США, Европе и Тихоокеанском регионе, принадлежащих Министерству обороны США и обеспечивающих передачу данных по планированию и тыловым задачам, перевозкам и учету личного состава в интересах объединенного командования. Сеть была создана в 1990-х управлением информационного обеспечения минобороны США в качестве развития сети MilNET. NIPRNET является крупнейшей военной сетью связи в мире [88].

4.2.2.5. Сеть SIPRNet

Сеть SIPRNet (Secret IP Router Network) – система взаимосвязанных компьютерных сетей, используемых Минобороны и Государственным департаментом США для передачи секретной информации по протоколам TCP/IP в «полностью безопасную» окружающую среду. SIPRNet предоставляет также доступ к гипертекстовым документам и электронной почте. По данным Пентагона в 2011 г. SIPRNet насчитывала около 4,2 млн пользователей. Помимо пользователей из министерства обороны и государственного департамента США доступ к

SIPRNet имеет также пользователи из соответствующих ведомств Австралии, Канады, Великобритании и Новой Зеландии [137].

4.2.2.6. Сеть JWICS

Сеть JWICS (Joint Worldwide Intelligence Communications System) –объединенная глобальная сеть разведывательных коммуникаций основывается на системе взаимосвязанных компьютерных сетей, используемых министерством обороны США, государственным департаментом США, министерством внутренней безопасности США и министерством юстиции США для передачи секретной информации вплоть до категории «совершенно секретно» по протоколам TCP/IP в безопасной среде. Фактически сеть JWICS совместно с сетью SIPRNet представляет собой своеобразный «секретный Интернет» министерства обороны США. В 1990 г. сеть JWICS заменила существовавшие ранее в министерстве обороны подсети DSNET2 и DSNET3 (служившие для передачи совершенно секретной и секретной информации соответственно), функционирующие в составе сети DDN (Defense Data Network) [139].

4.2.2.7. Системы спутниковой связи

Большое значение для обеспечения устойчивости и глобальности управления ВС США имеет использование систем спутниковой связи. Основное их назначение – это предоставление органам управления на театре военных действий или в конкретной местности надежных, защищенных каналов связи (передачи данных) с группировками вооруженных сил, тактическими соединениями, отдельными воинскими частями и каждым солдатом. Основным качеством спутниковой связи, которым не обладают другие виды связи, является способность предоставить каналы связи из любой точки мира в очень короткое время.

Перспективная система AEHF после полноценного развертывания должна стать одним из ключевых звеньев единой информационной системы GIG и управления государственных и военных организаций и основой космической системы обмена данными между субъектами боевых действий на суше и на море, в воздухе и в космосе [320].

Сравнительные тактико-технические характеристики систем MILSTAR и AEHF представлены в таблице 4.2 [320].

Таблица 4.2. Сравнительные ТТХ систем MILSTAR и AEHF [320]

Тип и объем информации	Время доставки информации потребителю		
	Система военной связи		
	Mllstar 1	Mllstar 2	AEHF
Целеуказание (1,1 МБайт)	1 ч	6 с	1 с
Видеоизображение (24 МБайт)	22 ч	2 мин	24 с
Радиолокационное изображение от БПЛА (120 Мбайт)	110 ч	12 мин	2 мин
Радиолокационное изображение от КА ДЗЗ (1 Гбайт)	880 ч	90 мин	17 мин
Подвижная связь	нет	нет	140 линий по 32 кбит/с

В единую систему военной спутниковой связи и управления США также входят военная система широкополосной спутниковой связи DSCS/WGS (Defense Satellite Communications System / Wideband Global SATCOM system), военная система узкополосной спутниковой связи UFO/MUOS (UHF Follow-On /Mobile User Objective System), военная космическая система ретрансляции данных SDS (Satellite Data System) с разведывательных спутников и военная космическая система узкополосной спутниковой связи (TacSat) для ВМС. В единую космическую систему связи и управления включены радиолокационные системы космического базирования (Space Radar-SR) и БПЛА, системы глобального позиционирования (GPS), космической метеорологической системы, спутниковых систем управления, контроля, компьютерного обеспечения, разведки, слежения и наблюдения за обстановкой на суше, на море, в воздухе и в космосе C4ISR (Command Control Communications Computers Intelligence Surveillance Reconnaissance). В состав единой военной спутниковой системы связи и управления США в период мирного и военного времени привлекаются спутники глобальной космической системы ретрансляции TDRSS (Tracking and Data Relay Satellite System). Все шире в составе единой системы военной спутниковой связи и управления используются арендуемые министерством обороны США ресурсы коммерческих систем спутниковой связи Intelsat, SES, Eutelsat, Iridium, Globalstar и др. Широкое применение в единой информационной системе глобальной связи и управления США нашли военные спутниковые системы связи Великобритании (SkyNet); Франции (Syracuze); ФРГ (SATCOMBw) и других союзников США [320].

Таким образом, спутниковая связь военного назначения США является основой информационной инфраструктуры вооруженных сил и по состоянию на начало 2013 г. включает в себя следующие системы: MILSTAR/AEHF, DSCS/WGS, UFO/MUOS, TacSat и SDS [320].

Более подробно средства спутниковых систем связи США рассмотрены в подразд. 4.4.2.6. «Спутниковые системы связи и ретрансляции данных» раздела 4.4.2. «Средства информационно-космического обеспечения».

4.2.2.8. Сети связи тактического звена управления

В настоящее время ведется модернизация систем связи тактического звена управления на основе мобильных адаптивных сетей.

Под мобильной адаптивной сетью понимается формируемая совокупностью мобильных узлов динамически меняющаяся сетевая конфигурация, обладающая следующими свойствами: отсутствием внешних механизмов настройки, то есть сеть является самоконфигурируемой и сетевой узел выполняет функции как маршрутизатора, так и оконечного устройства; относительно малым временем жизни сети в одной и той же конфигурации. Мобильная адаптивная сеть обладает рядом преимуществ по сравнению с сетями с фиксированной инфраструктурой: высокой живучестью, гибкостью топологии и автоматической адаптацией к изменениям сетевой конфигурации [107].

Новые коммуникационные возможности оказали стимулирующее воздействие на интерес к мобильным адаптивным сетям. Таким образом, в настоящее время для обеспечения включения ВС США в единое информационное пространство проводятся полномасштабные работы по внедрению сетевых информационных технологий в практику боевого применения войск. Командование и научно-исследовательские учреждения МО США уделяют огромное внимание данному направлению в связи с тем, что разработка концепции применения мобильных адаптивных сетей в военных целях и техническая реализация соответствующего оборудования являются перспективными путями развития вооруженных сил США в целом [107].

В настоящее время среди мобильных адаптивных сетей наибольшее развитие получили технологии Mesh-сетей (MANET). Такие сети могут базироваться на различных системных архитектурах и топологических схемах. Mesh-сети состоят из передающих узлов, организованных в ячеистую топологию, которая не полагается на фиксированные или статичные терминалы, но может использовать инфор-

мационное оборудование, например боевые радиостанции, отдельные узлы, формируя сеть связи в соответствии с решаемыми задачами и между абонентами, задействованными в таком решении. Избыточность и надежность являются ключевыми элементами таких сетей. Когда любой одиночный узел больше не работает, функциональные узлы могут еще сообщаться друг с другом, напрямую или через промежуточные узлы. В связи с этим такие динамические, самоорганизующиеся сети также описываются как самовосстанавливаемые [327].

Технологии для тактических сетей постоянно развиваются. К последним инициативам по их развитию можно отнести создание следующих технологических решений [327].

- C2OTM (Command-and-Control On the Move) – оперативное управление в движении, использует мобильные каналы связи для передачи данных в/из безопасного Интернета Минобороны США, образованного сетями SIPRNet и NIPRNet.
- DAMA (Demand Accessed Multiple Access) – группа стандартов, предоставляющая множественный доступ к каналов по требованию, используемых в гибких, настраиваемых пользователями спутниковых терминалах, передающих данные и речь.
- FBCB2 (Force XXI Battle Command Brigade and Below) – стандарты для динамического боевого управления мобильной боевой тактической сетью уровня бригады и ниже.
- JAUS (Joint Architecture for Unmanned Systems) – объединенная архитектура для беспилотных систем. Представляет собой общие протоколы операционных систем для выполнения боевых роботизированных операций в рамках концепции глобальной системы.
- JTRS (Joint Tactical Radio System) – сеть на базе перепрограммируемых SDR радиостанций, использующих единую архитектуру связи, на основе ячеистой сети.
- MBCOTM (Mounted Battle Command on the Move – мобильное управление боем в движении). Облегчает прием и передачу данных для устройств SINCGARS (Single Channel Ground and Airborne Radio System) единой системы одноканальной радиосвязи наземных войск и авиации в боевых машинах BRADLEY и SRYKER, помогая повышать ситуационную осведомленность. Функционирует поверх суще-

ствующей армейской системы боевого командования ABCS.

- MOSAIC (Multifunctional On the Move Secure Adaptive Integrated Communications) – многофункциональная мобильная адаптируемая сеть, основана на базе web 2.0, интернет-протоколах, поддерживающих беспроводной доступ. Может быть сопряжена с наземными и спутниковыми сетями для возможности установления связи в глобальном масштабе с высокой степенью гарантии безопасности информации за счет встроенного программируемого шифрования и способности к самовосстановлению.
- NCES (Net-Centric Enterprise Services – сетецентрические службы уровня подразделения на основе Web 2.0 для минобороны США).
- TACSAT – группа протоколов, задействующих сеть тактической спутниковой связи, орбитальную инициативу «объединенное боевое пространство» JWS (Joint Warfighting Space), также известную под названием Roadrunner, со встроенной разведывательной поддержкой бойцов во время сетецентрических боевых действий.
- WAND (Wireless Adaptive Network Development) – разработка беспроводной адаптивной системы связи, которая использует принципы ячеистой сети. Технология нацелена на тактические радиостанции с использованием коммерческих компонентов, которые являются самоперенастраиваемыми под радиоэлектронную обстановку, на фоне которой они функционируют, автоматически переключая частоты в целях ухода от помех и улучшая работоспособность сети в широком спектре задач.
- WIN-T (Warfighter Information Network – Tactical – армейская тактическая коммуникационная система). Высокоскоростные широкополосные сетевые протоколы для мобильной связи в тактическом звене американской армии.
- VOIP (Voice Over Internet Protocols) – коммерческий протокол передачи голоса по IP-протоколу, модифицированный для использования в военных сотовых и широкополосных коммуникационных сетях.

Все перечисленные технологии поддерживают политику «солдат как система» по интеграции отдельных подразделений и бойцов в сетецентрическую среду, интерфейс с высокоуровневыми архитекту-

рами, например спутниками, стратегическими БПЛА и боевыми роботами. Вдобавок эти технологии используют открытые коммерческие стандарты и многоуровневые архитектуры, что позволяет ускорить их модернизацию за счет добавления или отсоединения отдельных модулей системы, основанных на реализации передовых технологий [327].

4.2.2.9. Концепция BITS

Концепция BITS (Battlefield Information Transmission System – системы передачи информации на поле боя) – концепция создания принципиально новой объектовой системы передачи информации на поле боя для оперативно-тактического и тактического звеньев управления сухопутных войск США. Она явится, в определенном смысле, частью или продолжением единой интегрированной сети информационной инфраструктуры министерства обороны США – DISN и, по существу, будет представлять собой средство распространения зоны действия DISN на ТВД.

Информационная система BITS предназначена для обеспечения потребности в передаче информации в интересах перспективных автоматизированных систем боевого управления сухопутных войск США [303]:

- ABCS (Army Battle Command System) – уровень управления от бригады и выше.
- FBCB (Force XXI Battle Command for Brigade and Below) – уровень управления от бригады и ниже.

В законченном виде система связи СВ США в зоне оперативного развертывания будет включать в себя:

- районную систему общего пользования на коммутаторах ATM, обладающую высокой пропускной способностью, сопряженную через стационарные магистральные трансокеанские волоконно-оптические линии и спутниковые военные и коммерческие линии связи с информационными системами на континентальной части США, базами постоянной дислокации и сетью информационных систем ВС DISN;
- функционирующую на основе IP-протоколов систему сетей пакетной и одноканальной радиосвязи на уровне бригада и ниже, характеризующуюся высокой мобильностью пользователей, с мобильным центрами связи – узлами радиодоступа в районную систему общего пользования;

- системы персональной сотовой и спутниковой радиосвязи;
- системы спутниковой связи;
- космические системы прямого циркулярного вещания.

Топологическая структура системы BITS будет состоять из нескольких основных компонентов:

- территориальной полевой коммутируемой системы связи общего пользования (ССОП);
- сетей и средств обработки информации воздушного базирования.

Территориальная полевая коммутируемая ССОП имеет структуру «сетка» и включает наземные сети радиосвязи тактического звена управления. Данный компонент инфраструктуры состоит из сетей, предоставляющих услуги передачи речи и данных. Сети способны адаптироваться к перемещению узлов. Они не имеют центральных узлов или базовых станций, которые характерны для уязвимой топологии типа «звезда».

Сети и средства обработки информации воздушного базирования обеспечивают ретрансляцию данных и предоставление информационных услуг подразделениям, расположенным за пределами зон обслуживания локальных сетей. Они служат также для расширения зоны обслуживания системы связи. В качестве носителей оборудования связи в данной системе используются автономные летательные аппараты, зона обслуживания которых распространяется на ТВД. Эти аппараты соединены линиями связи между собой с узлами и станциями наземного оборудования, а также с другими воздушными и космическими компонентами единой информационной инфраструктуры.

Это разделение условно, поскольку интерфейсы между компонентами бесшовные и прозрачные для пользователей. Любой объект информационной инфраструктуры потенциально может в автоматическом режиме непосредственно взаимодействовать и обмениваться информацией с другим объектом [291].

4.2.2.10. Система WIN-T

Система WIN-T (Warfighter Information Network – Tactical) – автоматизированная система связи для оперативно-тактического звена управления в звене «бригада – батальон – рота – взвод», которая в перспективе может быть доведена до отдельного военнослужащего. WIN-T представляет собой высокоскоростную беспроводную тактическую сеть на базе реализации web 2.0 и архитектуры WNaN (Wireless

Network After Next), которые будут объединены с радиостанциями на основе технологии NGN (Next Generation Net). Например, с радиостанциями, разработанными по стандарту «программируемого радио» SDR программы JTRS (Joint Tactical Radio System Network), базирующимися на Mesh-архитектуре, которая позволит быстро адаптировать и перенастроить сети при изменении оперативных условий, включая воздействие помех, радиоперехват и хакерские атаки. Система WIN-T совместима с имеющимися в корпусе и дивизии информационными сетями. В 2012 г. на вооружение поступила 13-я версия системы WIN-T. Основной особенностью новой версии системы WIN-T, ранее недоступной, является ее способность управления боем на марше. Ранее приходилось разворачивать стационарные средства спутниковой связи, антенны радиосвязи и кабели между устройствами. При разработке сети WIN-T использовались готовые коммерческие продукты в области новых информационных и сетевых технологий и средства IP-технологии [10, 29, 108, 318, 327].

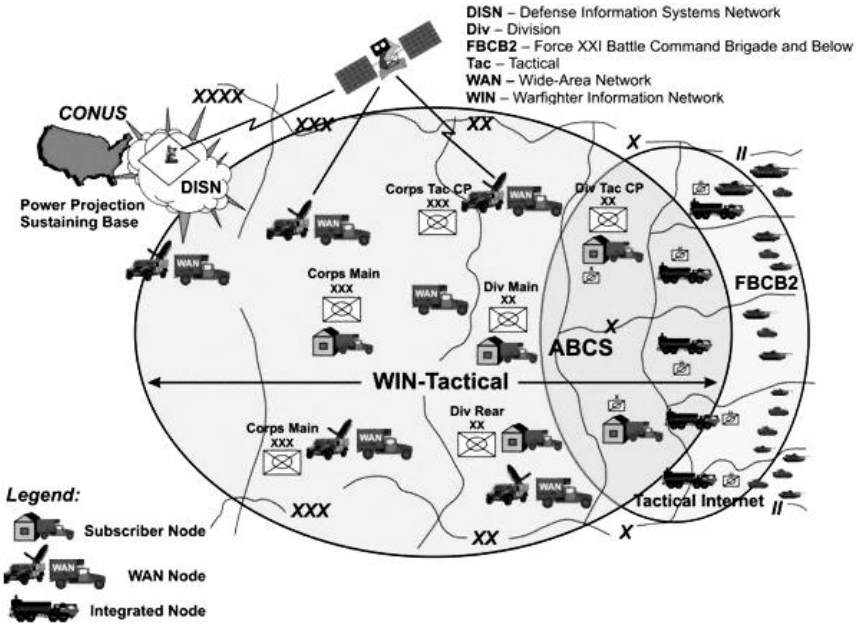


Рис. 4.5. Архитектура системы WIN-T [327]

Разработка WIN-T официально началась в 2002 г., при этом учитывались просчеты в Иракской кампании «Буря в пустыне». В сле-

дующих версиях системы учитывается опыт ведения боев в Афганистане в 2001 г. и в Ираке в 2003 г. Первые комплекты WIN-T поступили на вооружение в 2008 г., заменяя предыдущие системы Mobile Subscriber Unit [108].

Ведущим разработчиком системы WIN-T явилась компания General Dynamics с главным партнером Lockheed Martin. Ведущие разработчики этих двух компаний отвечают за коммуникации, сетевые системы и интегрирующие платформы, привлекая соисполнителей от BAE Systems, Harris Corporation, L-3 Communications и Cisco Systems [108].

4.2.2.11. Сеть тактический интернет

В ходе реализации программ модернизации сетей связи тактического звена предполагается также модернизировать систему «Тактический Интернет» (Tactical Internet). Эта система обеспечивает необходимые сетевые подключения в звене «дивизия – бригада» и поддерживает относительно высокую интенсивность информационного обмена и взаимодействия в таких АСУ войсками армейского корпуса, как [29]:

- АСУ маневром MCS (Maneuver Control System);
- АСУ обработкой и анализом разведывательной информации ASAS (All Source Analysis System);
- АСУ ПВО FAADCIS (Forward Area Air Defense Command, Control Intelligence System);
- АСУ огнем полевой артиллерии AFATDS (Advanced Field Artillery Tactical Data System);
- АСУ тыловым обеспечением CSSCS (Combat Service Support Command System).

Также ведутся разработки совмещенных систем связи и навигационного обеспечения. Так, в Ираке успешно использовалась распределенная информационная система MTS (Army's Movement Tracking System). В ней на основе радиоизлучающих датчиков, стационарных и портативных сканеров, системы GPS, беспроводного доступа и тактического интернета непрерывно отслеживается положение всех наземных подвижных объектов (танков, БТР, БМП) на театре военных действий, от экипажей которых органы тыла получали запросы на поставку топлива, боеприпасов и других видов обеспечения. В системе было задействовано около 4000 бортовых компьютеров и порядка 100 серверов. Система MTS обошлась армии США в 418 млн долл.

и была сформирована в течение 3 лет. Компьютеры штаба 5-го армейского корпуса – основной ударной силы группировки в Ираке – были способны самостоятельно сопровождать до 1000 наземных объектов. Командиры эскадрилий палубной авиации планировали вылеты своих экипажей вместе с коллегами из армейской авиации, также пользуясь общей информационной системой [121, 127].

Подводя итоги, можно сделать вывод, что в настоящее время и в среднесрочной перспективе минобороны США уже сформировало единую сеть: «средства разведки – пункты управления – средства поражения» на основе IP-технологий для всех участников боевых действий, средств разведки и поражения. Такая сеть обеспечивает своевременное предоставление командирам точных данных и знаний о ситуации на поле боя (ситуационную осведомленность), сокращает время на поражение цели до нескольких минут, а также обеспечивает полностью межмашинный обмен информацией в процессе подготовки и осуществления целеуказания [43].

Так, для этого в ВС США осуществляется поставка перспективных средств многовидовой тактической системы радиосвязи JTRS (Joint Tactical Radio System) и терминалов спутниковой связи FAB-T, развертывается новая система спутниковой связи TSAT на основе IP-технологии и др. Например, новые спутники AEHF смогут обеспечить передачу видеоизображения, получаемого от БПЛА, потребителю в течение нескольких секунд, в то время как на передачу изображения такого же объема через спутники MilStar-2 сейчас требуется больше 2 мин [43].

В долгосрочной перспективе (к 2020 г.) вся информация (голосовая информация, данные, фото- и видеоизображения и др.) будет передаваться через сеть Constellation Net. По мнению американских специалистов, такой подход позволит не только осуществить «горизонтальную» интеграцию средств управления, связи, разведки и наблюдения и обеспечить межмашинную обработку информации, но и повысить эффективность ее распределения, а также создать необходимые условия для обеспечения информационной безопасности и более эффективного применения высокоточных средств поражения [43].

4.2.3. Системы разведывательного обеспечения

4.2.3.1. Общие тенденции развития систем разведывательного обеспечения

В эпоху становления информационного общества во многом изменился и характер выполнения своих задач разведкой. Теперь в качестве основной задачи, кроме задачи опережающего оповещения высшего руководства страны о возможной агрессии, на разведывательные службы возложена и задача достижения информационного превосходства над противником.

Информационные системы сетецентрической среды, собирающие данные, охватывают открытые источники, традиционную разведку, системы наблюдения и обнаружения. Собранные данные становятся информацией после их обработки и приведения к виду, удобному для пользования [16].

По мнению военных специалистов, в результате успешной реализации концепции единого информационного пространства коренным образом изменится порядок обеспечения органов военного управления данными о противнике, своих войсках и окружающей местности.

Эффективность мероприятий, проводимых в рамках концепции сетецентрической войны, ставится в зависимость от взаимосвязанности средств автоматизации органов управления, систем вооружения и боевого обеспечения, а также от наличия эффективной интеграции различных сетей и, в первую очередь, автоматизированных систем боевого управления, связи, разведки и наблюдения. Возможность достичь адекватной степени интеграции зависит от насыщенности вооруженных сил средствами глобальной (например, спутниковой) и тактической (БПЛА, наземные сенсорные устройства и т.п.) разведки, интегрированными системами навигации и управления оружием (GPS), а также системами связи, обеспечивающими координацию действий и управление практически в режиме реального времени. В современных условиях основным препятствием для реализации концепции сетецентрической войны в организационно-техническом плане является тот факт, что сети разрознены. Информация от разных средств разведки (спутников связи, беспилотных аппаратов, самолетов, наземных сил) проходит по разным каналам и далеко не всегда и не в реальном масштабе времени попадает в соответствующие базы

данных тех потребителей, которым она в наибольшей степени необходима. При этом форматы данных часто оказываются несовместимыми между собой, что затрудняет горизонтальную интеграцию пунктов приема информации и ее потребителей [3, 95, 121, 127].

При традиционной организации информационного обеспечения операций органы (пункты) управления различных звеньев должны были принимать решения и руководить находящимися в их подчинении добывающими и боевыми формированиями на основе данных, полученных собственными силами и средствами разведки, а также той информации, с которой вышестоящий штаб считал целесообразным ознакомить подчиненные звенья управления. При необходимости последние могли установленным порядком подавать запросы на получение дополнительных сведений от вышестоящих органов управления, имеющих в своем подчинении системы космической и воздушной, агентурной и радиоэлектронной разведки [206].

Межвидовой обмен разведывательной информацией, полученной различными добывающими системами, также происходил по специальным заявкам с санкции соответствующих органов военного управления. При этом нередко требовались существенные доработки предоставляемых данных для их использования информационно-управляющими и особенно исполнительными элементами другого вида или рода войск. Сложный порядок и большая продолжительность процесса обмена информацией в ряде случаев не позволяли своевременно доводить необходимые сведения до исполнительных элементов [206].

При такой организации разведывательно-информационного обеспечения командующие и штабы одного вида вооруженных сил (уровня управления) могли и не знать о наличии необходимой им информации о противнике и своих войсках (силах) в органах управления другого вида (уровня), что приводило к дублированию задач по добыванию необходимых сведений, нерациональному использованию средств поражения, а нередко и к ошибочному нанесению ударов по своим подразделениям (объектам) [206].

Кроме того, каждая разведывательная система имела специфические программно-аппаратные средства, соответствующие требованиям конкретного вида ВС, а также собственные форматы представления добываемых сведений и протоколы обмена разведданными. В связи с этим информация, полученная автоматизированной системой разведки, например, ВМС или артиллерии, могла эффективно доводиться

и использоваться только потребителями данного вида вооруженных сил (рода войск) [206].

Реализация единого информационного пространства в рамках концепции сетецентрической войны должна не только устранить указанные недостатки, но и коренным образом изменить подход к организации оперативного планирования и управления войсками и оружием в ходе повседневной деятельности и во время военных действий. Разведывательная информация от различных систем добывания после обработки и утверждения соответствующим начальником будет непрерывно поступать в базы данных единого информационного пространства, откуда ее смогут получить (по запросу или в режиме автоматического доведения) все заинтересованные должностные лица при наличии у них сетевого подключения и соответствующих прав доступа к информации. При этом разведданные будут предоставляться в стандартных форматах, адаптированных для немедленного использования как в штабах, так и в системах наведения высокоточного оружия различной видовой принадлежности [206].

В настоящее время с полной уверенностью можно утверждать и то, что «информационная революция» оказывает принципиальное влияние на разведку, делая ее более комплексной, своевременной и достоверной. Этим и объясняется внедрение в разведку всех новейших технологических достижений, таких как быстродействующие ЭВМ последних поколений, датчики слежения на новых физических принципах, системы с использованием элементов искусственного интеллекта и многое другое. В оперативную и информационную работу разведывательных ведомств повсеместно внедряют передовые технические решения и технологии, созданные и разработанные государственными и частными исследовательскими организациями, а также заимствованные в других странах.

Американские военные специалисты считают, что современные и будущие войны – это войны разведок и что разведка является ключом к достижению успеха. Например, командир 1 бртд, задействованной в Ираке, генерал-майор М. Дэмпси (Martin E. Dempsy) отмечал: «По существу, здесь, в Багдаде, мы делаем две вещи: мы или боремся за информацию, или ведем борьбу на основе полученной информации». Более того, будущие войны представлены не просто как высокотехнологичные, а в первую очередь как «сетевые», что требует объединения всех участников боевых действий в рамках мероприятий по реализации положений концепции сетецентрической войны, предусматривающей предоставление точных и своевременных данных об

обстановке на поле боя и обеспечивающей поражение объектов и целей противника в реальном масштабе времени [43].

Реализация концепции сетецентрических войн позволяет перейти к ведению разведки в форме объединенных (комплексных) разведывательных операций разнородными силами, использующими разнообразные способы разведывательной деятельности. При этом главными изменениями будут сокращение временного цикла, то есть быстрая локализация района нахождения цели средством, имеющим большую зону охвата и низкую точность определения координат, а также постановка (перенацеливание) уточненных задач на доразведку высокоточным средствам разведки. Таким образом, вместо «времязатратного» способа действия воздушного поста оптико-электронной разведки района можно сразу применять более быстрый способ разведки маршрута или разведки объекта [43].

В качестве одного из наиболее наглядных примеров можно привести следующую ситуацию. Чтобы определить местонахождение цели с необходимой для применения средств ВТО точностью в настоящее время требуется одновременное задействование нескольких самолетов радио- и радиотехнической разведки только по одной цели. В принципе, возможно применение и одного такого средства, но в этом случае время выполнения этой задачи значительно возрастает. Объясняется это тем, что точность определения координат зависит от базы пеленгования, то есть, чтобы провести точное пеленгование цели одним самолетом (позволяющее применять высокоточные средства поражения), ему необходимо преодолеть некоторое расстояние, что крайне критично для пеленгования мобильных объектов. В этом случае процесс пеленгования может занимать более 10 мин, а точность далеко не всегда позволит применять высокоточные средства поражения [43].

При использовании связанных между собой разнородных средств разведки процесс определения местоположения цели занимает несколько секунд, и при этом обеспечивается требуемая точность определения координат за счет более широкой базы пеленгования. Для подобных целей может применяться и аппаратура, устанавливаемая по программе SMART (Scalable, Modular, Airborne, Relay, Terminals) Platforms, которая предусматривает размещение дополнительного оборудования (средств разведки, блоков передачи данных и т.д.) в интересах разведобеспечения на воздушных (в т.ч. БПЛА), наземных (возможно, танки, БМП) и морских платформах, связанных между собой в глобальной сети сбора и передачи данных [43].

Другой пример – одно средство РРТР способно обнаружить цель и определить ее местоположение с требуемой для применения ВТО точностью только после необходимого количества измерений. В свою очередь, средства оптико-электронной разведки могут обеспечить точное определение цели (объекта) сразу, но для того, чтобы найти этот объект, потребуется очень много времени, потому что такие средства разведки, как правило, имеют небольшую (узкую) полосу обзора. Если объединить эти два средства и передавать данные от средства РРТР (направление на цель) непосредственно на БПЛА видовой разведки, то можно существенно сократить время обнаружения местоположения цели, обеспечив при этом требуемую точность определения координат и минимизировав возможное дезинформационное воздействие [43].

В третьем случае оператор системы сбора, обработки и распределения разведывательной информации может получать данные о перемещении цели от самолета Е8-С радиолокационной разведки наземных целей и управления нанесением ударов системы JSTARS (Joint Surveillance Target Attack Radar System) и др., а затем запросить дополнительные сведения от БПЛА. Если БПЛА подтверждает (распознает) цель, то в таком случае происходит немедленная передача команды средству огневого поражения. Это сильно сокращает время обнаружения, распознавания и передачи данных целеуказания средствам поражения, что особенно важно при борьбе с мобильными целями [43].

Позволяя средствам разведки обмениваться информацией между собой (объединяя их на основе сетецентрической среды), военное руководство пытается достичь синергетического эффекта, когда комбинированное действие двух или нескольких разведывательных средств превышает эффективность, обеспечиваемую каждым средством в отдельности. «Объединяя средства разведки в единую «систему систем», мы тем самым повышаем угол поля зрения (охвата), разрешающую способность, сокращаем скорость перенацеливания средств, обеспечиваем ведение разведки в любое время суток в любых погодных условиях и т. д., а также снижаем недостатки каждого средства в отдельности», – отмечает один из военных экспертов США [43].

Дальнейшими планами командования ВС США предусматривается, что будущие возможности по ведению разведки позволят обеспечить проведение эффективных операций по поражению любых целей в любых погодных условиях днем и ночью в любой точке земного шара. Для выполнения этих задач и осуществляется комплекс органи-

зационных и технических мероприятий по созданию действительно эффективной и комплексной системы разведки, предусматривающей интеграцию всех ее средств на театре войны в единую разведывательно-ударную сеть на временной основе, осуществление как вертикальной, так и горизонтальной их интеграции, а также реализацию новых принципов разведывательного обеспечения операций [43].

Таким образом, проведенный анализ перспектив развития систем разведывательного обеспечения показал наличие следующих тенденций:

- основным средством получения разведывательных сведений становятся космические системы радио-, радиотехнической и оптико-электронной разведки, информация от которых обрабатывается комплексно с данными космических навигационных систем и позволяет точно определить местонахождение своих сил и средств, а также сил и средств противника;
- источниками разведывательных сведений становятся практически все средства вооружения, имеющие оптические, электронные, радио- и радиолокационные датчики, а также все участники боевых действий;
- за счет комплексирования разнородных средств резко снижается продолжительность циклов ведения разведки с одновременным увеличением их достоверности и точности;
- всю большую роль в качестве оперативных средств ведения наблюдения получают разведывательные средства на БПЛА. При этом перспективным направлением является создание на основе БПЛА разведывательно-ударных комплексов, реализующих принцип «обнаружил–уничтожил»;
- передача сведений от разведывательных датчиков и обеспечение разведывательной информацией потребителей производятся в едином информационном пространстве в соответствии с уровнем допуска потребителей и их принадлежностью к конкретному уровню управления;
- обработка разведывательных данных ведется с использованием суперкомпьютерных технологий на основе методов обработки Big Date и предусматривает формирование единого виртуального театра военных действий на основе совмещения данных от всех разведывательных датчиков;
- достижение принципиально нового уровня обобщения и детализации обстановки за счет комплексной обработки

информации от различных источников, учета различных незначительных, на первый взгляд, факторов, использования интеллектуальных алгоритмов обработки.

4.2.3.2. Автоматизированная система сбора, обработки и распределения разведывательной информации DCGS

Одним из основных мероприятий, проводимых в настоящее время военным руководством ВС США и направленных на обеспечение всесторонней «вертикальной» и «горизонтальной» интеграции средств разведки и различных разведывательных ресурсов, является развертывание автоматизированной системы сбора, обработки и распределения разведывательной информации DCGS (Distributed Common Ground System) [43, 318].

Программа DCGS предусматривает создание и внедрение аппаратно-программных средств, обеспечивающих комплексирование разведданных из разнородных источников, автоматизацию процессов обработки и дешифрования поступающей информации, а также формирование общей базы разведывательных сведений с распределенным доступом к ней. Наряду с этим планируется унифицировать архитектуру наземных средств сбора, анализа и представления данных о противнике, создать единое программное обеспечение, снизить избыточность поступающей информации, повысить качество ее отображения, а также скорость поиска и доведения до потребителя [318].

Заказчиком разработки автоматизированной системы DCGS выступило разведывательное управление военно-воздушных сил DARO, а главными задачами являлись [43]:

- объединение существующих и перспективных станций приема и обработки данных видовой разведки в единую структуру CIGSS (Common Imagery Ground / Surface System Architecture);
- объединение станций приема и обработки данных радио- и радиотехнической разведки в единую структуру JASA (Joint Airborne SIGINT Architecture);
- интеграция структур CIGSS и JASA в единую систему сбора, обработки и распределения разведывательных данных DCGS (Distributed Common Ground System).

Эти мероприятия осуществляются с целью принятия на вооружение унифицированных средств сбора, обработки и анализа, которые должны заменить семейство разрозненных комплексов. Система

DCGS обеспечит качественно новый уровень оперативной и технической совместимости систем разведки, наблюдения, боевого управления и средств поражения в рамках единой для всех видов вооруженных сил информационно-управляющей инфраструктуры [43, 318].

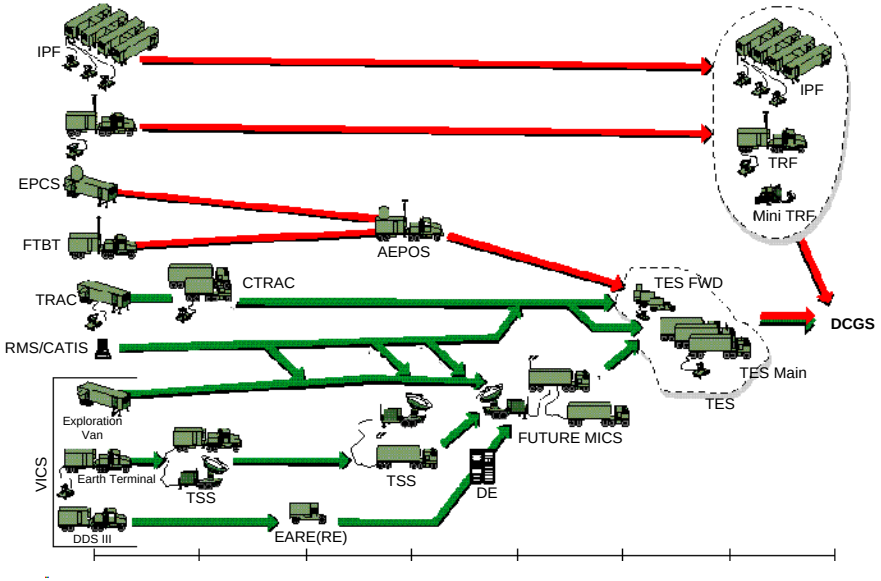


Рис. 4.6. Объединение различных разведывательных систем в систему DCGS

По замыслу руководства американских ВС, система DCGS, разработанная путем модернизации, интеграции и объединения существующих разнородных средств сбора, обработки и хранения развед-данных, должна представлять собой распределенную компьютерную сеть, организованную на базе стандартных телекоммуникационных Интернет-протоколов, снабженную своей поисковой системой и порталом для доступа к ее ресурсам [318].

В систему DCGS входят (рис. 4.6) [95]:

- на тактическом уровне – сеть управления огнем полевой артиллерии; наземные станции радиолокационной разведки; разведывательно-сигнализационные приборы; армейская авиация; беспилотные летательные аппараты;
- на оперативном уровне – экспедиционные силы морской пехоты; беспилотные летательные аппараты; силы войско-

вой разведки и специальных операций; комплексы РРТР и РЭП «Prophet»; средства разведки авианосных ударных групп;

- на стратегическом уровне – разведывательные самолеты (EC-130, E-8C, U-2R) и спутники; силы специальных операций; базы данных разведывательного сообщества; средства разведки союзников.

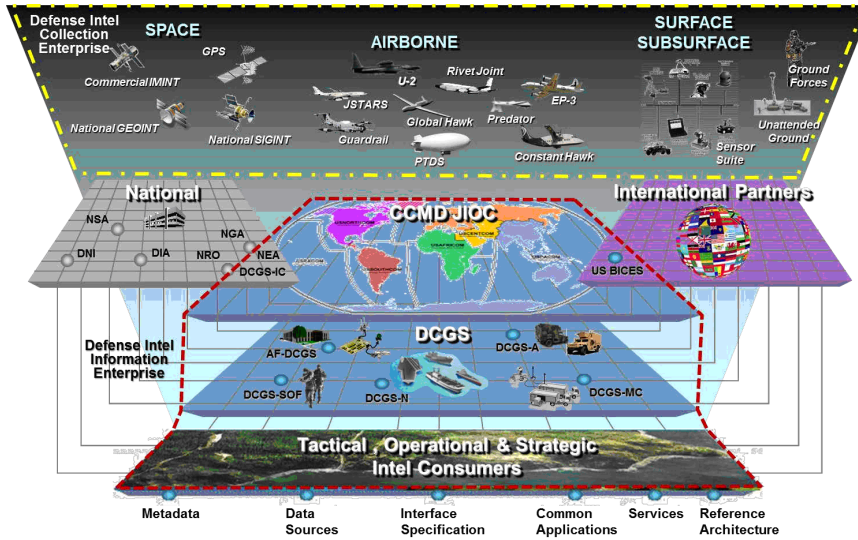


Рис. 4.7. Система глобального разведывательного обеспечения силовых ведомств США и их союзников

В интересах организации сбора, обработки и распределения разведывательных данных могут применяться следующие комплексы [95].

- Подвижный комплексный оконечный пункт тактической связи MITT (Mobile Integrated Tactical Terminal), который осуществляет прием данных, поступающих от разнообразных средств добывания всех звеньев управления, а также подготовку и распределение разведывательной информации в интересах обеспечения командиров тактического звена управления.
- Автоматизированная система обработки и анализа разведывательной информации сухопутных войск ASAS (All Source Analysis System). Ее аппаратура развертывается во

всех звеньях управления. Основными задачами АСУ ASAS являются: планирование и управление проведением разведывательных, контрразведывательных операций и РЭБ; управление средствами сбора, обработки и анализа разведывательной информации; доведение разведданных до потребителей.

- Станция обработки данных РЛС ETRAC (Enhanced Tactical Radar Corelator), функционирующая в интересах корпусного звена управления, осуществляет прием, обработку и распределение данных разведки, поступающих от станции радиолокационной разведки самолета-разведчика U-2R.
- Модуль наземной станции объединенной радиолокационной разведывательной системы JSTARS (Ground Station Module – GSM). Аппаратура модуля осуществляет прием данных радиолокационной разведки от бортовой станции AN/APY-3 самолета E-8C.

Разведывательные органы всех видов вооруженных сил США получают новое программное обеспечение, позволяющее осуществлять обработку и обмен разведданными от разных источников между системами DCGS всех видов вооруженных сил. Обмен изображениями и текстовой информацией происходит в режиме реального времени. Разведывательные данные поступают не конкретному потребителю, а на общий сайт или ресурс и становятся доступными всем заинтересованным лицам [95].

Для совместной обработки разнородных сведений о противнике в рамках организации взаимодействия DCGS с разведывательными системами ВС стран НАТО предполагается объединить в единый комплекс стоящие на вооружении и перспективные автоматизированные системы разведки Североатлантического союза. Интеграцию систем разведки блока НАТО планируется осуществлять в рамках программы ISTAR (Intelligence, surveillance, target acquisition, and reconnaissance), которая предусматривает приведение средств добывания, сбора, обработки и доведения разведывательной информации в соответствие с требованиями новых стандартов НАТО – STANAGs (Standardization Agreement). Данные стандарты призваны установить не только единые форматы представления различных сведений и протоколы обмена разведданными, но и другие важные параметры сопрягаемых АСР, необходимые для обеспечения их полной совместимости еще на этапе проектирования (амплитудно-спектральные характеристики сигналов, порядок их передачи, первичной обработки и хранения, несущие частоты

и виды модуляции, а также состав и структура баз данных разведывательной информации и соответствующих метаданных) [206].

При применении средств разведки различных видов, связанных при этом между собой, в несколько раз уменьшается время и повышается точность определения положения цели. Так, оператор системы DCGS может в диалоговом режиме, щелкнув мышкой на изображении цели, любые перемещения которой отображаются на его дисплее в реальном режиме времени, узнать всю информацию о цели, в том числе тип, координаты и немедленно передать команду на ее поражение оптимальному средству поражения. Характерным примером применения системы DCGS может быть следующий: оператор системы сбора, обработки и распределения разведывательной информации DCGS сможет получать данные о перемещении цели от самолета разведчика E-8C радиолокационной разведки наземных целей и управления нанесением ударов системы JSTARS (при этом все перемещения цели отображаются на дисплее), затем запросить дополнительные сведения от БПЛА (одним «кликом» в диалоговом окне), если беспилотный аппарат подтверждает (распознает) цель, то в таком случае происходит немедленная передача команды средству огневого поражения. Это радикально сокращает время обнаружения, распознавания и передачи данных целеуказания средствам поражения, что особенно важно при борьбе с мобильными целями [95].

Коммуникационную основу DCGS составляет глобальная информационная сеть GIG, строящаяся на основе интегрированной системы передачи данных DISN, а также перспективная автоматизированная система связи для оперативно-тактического звена управления WIN-T. Такая сеть, обладающая высокой пропускной способностью, масштабируемостью, а также устойчивостью к внешним воздействиям, обеспечит непрерывный и единообразный доступ к необходимым разведывательным данным всех авторизованных пользователей в соответствии с их категорией и полномочиями (правами) по доступу к информации [318].

Система DCGS имеет сервис-ориентированную архитектуру SOA. Принципиальным ее отличием от архитектуры «клиент – сервер» является наличие каталога услуг, который обеспечивает их учет и возможность поиска, предоставляя возможность обмена данными между территориально разнесенными сервисами без необходимости настройки жесткой адресации в сети. При этом сервисы-поставщики информации предоставляют услуги в формализованном виде, то есть публикуют данные о наличии развединформации, способе ее получения и

месте ее расположения в каталоге услуг, в котором накапливаются сведения обо всей имеющейся информации для ее последующего поиска. Такое построение позволяет сервисам-потребителям находить требуемую информацию в сети и осуществлять инициализацию соответствующих сервисов-поставщиков [318].

Основу системы DCGS составляет разрабатываемый интегрированный комплекс обработки информации DIB (DCGS Integration Backbone), который позволит связать станции DCGS между собой, а также с аналогичными системами других видов вооруженных сил. Кроме того, для подобных целей может применяться и аппаратура, устанавливаемая по программе SMART Platforms, которая предусматривает размещение дополнительного оборудования (средств разведки, блоков передачи данных и т. д.) в интересах разведывательного обеспечения на воздушных, наземных и морских платформах, связанных между собой в глобальной сети сбора и передачи данных [95].

Интегрированный комплекс обработки информации DIB представляет собой единый для всех видов вооруженных сил согласованный и утвержденный набор стандартов представления данных, интерфейсов, а также компьютерных программ, разработанных по принципу SOA, позволяющих осуществлять хранение, пересылку, обработку, объединение и представление разведывательной информации от разнородных средств разведки. Главной целью создания DIB-комплекса является обеспечение совместимости систем и средств разведки видов ВС и формирование единого информационного пространства ТВД [318].

Совместимость приложений и баз данных в новой архитектуре обеспечивается путем [318]:

- разработки новых сервисов на платформах программирования сетевых приложений Java 2 Enterprise Edition и Microsoft NET;
- создания специальных программных модулей сопряжения (адаптеров) для обращения к уже существующим базам данных и приложениям;
- адаптации некоторых ранее имеющихся приложений путем переработки части их программного кода для прямого включения в новую информационную среду;
- традиционного прямого межмодульного взаимодействия (в отдельных случаях).

В состав комплекса DIB входят [318]:

1. Библиотеки:

- данных видовой разведки национального управления геопространственной разведки в стандарте NITF (National Imagery Transmission Format);
- фонда геопространственных данных, коммерческих снимков земной поверхности;
- хранилища радиолокационных изображений движущихся целей, цифровых видеоданных, донесений;
- единой базы данных вооруженных сил США.

2. Сервисы обработки разведывательной информации:
   - планирования применения и оперативного управления средствами обнаружения;
   - интеграции информации;
   - наблюдения и предупреждения;
   - автоматического извлечения свойств целей, их распознавания и сопровождения;
   - поддержки многослойного представления данных;
   - управления системой наземных автономных разведывательных датчиков «Argus»;
   - точной координатной привязки к местности;
   - учета запланированных и выявленных воздушных трасс;
   - интерфейсы каналов глобальной системы непосредственного спутникового вещания GBS и тактических каналов связи;
   - система поддержки использования данных видовой разведки;
   - процессор обработки данных видовой разведки.
3. Средства визуального отображения гипертекста, изображений в формате NITF, геопространственных данных, текстовых файлов, данных измерительно-сигнатурной разведки и видеоизображений.
4. Сервисы общего назначения и поддержки функционирования систем: навигации и доступа к данным, системные, взаимодействия, поддержки синтеза данных, поисковых запросов, управления информационными потоками, безопасности информации.

Для удовлетворения отдельных требований относительно возможности интегрирования существующих приложений обработки/анализа разведывательной информации и баз данных в новую архитектуру комплекса DIB было установлено пять уровней интеграции –

от 0 до 4. Нулевой (классический) уровень позволяет взаимодействовать различным элементам системы на основе интерфейса «точка-точка». На втором и третьем уровнях организуется взаимодействие баз данных/приложений. Для этого случая разработан специальный адаптер данных/приложений, обеспечивающий свободный доступ к информации другим подсистемам. В частности, на третьем уровне производится перезапись в определенный формат некоторой части программного кода существующего приложения, что позволит использовать его в структуре комплекса DIB. Четвертый уровень подразумевает составление взамен старых приложений, не подлежащих модификации, новых, полностью основанных на web-сервисах. Предусмотрена возможность добавления, в случае необходимости, новых сервисов в состав комплекса DIB [318].

В дальнейшем планируется интеграция DIB в состав единого комплекса сетевого обслуживания – NCES (Net-Centric Enterprise Service) глобальной информационной сети министерства обороны GIG и в единую операционную среду – SOSCOE (System of System Common Operating Environment) перспективной автоматизированной системы управления тактического звена сухопутных войск, разрабатываемой в рамках программы «Боевая техника будущего» FCS (Future Combat Systems) [318].

Как считают американские военные специалисты, развертывание системы DCGS позволит не только приступить к масштабным преобразованиям системы разведки, но и перейти к новому принципу осуществления всего разведывательного обеспечения, именуемого «адаптивное взаимодействие» («Reach-in»). Данный принцип касается возможности пользователей глобальной информационной сети иметь доступ к информации от различных источников, в том числе других компонентов объединенных сил, развернутых на театре войны или находящихся на континентальной части США [95].

На начальном этапе, с учетом особенностей применения стоящих на вооружении сухопутных войск, ВВС и ВМС средств разведки и поражения, работы по программе DCGS велись этими видами ВС самостоятельно в рамках создания отдельных ее элементов как самостоятельных видовых систем. Так, в интересах СВ разрабатывается система DCGS-A (DCGS-Army), ВВС – DCGS-AF (DCGS-Air Force), а ВМС – DCGS-N (DCGS-Navy). В дальнейшем было обеспечено их функционирование в составе единой глобальной системы министерства обороны DCGS [318].

4.2.3.3. Система DCGS-AF

Мероприятия по развертыванию экспериментальной системы сбора, обработки и распределения информации DCGS-AF для ВВС начались в июне 2005 г. с размещения 64 рабочих станций (DCGS Block l 0.2) на авиабазе ВВС Лэнгли. Пробные испытания прошли успешно и не выявили серьезных ошибок в работе программного обеспечения. По словам президента фирмы Raytheon Intelligence and Information Systems М. Кибау, «... после испытаний на авиабазе система должна была пройти государственную приемку, а первый комплект аппаратуры DCGS Block l 0.2 планировалось поставить на боевое дежурство в декабре 2005 г.». Он также отметил, что «... их фирма уже поставила в ВВС, СВ, ВМС и морскую пехоту специальное программное обеспечение интегрированного комплекса обработки информации DCGS integration backbone» [43].

За счет развертывания новой системы DCGS-AF командование ВВС увеличит возможности [43]:

- по отображению видовой, картографической, текстовой и другой информации;
- по выполнению функциональных задач:
  - обработки данных видовой, радио- и радиотехнической и специальной технической разведки;
  - распределения информации;
  - управления средствами добывания;
  - осуществления целеуказания и целераспределения;
- по формированию распределенных баз данных: фото- и видеоизображения; карты;
- по полученным данным контроля за перемещением объектов и целей и др.;
- при решении других задач:
  - обеспечения безопасности;
  - управление потоками информации;
  - полученного специального инструментария поиска информации;
  - контроля очередности выполнения запросов;
  - поддержки WEB-порталов и т.д.

По мнению командования ВВС, полностью развернутая автоматизированная система DCGS-AF должна будет обеспечить тесное взаимодействие всех органов управления объединенных сил на театре

войны, а также с аналогичными структурами национального уровня и других видов ВС [43].

4.2.3.4. Система DCGS-N

Программа разработки автоматизированной системы сбора, обработки и распределения разведывательной информации ВМС DCGS-N является неотъемлемой частью мероприятий, проводимых в рамках концепции FORCEnet и внедрения единой системы DCGS в ВС США. Аппаратно-программные средства системы планируется интегрировать в боевые информационно-управляющие системы кораблей, что обеспечит пользователям доступ к различным базам данных [43].

Основу системы DCGS-N составляет разрабатываемый по заказу ВМС США интегрированный комплекс обработки информации DIB (DCGS Integration Backbone), который позволит связать станции DCGS-N ВМС между собой, а также с аналогичными системами других видов ВС [43].

В соответствии с программой DCGS-N для ВМС разрабатываются станции трех типов [43].

Станции DCGS-N первого типа предназначены для установки на береговых ПУ и штабных кораблях управления с целью осуществления обмена информацией на театре войны. Станциями второго типа оснащаются флагманские корабли авианосных и экспедиционных ударных групп (авианосцы и универсальные десантные корабли). Станции третьего типа предназначены для обеспечения информацией отдельных кораблей, выполняющих тактические задачи [43].

Как считают американские военные специалисты, развертывание системы DCGS-N позволит не только приступить к масштабным преобразованиям системы разведки, но и перейти к новому принципу осуществления всего разведывательного обеспечения, называемого «адаптивное взаимодействие» («Reach-in»). Данный принцип касается возможности пользователей глобальной информационной сети GIG иметь доступ к информации из различных источников, в том числе от других компонентов объединенной сетецентрической среды, развернутых на ТВД или находящихся на континентальной части США [43].

Принцип Reach-in позволяет организовать взаимодействие между органами управления и аналитическими структурами (органами). По сравнению с существовавшим ранее принципом «иерархического взаимодействия» («Reach-back»), предусматривающим необходимость обращения к разведывательным органам (аналитическим цен-

трам) строго в соответствии с командной субординацией, принцип осуществления разведывательного обеспечения «адаптивное взаимодействие» предполагает возможность вхождения пользователей непосредственно в сеть для доступа к требуемым данным независимо от того, где (в какой базе данных) они хранятся [43].

Принцип «адаптивного взаимодействия» согласно руководящим документам ВС США является основополагающим для всех операций и не зависит от того, какие органы будут задействованы для обеспечения объединенных сил. Основными особенностями архитектуры (аналитических и разведывательных центров, органов управления, принятия решений и т. д.) системы разведывательного обеспечения будет снижение количества органов и центров передового развертывания, что повлечет за собой сокращение времени реагирования, а также снижение потребностей в технике и квалифицированном персонале непосредственно в зоне конфликта. По своей сути архитектура органов и центров будет представлять собой единую интерактивную систему с разветвленной сетью взаимодействия и доступа [43].

Применение принципа «адаптивного взаимодействия», а также развертывание системы DCGS-N позволят пользователям на театре войны осуществлять быстрый доступ к разнообразным базам разведывательных данных, имеющим определенную иерархию, в частности к таким, как:

- «Национальная информационная библиотека» NIL (National Information Library) Национального управления геопространственной разведки;
- «Командная информационная библиотека» CIL (Command Information Library);
- «Базы данных видовой информации» IPL (Image Product Library), размещаемые в стационарных и мобильных (на штабных кораблях, авианосцах, ПЛАРБ и др.) комплексах системы DCGS-N.

Серьезность проводимых в ВС США мероприятий не вызывает сомнений. Главными принципами этих мероприятий можно считать обеспечение реальной интеграции сил в составе группировок, применение открытой архитектуры и модульности построения современных систем и комплексов вооруженной борьбы, а также осуществление взаимодействия всех участников операции (боевых действий) как по вертикали, так и по горизонтали. Следует отметить, что недостатком разрабатываемых ранее систем разведки и доведения информации было полное отсутствие взаимодействия с другими системами [43].

4.2.3.5. Система DCGS-A

Непосредственная реализация программы разработки и развертывания системы DCGS-A, начавшаяся в 2003 г., предполагала несколько этапов. Первый этап предусматривал модернизацию стационарных центров приема, обработки и хранения разведывательной информации с целью обеспечения возможности комплексирования в них данных и усовершенствования доступа к национальным и объединенным базам данных. На втором и третьем этапах (2004-2005 г.) была достигнута оперативная и техническая совместимость средств разведывательного обеспечения пяти типов: элемента контроля и анализа системы ASAS (All-Source Analysis System), системы управления агентурной разведкой и контрразведкой, системы анализа разведывательной информации тактического звена сухопутных войск TES-A (Tactical Exploitation System - Army) и наземных элементов систем JSTARS и Guardrail Common Sensor. Это позволило представлять обстановку на ТВД на основе совместного использования данных, поступающих от них, а также осуществлять в реальном масштабе времени обмен визуальной информацией и сообщениями между операторами этих средств. В 2006 г. начался четвертый этап работ, обеспечивающий формирование единой картины динамично меняющейся обстановки на ТВД дополнительно с учетом данных от систем «Профет», топографического и метеорологического обеспечения, на основе оптимизации программного обеспечения с целью снижения избыточности поступающей информации. На пятом (заключительном) этапе DCGS-A была полностью развернута и готова к интеграции в общую для ВС США систему DCGS. Полная готовность DCGS-A – 2012 г. [318].

В сухопутных войсках США разработка варианта системы DCGS-A началась с анализа основных недостатков, стоящих на вооружении систем сбора и обработки разведывательной информации. При этом отмечались излишнее разнообразие их оборудования, большая избыточность поступающих от разнородных систем и комплексов данных, сложность, а зачастую и полная невозможность организации взаимодействия и оперативной совместимости, а также несовершенство механизма распределения обработанных сведений разведки [318].

Было решено, что система DCGS-A должна объединить функции (рис. 4.8) [318]:

- автоматизированной системы обработки и анализа развед-данных ASAS;
- наземных управляющих элементов комплекса PPTP AN/TSQ-199 Enhanced Trackwolf;
- системы РР и РЭП Prophet;
- системы PPTP Guardrail Common Sensor;
- системы радиолокационной разведки наземных целей и управления нанесением ударов JSTARS, системы топографического обеспечения Digital Topographic Support System (DTSS);
- системы метеорологического обеспечения Integrated Meteorological System (IMETS);
- системы анализа разведывательной информации тактического звена сухопутных войск TES-A и др.

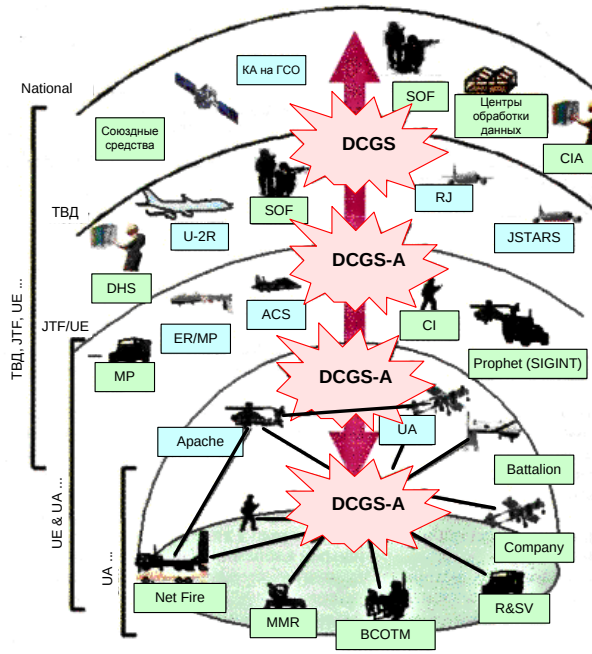


Рис. 4.8. Система DCGS-A и ее взаимодействие с DCGS

Основные усилия разработчика, американской фирмы Northrop Grumman, были направлены на создание и внедрение аппаратно-программных средств с открытой архитектурой построения, обеспечи-

вающих комплексирование сведений от всех видов разведки (видовой, радио- и радиотехнической, измерительно-сигнатурной и агентурной), унификацию архитектуры наземных средств сбора, анализа и представления данных о противнике, а также повышение степени детализации представляемой информации, качества визуальных данных и оперативности доведения разведывательной информации до потребителя. В качестве базовой системы, наиболее полно решающей задачи разведывательного обеспечения боевых действий, аппаратно-программные средства которой составляют основу DCGS-A, выбрана система ASAS [318].

В настоящее время разработаны три класса аппаратно-программных средств DCGS-A: стационарные, мобильные и встроенные.

Стационарные аппаратно-программные средства предназначены для развертывания центров приема, обработки и хранения разведывательной информации в тылу (на военных базах в континентальной части США) или при региональных командных пунктах на ТВД. В круг решаемых ими задач помимо обобщенного анализа данных и целеопределения входит круглосуточное планирование разведывательного обеспечения боевых действий сухопутных войск на всех этапах. К настоящему времени закончено развертывание 5 таких центров [318].

Мобильные комплексы необходимы для обработки и анализа разведданных, полученных от частей и подразделений передового развертывания в оперативно-тактическом звене управления. Они имеют модульную архитектуру построения с гибкой конфигурацией в зависимости от уровня решаемой задачи. Основой любого варианта развертывания является базовый комплект аппаратных средств, размещаемый на четырех многоцелевых автомобилях повышенной проходимости HMMWV или Humvee (High Mobility Multipurpose Wheeled Vehicle). В его состав входят: 16 рабочих станций (2 в каждом автомобиле и 8 удаленных), по 2 сервера баз данных и безопасности, сетевое оборудование, аппаратура связи, дизель-генератор и система кондиционирования. Рабочие станции и сетевое оборудование DCGS-A аналогичны используемым в системе ASAS. Боевой расчет такого комплекса 28 человек. В 2013 г. планировалось иметь на вооружении – 62 базовых комплекта мобильных комплексов, стоимостью 5 млн долл. каждый [318].

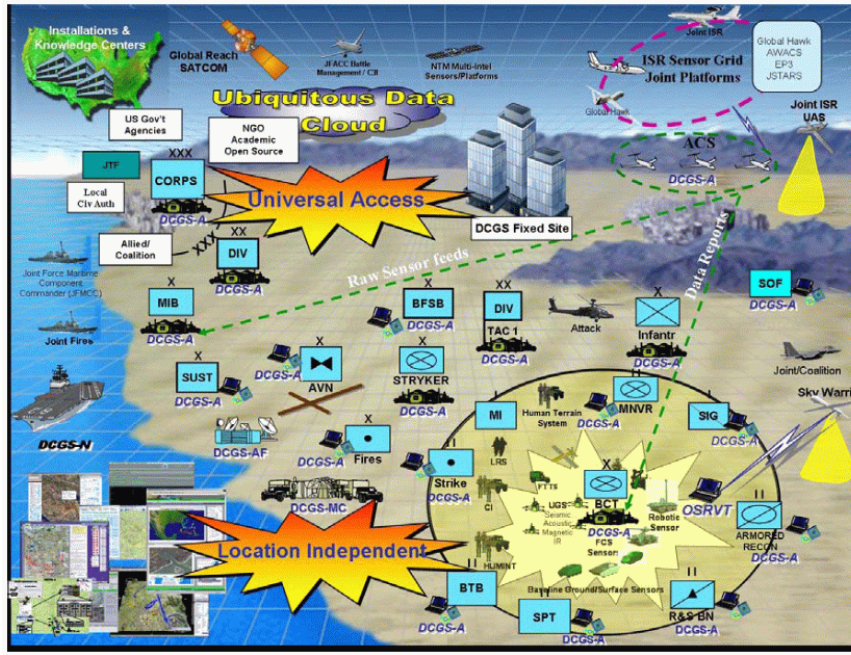


Рис. 4.9. Система DCGS-A на ТВД

Для решения задач разведывательного обеспечения в движении или до полного развертывания мобильного комплекса применяется малогабаритный носимый комплект аппаратуры, в состав которого входит АРМ ASAS-Light (на основе коммерческого переносного малогабаритного компьютера Panasonic Toughbook CF-29), универсальный тактический терминал JTT-B (Briefcase), УКВ-радиостанция AN/PSC-5 Spitfire и быстроразвертываемая турникетная антенна [318].

Встроенный вариант DCGS-A представляет собой комплект специального ПО, предназначенный для установки на бортовые ЭВМ боевых бронированных, многоцелевых дистанционно управляемых и роботизированных машин, БПЛА, средств огневой поддержки войск и разведки, разрабатываемых в рамках программы FCS, а также самолетов перспективной системы ACS (Aerial Common Sensor) и других, в первую очередь автономных, средств огневого поражения и его обеспечения [318].

Для обмена данными в пределах системы DCGS-A, а также с потребителями используется объединенная система связи и передачи разведывательной информации разведывательного сообщества JWICS

и сеть передачи засекреченной информации по интернет-протоколу SIPRNet. Доступ к этим сетям обеспечивается через мобильные станции спутниковой связи специального назначения [318].

4.2.3.6. Система ASAS

Система ASAS (All Source Analyses System) является компонентом семейства автоматизированной системы управления СВ США ABCS (Army Battle Command System) и основным компонентом DCGS-A. Она предназначена для сбора, обработки, анализа, объединения, доведения и отображения в близком к реальному масштабе времени данных о противнике, получаемых с помощью технических средств разведки [318].

Система ASAS в автоматизированном режиме позволяет решать следующие задачи [318]:

- обрабатывать развединформацию, поступающую от различных источников, в звеньях управления от армейского корпуса до батальона включительно;
- отслеживать текущую обстановку, распознавать отдельные цели и вскрывать мероприятия, проводимые противником;
- выявлять изменения в составе и дислокации группировки войск противника;
- организовывать применение сил и средств радиоразведки и РЭБ;
- обеспечивать командные пункты и штабы наиболее полными сведениями о силах противника, имеющихся в его распоряжении системах оружия и их местоположении, а также об угрозах другого характера;
- передавать обработанную информацию в формализованном виде в другие автоматизированные системы соответствующих органов управления для осуществления оперативного планирования и выдачи данных целеуказания средствам поражения;
- оценивать результаты нанесения ударов по выданным целям.

Принцип действия системы ASAS основан на применении методов автоматизированной и человеко-машинной обработки сведений, поступающих от систем и средств РРТР, измерительно-сигнатурной, воздушной видовой, радиолокационной и агентурной разведок. Информация, получаемая в масштабе времени, близком к реальному, от

разведывательных средств стратегического и оперативно-тактического уровня, а также передаваемые свыше по каналам связи оперативно-срочные донесения предварительно анализируются операторами на специализированных АРМ и в формализованном виде сохраняются в базе данных MIDB (Multi Intelligence Data Base). В дальнейшем эта информация подвергается автоматизированной обработке с целью сопоставления и выявления пространственных и временных корреляций (взаимосвязей) между отдельными разведывательными признаками, выделения характерных особенностей объектов, их идентификации путем сравнения с шаблонами, определения принадлежности и классификации целей [318].

При обработке данных в системе ASAS применяются так называемые электронные шаблоны, которые позволяют совмещать информацию от разнородных разведывательных источников, анализировать ее по заданному критерию и пропускать только достоверные разведывательные сведения. Результаты обработки сохраняются в базе MIDB и передаются для отображения и использования в другие подсистемы АСУ ABCS. Для распознавания позиций комплексов оружия противника используются типовые модели их развертывания на местности, заранее разработанные на основе разведывательных сведений видовой и агентурной разведок [318].

Система ASAS обеспечивает формирование однотипной разведывательной архитектуры на всех уровнях управления сухопутными войсками США на ТВД. Данная архитектура включает три основные группы элементов – сенсоры (датчики), средства обработки информации и средства связи, совместимые на уровне единых стандартов представления данных, протоколов обмена и процедур преобразования. Автоматизированные рабочие места обработки и анализа информации размещаются на КП в звене «армейский корпус – батальон», а также в бригадах и батальонах Р и РЭБ [318].

Опыт боевого применения ASAS в Ираке и Афганистане показал, что она позволяет значительно ускорить процесс обработки разведывательной информации. Использование данной системы позволило сократить тактические разведывательные нормативы в 2-3 раза, периодичность оценки обстановки увеличить в 2-4 раза (для дивизии – 30 мин, армейского корпуса – 60 мин, группы армий/оперативно-тактического армейского командования – 4 ч) [318].

Вместе с тем были выявлены следующие недостатки [318]:

- для работы с аппаратно-программными средствами ASAS требуется высококвалифицированный специально подготовленный персонал;
- реализованные алгоритмы установления корреляций между событиями недостаточно полно учитывают надежность источника и достоверность информации в динамике боевых действий;
- формы представления графической информации затрудняют ее передачу по каналам связи;
- отображение объектов на фоне карты местности производится только на плоскости, при этом третья координата (высота) не учитывается;
- в связи с ограниченной производительностью АРМ и каналов передачи данных требуется жесткое соблюдение дисциплины связи.

К слабым сторонам системы ASAS следует отнести также возможность радиоподавления каналов КВ- и УКВ-радиосвязи. В числе важных и уязвимых элементов системы управления, в зависимости от обстановки, могут оказаться КП и ПУ разведывательных частей и подразделений, центры, комплексы, пункты разведки и пеленгования, линии передачи информации и команд на пеленгование, самолеты и вертолеты (в том числе БПЛА) разведывательной авиации. Радиоэлектронное подавление ПУ разведывательных частей снижает эффективность их работы на 30-40%. Система имеет ограниченные возможности по обработке и слиянию информации в комплектации от КП бригады и ниже [318].

В настоящее время продолжаются НИОКР по совершенствованию ASAS и прежде всего ее подсистемы автоматизированной обработки и анализа разведывательной информации. При этом одним из основных направлений разработок является перевод программного обеспечения на использование интернет-технологий, в частности возможностей единого комплекса сетевого обслуживания NCES, а также поэтапная интеграция системы в состав перспективной системы DCGS-A. Расходы на эти цели в период с 2007 по 2013 г. составили около 3,4 млн долларов ежегодно [318].

4.2.3.7. Космические средства ведения разведки

Космические разведывательные системы используются для слежения за повседневной деятельностью и районами сосредоточения вооруженных сил потенциального противника, районами военных конфликтов, выявления и уточнения характеристик объектов критической инфраструктуры, наблюдения за их состоянием и особенностями функционирования, вскрытия фактов использования радиоэлектронных средств (РЭС) и выявления по ним местоположения войск и сил. Космические разведывательные системы являются основой информационного обеспечения для систем ВТО.

Анализ работ [237, 238, 241, 242, 244, 246, 258, 259, 260, 261, 262] показал, что в США разведка из космоса ведется следующими системами:

- системы оптико-электронной разведки (КА KH-11, TacSat-3, ORS);
- система радиолокационной разведки (КА Lacrosse);
- системы радиотехнической разведки (КА Ferret, SSU, SSU-2, SSU-3, SSU-4);
- системы радио- и радиотехнической разведки (КА типов Vortex, Mercury Magnum, Orion, Mentor, Intruder, Jumpseat-2, Jumpseat-3, TacSat-4).

Более подробно средства спутниковых систем связи США рассмотрены в подразделе 4.4.2.1. «Космические системы ведения разведки».

4.2.3.8. Наземные и воздушные средства ведения разведки

В настоящее время командованием СВ США в свете реализации концепции сетецентрической войны осуществляется активная проработка вопросов создания новых и использования существующих технических средств РРТР и РЭП в качестве наступательного информационного оружия [29].

В качестве основных компонентов РРТР и РЭП в период до 2010 г. командованием СВ рассматривались [29]:

- интегрированная система РРТР и РЭП JEWCS (Joint Electronic Warfare Core Staff);
- система комплексной высокоточной РРТР Guardrail/Common Sensors;

- система армейской многофункциональной авиационной разведки Airborne Reconnaissance Low (ARL-M);
- система воздушной разведки и целеуказания на базе тактических БПЛА RQ-6 Outrider (Outrider Tactical Unmanned Aerial Vehicle).

Система JEWCS, поступающая на вооружение СВ с 1997 г., предназначена для вскрытия и отображения радиоэлектронной обстановки в зоне ответственности дивизии с определением типа, принадлежности и месторасположения работающих РЭС противника, РЭП средств связи, выдачи целеуказания на поражение РЭС в реальном масштабе времени. В состав системы входят наземный и воздушный компоненты, которые, при необходимости, могут работать в автономном режиме [29].

Наземный компонент выполнен в двух вариантах комплексов: тяжелом – GBCS-H (Ground Based Common Sensors – Heavy) на базе боевой машины пехоты (БМП) M2 Bradley и легком GBCS-L (Ground Based Common Sensors – Light) на двух автомашинах Hummer для оснащения пехотных, воздушно-десантных и штурмовых дивизий. Воздушный компонент AQF (Advanced Quick Fix), размещенный на базе вертолета EH-60A, одинаков для всех дивизий [29].

Система обеспечивает обнаружение и высокоточное (50-100 м) определение местоположения наземных радиосредств (в КВ- и УКВ-диапазонах), РЛС полевой артиллерии, разведки поля боя и войсковой ПВО (в диапазонах 0,5-40 Ггц), а также РЭП средств связи (в УКВ диапазоне) [29].

Система Guardrail/Common Sensors предназначена для обнаружения, распознавания типов функционирующих РЛС, перехвата сообщений средств радиосвязи, высокоточного определения местоположения РЛС, радиостанций и постановщиков помех противника. В полном составе система развертывается в звене «корпус», обеспечивая круглосуточное ведение разведки. Ее тактико-технические характеристики: дальность действия 130-150 км; точность определения координат 50-150 м на дальности 100 км; диапазон разведываемых частот для РЛС 0,5-40 ГГц, для радиостанций 20-340 МГц; количество целей, разведываемых в минуту, в УКВ-диапазоне – 100, в КВ – 20-30. Разведка, как правило, ведется с высоты 3–7 км на удалении 40–100 км от линии соприкосновения или на расстоянии 10 км при радиоразведке вторых эшелонов в условиях подавления войсковой ПВО [29].

Кроме того, в СВ пока используются комплексы радиоразведки AN/TSQ-152(V) Trackwolf и AN/TSQ-199 Enhanced Trackwolf,

которые в настоящее время частично устарели и по которым в ВС США периодически поднимается вопрос о снятии их с вооружения.

Комплексы радиоразведки AN/TSQ-152(V) Trackwolf и AN/TSQ-199 Enhanced Trackwolf. На вооружении подразделений радио- и радиотехнической разведки бригад военной разведки, обеспечивающих вскрытие объектов для радиоэлектронного подавления, в настоящее время стоят комплексы РР AN/TSQ-152(V) Trackwolf и AN/TSQ-199 Enhanced Trackwolf. По мнению американских военных экспертов, в настоящее время именно эти комплексы являются самым эффективным средством добывания информации о системах управления и связи противника в интересах подготовки и проведения информационных операций на ТВД в звене выше армейского корпуса [95].

Мобильный автоматизированный комплекс AN/TSQ-152(V) Trackwolf имеет в своем составе две основные функциональные системы [95].

1. Система радиоперехвата и обработки данных: приемники анализа, управления и перехвата; аппаратуру автоматического выделения и обработки сигналов; восемь панорамных разведывательных приемников AN/TRR-36; по два комплекта аппаратуры технического анализа, регистрации и документирования AN/TSY-1 и AN/TSX-1 соответственно.
2. Система пеленгования и определения местоположения объектов: станции пеленгования и одноточечного определения мест работающих радиосредств AN/TRD-27, а также связи и измерения высоты ионосферного слоя атмосферы.

Основным достоинством комплекса является то, что благодаря использованию метода однопозиционного пеленгования SSL (Single Station Location) он позволяет определять местоположение объектов разведки из одного пункта. Аппаратура комплекса Trackwolf размещается в контейнерах, которые устанавливаются на 5-тонных грузовых машинах повышенной проходимости. Комплекс развертывается в тылу своих войск на удалении в 80-200 км от линии соприкосновения войск. Он обеспечивает обнаружение и радиоперехват сигналов радиосетей в диапазоне радиочастот 3-30 МГц, а также осуществляет определение местоположения КВ-радиостанций противника в оперативном и оперативно-стратегическом звеньях управления. Опыт использования комплекса Trackwolf, в том числе во время боевых действий, подтвердил, по мнению американского командования, его высокую эффективность [95].

Комплекс AN/TSQ-199 Enhanced Trackwolf разработан на основе выводов по использованию комплекса Trackwolf в операции «Буря в пустыне». В нем, по оценке американских военных специалистов, реализованы последние достижения в области передовых технологий, в том числе ранее не использовавшиеся наработки по программному обеспечению и конструированию переносных цифровых радиоприемных устройств в контейнерном исполнении, с открытой архитектурой построения. Предполагается, что использование этих достижений должно обеспечить комплексу более высокую оперативность развертывания, транспортабельность и адаптивность к изменению программного обеспечения в зависимости от поставленных задач. Он станет, по мнению командования сухопутных войск, одним из важных компонентов обеспечения ведения «информационной операции» на поле боя [95].

Комплекс Enhanced Trackwolf предназначен для автоматического обнаружения, перехвата и анализа радиопередач, в том числе повышенной скрытности в КВ-диапазоне, а также для высокоточного пеленгования радиопередающих средств, работающих в этом диапазоне. В полностью развернутом состоянии он включает три пространственно разнесенные автоматические станции AN/TSQ-205, которые могут функционировать как совместно, так и автономно. В комплекте станции AN/TSQ-205 имеется девять автоматизированных рабочих мест операторов: пеленгаторный пост, два поста управления и анализа, шесть постов радиоперехвата. Ее аппаратура характеризуется широким динамическим диапазоном и обеспечивает в автоматическом режиме высокоэффективное обнаружение и перехват разведываемых радиопередач (в том числе использующих сложные методы сигналопостроения и скачкообразную перестройку частоты) в диапазоне 3-30 МГц, идентификацию сигналов и определение с высокой точностью направлений на источники радиоизлучения в условиях сложной сигналопомеховой обстановки. Каждая станция обеспечивает одновременный автоматический перехват свыше 30 цифровых каналов радиосвязи и запись данных в течение более чем 120 ч [95].

Доставка оборудования комплекса Enhanced Trackwolf в районы предназначения может осуществляться военно-транспортными самолетами, а также автомобилями повышенной проходимости и другими транспортными средствами. При передислокации на новую позицию, в целях обеспечения непрерывности ведения радиоразведки, одна из станций комплекса, оставаясь на прежнем месте, используется для мониторинга перехватываемых радиосетей, а две другие достав-

ляются на новое место развертывания. После начала их функционирования осуществляется перебазирование оставшейся станции на новую позицию. При этом развертывание и свертывание комплекса производится менее чем за 4 ч. По взглядам американских экспертов, поступление AN/TSQ-199 на вооружение разведывательных подразделений сухопутных войск позволяет значительно повысить их возможности по контролю за электромагнитным спектром и функционированием ключевых узлов в системах управления противника [95].

В целом командование сухопутными войсками США рассматривает комплексы Enhanced Trackwolf и Trackwolf как основные средства радиоразведки, которые позволят вести эффективную борьбу с системами управления противника на поле боя. Предполагается, что их использование внесет ощутимый вклад в достижение декларируемых американским военно-политическим руководством целей добиться установления полного контроля за функционированием информационных структур противника, обеспечивающих процессы принятия решений и оказывающих противодействие системам управления вооруженных сил США [95].

Система армейской многофункциональной разведки ARL-M на базе самолетов армейской авиации RC-7B предназначена для ведения круглосуточной видовой, оптоэлектронной, радио- и радиотехнической разведки с малых высот в районах низкой интенсивности боевых действий. Она обеспечивает вскрытие дислокации войск, отдельно действующих его подразделений, засад, укрытий снайперов и других замаскированных объектов, а также обнаружение средств радиосвязи и постановщиков радиопомех противника, определение их местонахождения [29].

В полном составе система включает 3 самолета-разведчика RC-7B и наземный мобильный центр обработки информации. В состав оборудования самолета входят: оптоэлектронная камера дневной съемки, ИК-станции переднего и нижнего обзора, РЛС с синтезированной апертурой антенны и автоматической селекцией движущихся целей, станции радиоразведки и пеленгования в УКВ- и КВ- диапазонах. Разведка ведется с малых высот на безопасном удалении от линии соприкосновения войск. Данные разведки передаются на наземный центр [29].

Система воздушной разведки и целеуказания на базе тактических БПЛА Outrider предназначена для круглосуточного всепогодного наблюдения, поиска и обеспечения целеуказания по объектам

противника на поле боя в реальном масштабе времени в интересах дивизий, бригад и отдельных батальонов СВ [29].

В качестве полезной нагрузки используются съемные комплекты аппаратуры радиотехнической, радиолокационной и оптоэлектронной разведки, а также бортовая аппаратура передачи данных и управления полетом.

Разведывательное оборудование включает [29]:

- ИК-станцию переднего обзора (3-5 мкм), размещаемую на подфюзеляжной стабилизированной платформе;
- лазерный дальномер-целеуказатель (дальность действия не менее 10 км);
- РЛС с синтезированной апертурой антенны (дальность действия до 7 км при высоте полета 3600 м);
- тепловизионную станцию;
- станцию радиотехнической разведки (0,5-18 ГГц).

Аппаратура передачи данных работает в диапазоне 3,9-6,2 ГГц и может обеспечивать ретрансляцию сообщений на дальности до 200 км.

Предусматривается, что система будет развертываться на удалении до 60 км от линии соприкосновения. Полет будет осуществляться на заранее введенной программе, которая может изменяться в процессе полета. Радиус полета БПЛА обеспечит ведение видовой и радиотехнической разведки в пределах 200 км за линией фронта с точностью определения местоположения объектов не менее 100 м [29, 9].

В августе 2012 г. специалисты компании Boeing впервые продемонстрировали работу системы расширенного управления БПЛА, выполненную по технологии SWARM (Swarming), позволяющую управлять «роем» или «стаей» роботизированных боевых единиц. В ходе испытаний два БПЛА ScanEagle компании Boeing и БПЛА компании Procerus Unicorn совершили совместный полет, самостоятельно обмениваясь данными, необходимыми для выполнения миссии. При этом БПЛА совместно сканировали местность, составляли карту полета и отправляли данные в пункт управления. Полетом группы БПЛА, действующей автономно, управлял один оператор при помощи ноутбука и военной радиостанции [29, 65].

4.2.4. Системы управления и поддержки принятия решений

4.2.4.1. Общие тенденции развития систем управления и поддержки принятия решений

Планируется, что в ближайшее время ВС ведущих технически развитых стран получат в распоряжение интегрированную архитектуру принятия решений, базирующуюся на искусственном интеллекте, нанотехнологиях, эффективной обработке больших массивов информации, многофункциональных процессорах со способностью поддерживать принятие решений в реальном масштабе времени, технологиях сжатия данных для повышения скорости обработки. При этом использование командованием информационных систем с элементами искусственного интеллекта как множителей эффективности боевых действий окажет влияние на доктрину, организацию и обучение вооруженных сил. В частности, моделирующие установки позволят в интегрированном и интерактивном режимах прогнозировать варианты действий, менять их тактику, принимать решения и действовать [16].

По оценке западных военных экспертов, в сетецентрических войнах с участием объединенных вооруженных сил будут широко использоваться системы дистанционно управляемого и самонаводящегося (обладающего искусственным интеллектом) высокоточного оружия в сочетании с элементами глобальной информационной войны. В связи с этим актуализируются исследования, направленные на повышение эффективности применения объединенных сил за счет внедрения перспективных информационных технологий в процессы оценки обстановки и принятия решений, оперативного планирования, а также управления войсками и оружием в операциях различного характера и масштаба [206].

Одним из основных подходов к использованию новых технологических достижений в интересах управления войсками и оружием является концепция единого информационного пространства. Она предполагает создание глобальной информационной сетецентрической среды, обеспечивающей комплексную обработку в реальном масштабе времени сведений о противнике, своих войсках и окружающей местности в интересах поддержки принятия решений по созданию группировок войск (сил) оптимального (для достижения поставленных целей) состава и их эффективного применения в различных условиях обста-

новки. Реализация концепции единого информационного пространства должна коренным образом изменить подход к организации оперативного планирования и управления войсками (оружием) в ходе повседневной деятельности и во время военных действий [206].

Наличие сетецентрической среды должно обеспечить эффективное взаимодействие всех участвующих в операции органов управления и войск (сил), которые условно можно разделить на три основные группы элементов [206]:

- добывающие элементы (силы и средства разведки);
- информационно-управляющие элементы;
- исполнительные элементы (системы оружия и воинские подразделения объединенных сил).

Информационно-управляющие элементы в сетецентрической среде представляют собой органы и пункты управления, автоматизированные системы управления и связи, обеспечивающие их функционирование, а также территориально распределенные базы данных оперативной, разведывательной и другой необходимой информации (топогеодезической, геопространственной, фоноцелевой, гидрометеорологической и т. п.), предоставляемой пользователям в реальном масштабе времени.

Определять общее количество и соотношение этих разнородных элементов предполагается с использованием математической модели конкретной операции по отработанным методикам оптимизации их структуры. Это позволит с учетом представления органов управления и войск (сил) в данной модели в виде элементов территориально-распределенной вычислительной сети свести процесс оперативного планирования и управления объединенных сил к известной задаче оптимизации структуры элементов сети, каждый из которых представляет собой реальное воинское формирование/систему оружия, и порядка их применения в интересах достижения целей операции [206].

Для реализации сетецентрической системы управления предполагается сформировать интегрированную информационно-сетевую инфраструктуру, коммуникационный компонент которой будет формироваться на базе глобальной информационной решетки – GIG, а основу информационного компонента составят территориально распределенные базы данных разнородной информации, объединенные в единое информационное пространство с использованием протокола IP v.6 [206].

Таким образом, сетецентрическая система управления будет включать автоматизированные системы управления и базы данных

командно-распорядительной (боевого управления), оперативной (о составе, состоянии, положении своих войск (сил) и условиях обстановки), разведывательной (о противнике), геопространственной (о характере земной поверхности и морских акваторий), фоноцелевой (о состоянии и расположении объектов/целей и их контрастных характеристиках), гидрометеорологической и другой необходимой информации, доступной каждому пользователю в объеме, определяемом его задачами и правами доступа к сведениям [206].

Интегрированная из коммуникационных сетей и сетей датчиков, программного обеспечения и организационных структур сетецентрическая система управления обеспечит [2, 121, 127]:

- сбор информации от разнородных средств разведки в интересах ее последующего комплексирования;
- высокопроизводительную обработку в реальном масштабе времени информации, описывающей общую картину ситуации, складывающейся на ТВД;
- ведение каталогов баз данных, относящихся к зоне операции и способностям противника, а также доступ к этим базам лиц, принимающих решения, всех уровней военного управления;
- создание единого информационного пространства для информационного обмена участниками операций и доступа к информационным услугам, основанного на устойчивых и высокоскоростных средствах связи и телекоммуникациях;
- оперативное доведение информации (в масштабе, близком к реальному времени) о ходе проведения операций, точные и своевременные разведывательные данные о местоположении и действиях как противника, так и своих войск;
- способность одновременного проведения взаимоувязанного комплекса операций на всем ТВД, выполняемых непрерывно с рассредоточенных основных мест применения сил и средств;
- встроенные способности самозащиты и противодействия подсистем информационной системы воздействию широкого спектра средств противника (в том числе воздействиям в информационном пространстве).

Формирование единой сетецентрической системы управления потребует принципиально новых технологических, алгоритмических и системных решений в области управления.

В основе сетецентрического управления лежит требование полноты и сверхоперативности информации о текущем состоянии всего многофакторного пространства угроз и собственных сил и средств. Успех определяется не только возможностями точечных воздействий отдельными видами оружия, но и превосходящими возможностями по управлению сложнейшими процессами многоходового многофакторного противоборства [162].

Задача сетецентрического управления – сверхоперативный сбор многоканальной информации, формирование в реальном масштабе времени динамической интегральной информационной картины событий, обеспечение требуемых темпов выработки и исполнения алгоритмов, организационных мероприятий согласованного и эффективного управления комплексным противоборством [162].

Необходимое условие достижения превосходства сетецентрического управления – переход к сетевым архитектурам и аппаратным средствам с качественно новым уровнем универсального системно-сетевого интеллектуального управления распределенными процессами управления. Применительно ко всем реализуемым посредством сетецентрической среды задачам такое управление на системном уровне единообразно обеспечит [123, 162]:

- устранение первопричин непрерывного воспроизводства разнородной компьютерной информации, которая является причиной комбинаторной сложности, что препятствует интеграции глобально распределенных данных, программ, процессов и систем (интегральная системная сложность компьютерной среды перестает существенным образом зависеть от своего размера);
- глобальное распространение свойства универсальной программируемости структурно-сложных распределенных вычислений на любую совокупность компьютеров, связанных сетями;
- свободную масштабируемость и конфигурируемость вычислительных сред в сетевых ресурсах;
- организацию надежных вычислений и процессов управления в ненадежных вычислительных средах, например в условиях деструктивного внешнего воздействия.

Сетецентрическое управление реализуется встраиваемыми компьютерами, связанными сетями, посредством которых в ходе управления поведением объектов бесшовно реализуются информационные и алгоритмические взаимодействия. Важнейшим компонентом

в таких системах являются бортовые системы сетецентрического управления, которыми оснащаются все объекты, функционирующие в едином алгоритмическом пространстве распределенных вычислений и сетецентрического управления. При этом желательно на аппаратном уровне (без использования операционных систем или других промежуточных системно-программных слоев) достигнуть полной совместимости всех подсистем сетецентрического управления [162, 345].

Основу сетецентрического управления составляют сквозные модели систем объектов, взаимодействующих в едином информационном пространстве, в котором в реальном времени и с высокой надежностью обеспечивается циклическое повторение всех этапов исполнения контуров управления различных уровней, таких как [162, 345]:

- многоканальный сбор, первичная обработка и накопление разноплановой фрагментарной информации, поступающей с различных компонентов системы, отражающих состояние внешней среды и их текущее внутреннее состояние;
- формирование посредством глубокой компьютерной переработки собираемой и накапливаемой информации целостной картины из информационных фрагментов, которая определяет текущее состояние системы целом и ее частей и является основой для выработки управляющих воздействий;
- выработка и доставка управляющих воздействий, структурированных при формировании общей модели таким образом, что управляющая информация каждого такого канала воздействия выстроена в соответствии с «компетенцией» и уровнем доступа соответствующего управляемого компонента.

Основой технических средств сетецентрического управления должна стать системно- и структурно-целостная, универсально-программируемая вычислительная среда, включающая локальные и глобальные компьютерно-сетевые средства как единое целое, которая обладает встроенным системным интеллектом и сквозными технологиями бесшовного программирования, направленными на поддержку комплексных решений задач [162]:

- формирования концепций, моделей и алгоритмов управления;
- моделирования развития конфликтов, сценариев, ситуаций;

- проектирования нужного направления развития противоборства;
- реализации вычислительных информационно-управляющих сред (в том числе конфигурирование, программирование, интеграция, модернизация);
- управления эксплуатацией и применением средств;
- управления силами на различных уровнях управления;
- реализации систем поддержки принятия решений и боевых экспертных систем на основе технологий искусственного интеллекта.

Ограниченность системных возможностей современных вычислительных систем и сетей связана с исчерпанием системообразующих возможностей классических микропроцессорных архитектур. Они изначально ориентированы на последовательные вычисления и поэтому не имеют архитектурных возможностей эффективной поддержки бесшовно программируемых распределенных и параллельных вычислений в совокупных сетевых ресурсах, без которых невозможно полномасштабное и эффективное решение всего многообразия задач сетецентрического управления [162].

В связи с этим актуальным является формирование универсального алгоритмического пространства распределенных вычислений и сетецентрического управления по принципу «все влияет на все и сразу», которое способно охватить совокупные сетевые и вычислительные ресурсы всех видов вооруженных сил. В этом случае открываются возможности оперативного реконфигурирования, а также перепрограммирования и онлайн исполнения любых моделей сетецентрических систем, обеспечивающих высокодинамичное управление всей совокупностью боевых действий в сильносвязном информационно-алгоритмическом пространстве. При этом в среднесрочной и долгосрочной перспективе такое пространство может быть распространено (при ограниченных затратах средств и времени) на все виды вооружений и процессы непрерывного ресурсообеспечения этих действий (как в случае тотальных, так и в случае множественных локальных угроз и воздействий) [121, 123, 162].

В настоящее время в США и в странах НАТО принято разделять системы управления на несколько классов в зависимости от выполняемых функций – Command (командование, управление), Control (контроль), Communication (передача информации), Computers (вычисления, расчеты), Intelligence (знание), Surveillance (наблюдение), Reconnaissance (разведка).

Системы класса «С4» помимо выполнения функций, реализованных в системах класса «С2» и «С3», должны решать следующие задачи [342]:

- полной автоматизации методов сбора и обработки информации;
- информационной поддержки выработки командиром вариантов решения по принципу «набросок – в решение»;
- математического моделирования результатов боевых действий по избранным вариантам выполнения боевых задач с графическим отображением их смоделированного хода и результатов на электронных картах, в том числе с использованием средств 3D отображения поля боя;
- информационной поддержки разработки планирующих документов по принципу «набросок – в план», осуществляющей преобразование графических и аудиоматериалов в планирующие документы;
- информационной поддержки принятия частных решений в ходе выполнения боевой задачи, осуществляющей обновление оценок и выводов на основе информации, полученной в ходе операции.

Таким образом, принципиальное отличие систем класса «С4» от класса «С2» заключается в более высокой степени автоматизации информационных и управленческих задач.

Даже в ВС наиболее развитых в промышленном отношении стран все системы класса «С4I» и «С4SR» по своей принадлежности к уровню военного управления относятся только к системам управления оперативного или оперативно-стратегического звена [342].

В настоящее время все имеющиеся на вооружении иностранных государств АСУ тактического звена относятся к классу «С2» или «С2+» и различаются между собой лишь незначительным расширением спектра решаемых задач. При этом все системы тактического назначения принципиально «не дотягивают» даже до класса «С3» [29, 342].

По мнению экспертов, основными препятствиями на пути развития АСУВ тактического звена из класса «С2» в классы «С3» и «С4» являются [342]:

- отсутствие математически корректных алгоритмов оценки действий войск на тактическом уровне ввиду огромного разнообразия применяемых ими способов и приемов выполнения боевых задач;

- сложность создания автоматизированной системы сбора и оценки данных тактической обстановки ввиду разнообразия ее параметров и скоротечности изменений (по сравнению с оперативным звеном управления);
- возникающая в связи предыдущим пунктом необходимость ручной работы по сбору, обработке и отображению большого количества переменных данных, превышающая возможности ответственных должностных лиц по вводу таких данных в систему;
- необходимость обработки относительно большого количества данных в единицу времени, которые по своим объемам в настоящее время превышают возможности машинного обеспечения, используемого в тактическом звене управления;
- сложность создания самоорганизующихся сетей связи и надежных локальных сетей (систем передачи данных) между большим количеством высокомобильных объектов управления.

В связи с этим актуальной задачей развития систем управления является наращивание информационных возможностей систем управления оперативного и оперативно-стратегического звена, а также реализация систем управления класса «С3» и «С4» в тактическом звене управления.

Рассмотрим основные технологические решения и тенденции в области создания системы сетецентрического управления на примере АСУВ армии США.

4.2.4.2. Системы управления ВС США стратегического уровня

Центральной системой управления войсками является глобальная система оперативного управления GCCS (Global Command and Control System). Ее оборудование обеспечивает связь высшего военно-политического руководства и объединенного штаба Комитета начальников штабов ВС США со штабами видов ВС, управлениями центрального подчинения МО США, объединенными командованиями в зонах ответственности и функциональными командованиями, а также с командующими объединенными оперативными формированиями. Согласованно с ней создается глобальная система управления тылом GCSS (Global Combat Support System) [29].

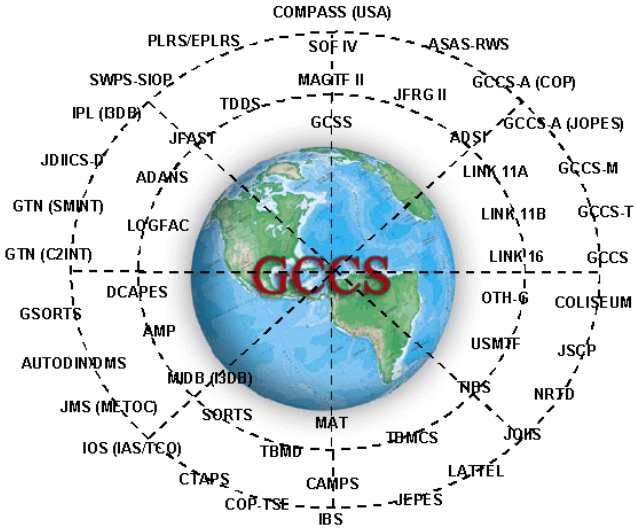


Рис. 4.10. Структура системы GCCS,
объединяющей разнородные АСУ и СС

Видовыми компонентами GCCS являются глобальные системы [29]:

- GCCS-Army – для управления СВ;
- GCCS-Maritime – для управления ВМС;
- TBMCS (Theater Battle Management Core System) – опорная АСУ ВВС в зоне военных операций, а в перспективе – интегрированная АСУ ВВС JC2S (Joint Command and Control System).

Система GCCS официально введена в эксплуатацию в августе 1996 г. Она позволяет автоматизировать процессы предупреждения о нападении, контролировать приведение ВС в боевую готовность, планировать и руководить боевыми действиями, предоставлять командованию оперативно-тактическую информацию, а также организовывать тыловое обеспечение [29].

В то же время глобальная система управления GCCS совершенствуется для СВ по программе Enterprise, для ВВС – Horizont, а для ВМС – Copernic. Например, завершение программы Enterprise позволит решать следующие задачи: обнаруживать, распознавать и сопровождать несколько тысяч воздушных и наземных целей; автоматически наводить управляемое оружие на сотни целей; обеспечивать ко-

мандиров всех уровней электронными картами текущей обстановки; управлять подчиненными подразделениями и осуществлять автоматизированную подготовку вариантов возможных действий войск в пределах ТВД. Таким образом, планируется, что армия США получит к 2020 г. новую систему управления ВС, которая интегрирует все АСУ. Она будет обеспечивать осуществление связи на всех уровнях управления, а также автоматизацию процесса принятия решений командирами всех уровней [29, 50].

Перспективное строительство системы управления ВС США нацелено на придание ей свойств глобальной автоматизированной разведывательно-ударной системы JC2 (Joint Command and Control – Объединенная система командования и управления). Она обеспечивает вертикальное и горизонтальное взаимодействие органов управления войсками и оружием всех уровней, а также других органов государственного управления на основе глобальной информационно-управляющей решетки МО США GIG. При этом JC2 и GIG будут сетецентрическими системами, представляющими собой единое интегрированное информационное пространство, функционирующее в реальном масштабе времени или близком к нему. США планирует завершить создание этой глобальной информационно-управляющей системы к 2020 г. [2, 29].

4.2.4.3. Системы управления ВС США оперативно-тактического уровня

В сухопутных войсках осуществляется первоначальный этап реализации концепции сетецентрических войн. Он связан с выполнением ряда программ, к наиболее перспективным из которых командование СВ США относит следующие [29]:

- Army Battle Command System (ABCS);
- Force XXI Battle Command, Brigade-and-Below (FBCB2);
- Army Airborne Command and Control System (A2C2S).

Первые две программы предусматривают совершенствование существующей системы боевого управления СВ в звене «корпус – дивизия – бригада» (ABCS) и создание перспективной архитектуры системы управления высокомобильными формированиями СВ дивизионного и бригадного звеньев OFBCS (Objective Force Battle Command System) [29].

Программой A2C2S предусматривается разработка и принятие на вооружение тактических воздушных командных пунктов, создавае-

мых на базе вертолета UH-60L Black Hawk для организации управления в звене «дивизия – бригада». Всего на вооружение СВ США планируется поставить свыше 100 таких командных пунктов [1, 29].

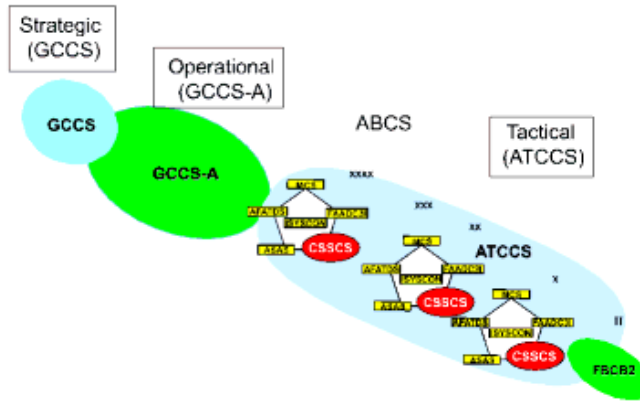


Рис. 4.11. Структура систем управления в СВ ВС США

Для успешного внедрения и использования АСУ в войсках штабов СВ США был разработан документ «Армейская перспектива – 2010», в котором основные оперативно-стратегические концепции, содержащиеся в доктрине Комитета начальников штабов «Единая перспектива – 2010», рассмотрены применительно к СВ. В нем были сформулированы шесть требований, отражающих видение командованием СВ США процесса планирования использования последних достижений в области современных технологий для усиления своей роли в будущих межвидовых операциях [29]:

- достижение информационного превосходства;
- проецирование силы (способность быстро осуществлять проецирование своей огневой и ударной мощи в любом регионе мира);
- защита войск (наиболее важным, как считают американские специалисты, является скрытие и рассредоточение наиболее уязвимых элементов АСУ);
- формирование благоприятных условий на поле боя (создание необходимых условий для достижения успеха за счет снижения возможностей противника по ведению согласованных действий еще до начала операции);
- ведение решительных боевых действий (массированное, непрерывное и длительное воздействие на противника с

различных направлений всеми силами и средствами вооруженной борьбы с обязательным использованием методов информационного противоборства).

В СВ введена в эксплуатацию АСУ армейского корпуса ATCCS (Army Tactical Command and Control System), оборудование которой развертывается от корпусного до батальонного центров управления. Ее главными компонентами являются:

- АСУ войсками корпуса MCS (Maneuver Control System);
- АСУ полевой артиллерии AFATDS (Advanced Field Artillery Tactical Data System);
- АСУ войсковой ПВО FAADS (Forward Area Air Defense System);
- АСУ разведки и РЭБ ASAS (All Source Analysis System);
- АСУ тылом GSSCS (Combat Service Support Control System);
- АСУ уровня бригады и ниже FBCB2 (Force XXI Battle Command, Brigade and Below).

АСУ MCS представляет собой главную АСУ корпуса. Через нее ведется основной обмен информацией с АСУ GCCS-Army.

АСУ AFATDS является полностью интегрированной системой управления, осуществляющей планирование, координацию, боевое управление ведением огня при ближней огневой поддержке, подавление артиллерии противника, огневых средств ПВО и др. Она обеспечивает выполнение всех оперативных функций огневой поддержки, включая автоматизированное целеуказание на основе анализа важности объектов удара. АСУ будет развертываться от огневых взводов до корпуса, передавать данные в единую базу данных ABCS, взаимодействовать с АСУ и системами оружия других видов ВС [29].

АСУ ПВО FAADS интегрирует огневые подразделения ПВО, информационные средства и пункты управления в единую систему, способную противостоять воздушным угрозам (БПЛА, вертолетам, самолетам, крылатым ракетам и др.). Кроме того, АСУ обеспечивает автоматизированное управление подразделениями войсковой ПВО [29].

Современная мобильная АСУ разведки и РЭБ ASAS развертывается в звене от батальона и выше до корпуса [29, 40].

В рамках перехода к сетецентрическому управлению на дивизионном уровне СВ США принято на вооружение АСУ в виде командного пункта будущего, внедряемого в настоящее время. Она первоначально была разработана как демонстрационный образец по пер-

спективным технологиям для 1-й механизированной дивизии СВ в Ираке и соединила надежной системой обмена информацией штаб дивизии и все пять бригад. Основу функционирования командного пункта будущего составляет АСУ, обеспечивающая визуализацию, информационный анализ и координацию совместной деятельности в унифицированной интегрированной среде, которая в целом оказывает помощь командирам и оперативным офицерам в анализе информации, обмене мнениями и выработке способов и порядка совместных действий. АСУ командного пункта будущего производит синтез данных реального масштаба времени или близкого к нему, поступающих от множества функционально-управленческих программных приложений [29].

Это позволяет обеспечить возможность организовать непрерывный мониторинг ситуации в боевом пространстве с отслеживаем местоположения элементов боевого порядка своих сил и сил соседей на электронных картах или на фоне снимков района боевых действий, полученных со спутников или БПЛА, а также оценивать силы противника и характер их намерений на основе разведданных, получаемых от различных источников [29, 45].

4.2.4.4. Системы управления ВС США тактического уровня

С середины 1990-х в ВС США реализовывалась амбициозная программа «Боевые системы будущего» FCS (Future Combat System). Она подразумевала максимальное использование самых современных информационных и военных технологий с тем, чтобы завлечь вероятного противника в сетецентрическую войну, в которой у противоборствующей стороны не остается никаких шансов на успех. Новая концепция должна была произвести революцию в тактике ведения наземных операций [29, 342].

Программа FCS определила архитектуры перспективных глобально распределенных систем сетецентрического (в едином информационном пространстве компьютерных сетей) управления боевыми единицами, их группами, системами и средствами обеспечения. Она представляет собой многоуровневую систему сетецентрической интеграции стационарных и мобильных объектов разного назначения, оснащенных встроенным компьютерным интеллектом, в едином информационно-функциональном пространстве управления с их взаимодействием в реальном масштабе времени [162].

Целью программы FCS являлась разработка такого комплекса, который достигнет оптимального баланса между показателями решающих тактико-технических характеристик, включающих [29, 342]:

- единые транспортные и бронеплатформы;
- автономные робототехнические системы;
- функциональные возможности командования и мобильных объектов управления оснащенных ЭВМ, объединенных в сеть управления, связи, соответствующие классу С4;
- возможность наблюдения, разведки, обнаружения и наведения в автоматизированном режиме для всех элементов (объектов управления) системы;
- возможность высокоточной стрельбы прямой и непрямой наводкой для всех средств поражения, объединенных со средствами разведки и управления в единую сеть.

Программа FCS состояла из 18 компонентов и двух отдельных подсистем. Эти две подсистемы – солдаты и средства связи. Остальные 18 компонентов разделены на четыре подгруппы: наземные машины с экипажем, беспилотные летательные аппараты, автоматические системы (отдельные устройства) и наземные дистанционно управляемые машины (рис. 4.12).

Рис. 4.12. Структура комплекса FCS

При этом ключевым системообразующим элементом программы FCS являлись средства связи и компьютерные сети, обеспечивающие поддержание функционально интегрированного информационного поля над зонами боевых действий посредством построения надежной работы мобильных беспроводных сетей. Автономные элементы должны были быть подключены к общей сети и обмениваются информацией в режиме Peer-to-Peer (P2P). Так, участники в реальном масштабе времени могли обеспечиваться данными о местоположении противника, поступающими с отдаленных автоматических датчиков, разведывательных машин, беспилотных аппаратов и т.п. [162].

Планировалось, что подразделение, оснащенное системой FCS, будет иметь возможность приспосабливаться к изменяющемуся объему задач и будет способно обеспечить [23, 29]:

- применение мобильных, объединенных в сеть средств, выполняющих функции Command, Control, Communication и Computers (командование, контроль, передача информации и расчеты);
- управление автономными робототехническими системами;
- высокоточную стрельбу прямой и непрямой наводкой;
- использование платформ бортовых и наземных штатных датчиков;
- наблюдение, разведку, обнаружение и наведение.

Для работы сетевой системы FCS солдаты и платформы должны были оснащаться специальным комплектом оборудования, пользовательскими устройствами с навигационной системой. Специальные комплекты, которые получили обозначение B-kit, включали в себя тактическую радиостанцию JTRS GMR (Joint Tactical Radio System's Ground Mobile Radio), компьютер и сетевое оборудование. Программой FCS также предусматривалась установка комплектов B-kit на имеющиеся боевые машины пехоты Bradley, танки Abrams и бронеавтомобили HMMWV. Автономная навигационная система ANS (Autonomous Navigation Systems) включает следующие компоненты [29, 57]:

- LIPM (LADAR Imaging Perception Module);
- IPM (Imaging Perception Module);
- MMWR (Millimeter Wave RADAR);
- GPS/INS и компьютерную систему ACS (ANS Computer System).

Однако полностью решить все задачи при создании FCS не удалось. Все ее элементы были отработаны достаточно слабо, что связано с высокой сложностью и масштабностью поставленных задач, а

также со значительным сокращением военного бюджета США. В результате, в мае 2011 г. в прессе появились официальные сообщения о закрытии программы FCS [342].

Вместе с тем США не отказались от совершенствования своих технологий в сфере автоматизации управления военными формированиями тактического звена. Часть наработок, в частности в области применения беспилотных летательных аппаратов и средств передачи информации, была передана в другие программы.

В настоящее время наиболее известной из всех существующих АСУВ тактического звена является американская система класса C2SR – FBCB2 (Force XXI Battle Command Brigade and Below). По программе разработки FBCB2, которая велась с 1990-х гг. параллельно с программой FCS, предполагалось создать надежно функционирующую систему класса «С2», которая объединяла бы не «перспективные боевые платформы» (которые в 1990-х еще находились в стадии эскизных проектов), а уже имеющиеся в войсках средства ведения боевых действий, и в разы повысить их боевую эффективность за счет сокращения цикла боевого управления и повышения ситуационной осведомленности [342].

Серийное производство FBCB2 было налажено с 2002 г. В 2003 г. система была опробована в боевых условиях в Ираке в составе 4 механизированной дивизии. С октября 2008 г. начато внедрение прошедшей модернизацию пятой версии (v. 1.5) программного обеспечения FBCB2. По плану до конца 2011 г. аппаратно-программными комплексами системы FBCB2 должны были быть оборудованы каждый танк, БМП, самоходная артиллерийская установка и все командирские автомобили бригад сухопутных войск (армии) США, а также корпуса морской пехоты (всего более 100 000 комплектов). В 2015 г. планировалось оснастить носимыми комплексами системы каждого солдата специализированных боевых подразделений [2, 29, 342].

Система FBCB-2 является ключевой компонентой АСУ СВ США ABCS [343].

Система FBCB2 является совокупностью взаимодействующих программных и аппаратных средств, разработанных, в первую очередь, для обеспечения ситуационной осведомленности подразделений, экипажей бронетанковой техники, машин, отдельных солдат и передачи информации командирам боевых и обеспечивающих подразделений [29].

Наличие в общевойсковых соединениях довольно совершенной АСУ огнем артиллерии, а также оснащение образцов вооружения

элементами интегрированной бортовой информационно-управляющей систем подобно той, что устанавливается на танках Abrams M1A2 SEP, уже сейчас дает возможность автоматизированного командного управления боевыми машинами и подразделениями. Это в значительной степени может обеспечить переход формирований СВ США к ведению сетецентрических действий [29].

Аппаратно-программные комплексы FBCB2 выпускаются в двух вариантах. Основной – техническое обеспечение на базе компьютера AN/UYK 128 Applique с сенсорными экранами (500 МГц / 4 Гбайт / Windows 95/NT в особо прочном корпусе), связанного с приемником NAVSTAR и цифровой радиостанцией, и программное обеспечение боевого управления. Взаимодействие AN/UYK-128 с компонентами FBCB2 осуществляется по протоколу TCP/IP [29, 342].

Второй – чисто программная версия для встроенных в системы оружия устройств обработки информации. Оборудование FBCB2 стыкуется с другими бортовыми устройствами системами боевой машины (в том числе с лазерным дальномером) для взаимного опознавания, автоматического формирования сообщений о целях противника и вызова огня [29, 342].

Весь аппаратно-программный комплекс FBCB2 стыкуется с различными средствами передачи данных (средствами связи различного диапазона). Обмен данными в «Тактическом Интернете» производится с использованием систем радиосвязи EPLRS и SINGARS и системы подвижной спутниковой связи INMARSAT L-диапазона. Комплекты FBCB2 являются едиными для всех уровней управления «бригада-отделение (танк)» и могут быть смонтированы (развернуты) на полевых пунктах управления бригады (здание, палатка, заглубленный или защищенный пункт управления), на любом транспортном средстве типа автомобиль, на бронеобъекте (танк, БМП, БРМ, БТР), а также на вертолете [29, 342].

АСУ FBCB-2 обеспечивает выполнение следующих задач [343]:

- предоставления постоянно обновляемой информации о боевой обстановке, состоянии и действии своих войск и сил противника, фильтруемой по звену управления, эшелону и местоположению абонента;
- определения географического положения абонента (если тот находится в воздухе, то определяется также и высота полета);

- отображения на экране монитора карты тактической обстановки;
- составления и распространения в автоматизированном режиме в электронном формате формализованных сообщений и подтверждений о получении сообщений, приказов и распоряжений, заявок на огневую поддержку, целеуказаний и приказов на ведение огня, сигналов-предупреждений, оперативных докладов;
- формирования и наложения на электронную карту боевой обстановки элементов рельефа местности, препятствий, данных разведки, оперативных нормативов, геометрических данных, схем-приложений к боевым приказам;
- обмена между компонентами АСУ FBCB-2 и другими элементами АСУ ABCS в полуавтоматическом режиме выделенными данными, имеющими критическое значение для выполнения боевой задачи.

Функционирование АСУ FBCB-2 невозможно без системы связи тактического звена управления «Тактический Интернет». Совместно они формируют единую информационно-командную систему, компоненты которой тесно взаимодействуют друг с другом. Реализация проекта FBCB2 требует и модернизации систем связи. Так, в частности, предполагается модернизировать систему «Тактический Интернет», которая обеспечивает необходимые сетевые возможности в звене «дивизия – бригада». Она также обеспечивает относительно высокую интенсивность информационного обмена и взаимодействия между автоматизированными системами управления MCS – ASAS – FAADS – AFATDS – GSSCS [29, 343].

Для пересылки и приема информации FBCB-2 использует переменный формат текстовых сообщений VMF (Variable Message Format) вне зависимости от принадлежности получателя – отправителя. Формат VMF утвержден в настоящее время в качестве основного для передачи текстовых сообщений в системе электронной почты АСУ ABCS [343].

Данные в сетях связи FBCB-2 передаются по стеку протоколов TCP/IP, адаптированному в соответствии с требованиями и условиями функционирования сетей радиосвязи в тактическом звене управления. В пределах КП бригады и батальона все средства связи и средства АСУ соединены между собой ЛВС. Машины КП соединяются между собой и с районным УС системы Enhanced MSE волоконно-оптической линией связи с пропускной способностью 100 Мбит/с.

Районная вычислительная сеть, охватывающая КП бригады и батальонов, строится на основе радиостанций NTDR и терминалов связи JNN. Кроме того, радиостанции NTDR обеспечивают резервные каналы связи для звена управления «бригада и выше» [343].

В системе FBCB-2 использована система идентификации «свой-чужой» BFT, которая использует существующие национальные средства космической инфраструктуры и национальные технические средства контроля National technical means (NTM). Эти устройства дают возможность командирам отслеживать и получать информацию о местоположении своих сил практически в реальном масштабе времени. Технической реализацией системы BFT является узкополосная система LPI/LPD COBRA (Collection Of Broadcasts from Remote Assets – сбор трансляций от удаленных средств) для передачи коротких сообщений, обладающая высокой безопасностью и скрытностью. Эта система использует шифрование, сертифицированное АНБ и сопряжена с навигационной системой GPS [344].

В настоящее время американскими военными специалистами прорабатываются вопросы создания перспективной управляющей сети в интересах будущих сил, которая будет состоять из пяти уровней: стандартного, транспортного, сервисов, приложений, сенсоров и платформ. Интеграция этих уровней обеспечивает бесшовную доставку данных и сообщений, а также позволяет достичь высокой ситуационной осведомленности и обработки данных от различных сенсоров, а также сетецентрического управления ведением огня. Проект интегрируемых систем включает в себя [344]:

- общие стандарты и протоколы информационного обмена между модульными объединенными силами на основе IP-технологий, а также совместимое аппаратное обеспечение;
- сетевые транспортные системы, такие как WIN-T, JTRS и др.;
- сетевые сервисы, которые будут обеспечены общим оперативным пространством глобальной системы (ранее FCS), сетецентрическими сервисами, WIN-T и сервисами управления сетью;
- программные приложения, которые обеспечат боевое управление, сетевые возможности управления и общую наземную распределенную систему управления;

- различные сенсоры на необитаемых наземных платформах, БПЛА и пилотируемых платформах, которые будут связаны и объединены в единую разведывательную сеть.

Интеграция всех этих уровней будет проходить на основе платформы LandWarNet, обеспечивающей охват системой управления абонентов от отдельного солдата до мобильных пунктов управления и опорных баз.

Задача модернизации военных систем управления на основе сетецентрических технологий состоит в том, чтобы разработать надежные сетевые решения, которые позволяют командирам различного уровня и отдельным солдатам иметь доступ к информации в любом месте и в любое время. Это осуществляется за счет интеграции существующих систем везде, где это возможно, и разработки новых, готовых к работе в сети программ. Ключевым элементом общей стратегии модернизации систем управления боем является развитие новых вертикальных возможностей систем управления и сопряжение многофункциональных коммуникационных систем [344].

4.3. Системы высокоточного оружия и защиты от них

Высокоточное оружие внесло особый вклад в формирование характера вооруженной борьбы в воздушной сфере в военных конфликтах конца XX века. Под его влиянием непрерывно совершенствовались формы и способы боевого применения средств воздушного нападения (СВН), изменялась тактика действий авиационных группировок, появлялись новые тактические приемы для подавления системы ПВО и нанесения ударов по различным наземным объектам. Оценивая роль ВТО в решении задач военных конфликтов последнего десятилетия и учитывая перспективы его развития в начале XXI века, можно с уверенностью утверждать, что оно и впредь будет оказывать определяющее влияние на формирование характера вооруженной борьбы не только в воздушно-космической сфере, но и, в общем – в сетецентрических войнах будущего [340].

4.3.1. Современное высокоточного оружие

4.3.1.1. Общая характеристика высокоточного оружия

Высокоточное оружие (ВТО) – это комплекс вооружения, в котором интегрированы средства разведки, управления, доставки и поражения, функционирующие в реальном масштабе времени и обеспечивающие наведение боеприпаса на цель с ошибками меньшими, чем радиус его поражения [300].

За последнее десятилетие технологии создания ВТО совершили качественный скачок в своем развитии, существенно расширив возможности по преодолению и огневому подавлению систем ПВО, поражению объектов в любой точке земного шара, в любое время суток и в любых климатических условиях. Раздвинулись рубежи пуска ВТО, снизилась его заметность, увеличилась скорость полета, используются комбинированные системы наведения. Отличительной особенностью ВТО от обычных боеприпасов является наличие в нем командной, автономной или комбинированной систем наведения, осуществляющих управление траекторией полета к цели (объекту поражения) и обеспечивающих заданную в зависимости от характеристик атакуемой цели вероятность ее поражения [300].

Начиная с 1990-х гг., отмечается неуклонный рост использования ВТО в вооруженных конфликтах ВС США и их союзников. В ходе операций «Буря в пустыне» (Ирак, 1991 г.), «Решительная сила» (Югославия, 1999 г.), «Несгибаемая свобода» (Афганистан, 2001 г.) и «Свобода Ираку» (Ирак, 2003 г.) доля применения образцов ВТО от общего количества всех средств поражения составила около 10%, 25%, 60% и 70% соответственно.

Только в период с 19 марта по 18 апреля 2003 г. при ведении боевых действий в Ираке коалиционной группировкой было израсходовано около 29 тыс. единиц авиационного вооружения различных классов и назначения, из них около 19 тыс. – образцы ВТО. По оценкам американских военных специалистов, более 90% из них поразили назначенные цели [29, 37].

В настоящее время в вооруженных силах высокоразвитых государств доля ВТО в системе вооружения ВС составляет около 50%. Ожидается, что в ближайшие 5-10 лет этот процент значительно повысится и может составить 75-90% [334]. К 2020 г. ожидается создание запаса высокоточных крылатых ракет, позволяющего применять их в количестве до 1000 единиц в сутки в течение 60 суток. К 2030 г. – 90

суток (при стоимости одной крылатой ракеты, подобной BGM-109 Tomahawk, примерно 1 млн долларов) [28, 29].

С появлением высокоточного оружия в количествах, достаточных для ведения полномасштабных бесконтактных войн, в государствах, располагающих таким оружием, широкое распространение получили подходы к созданию стратегических неядерных сил. Военные специалисты этих стран полагают, что стратегические неядерные силы постепенно вытеснят нынешние стратегические ядерные силы, возьмут на себя их функции сдерживания и позволят решать значительно больший круг задач с меньшими затратами и потерями [300].

С начала 2000-х гг. технически развитые страны активизировали исследования в области придания своим вооруженным силам способности высокоточного воздействия на цели в кратчайшие сроки и на большие дальности с использованием набора ударных средств в обычном (неядерном) оснащении. Для достижения поставленной цели развернуты работы по созданию новейших типов высокоточных мобильных стратегических неядерных вооружений, в том числе таких, как планирующие и маневрирующие гиперзвуковые боеголовки, высокоточные крылатые ракеты, проникающие в грунт боеголовки, баллистические ракеты с боеголовками индивидуального наведения в обычном оснащении [95].

Главным отличительным свойством систем высокоточного оружия является реализованный принцип «выстрел – поражение». Его дальнейшее развитие идет в направлении «интеллектуализации» данного оружия путем придания ему способности «распознавать» цели, в том числе на поле боя и в условиях помех, а при воздействии по крупным целям – выбирать наиболее уязвимое место цели для ее поражения [300].

Под ВТО подразумеваются типы обычных вооружений и средств их доставки [331, 336]:

- разведывательно-ударные комплексы (РУК), реализующие принцип «обнаружил – выстрелил – поразил»;
- артиллерийские управляемые и самонаводящиеся боеприпасы (снаряды и мины, в том числе кассетные);
- управляемые авиабомбы (УАБ), в том числе модульной конструкции (с ракетным ускорителем);
- управляемые ракеты типа «воздух-поверхность»;
- крылатые ракеты воздушного и морского базирования;
- межконтинентальные баллистические ракеты в обычном снаряжении, а также управляемые на траектории, в том

числе с кассетными боеголовками и самонаводящимися боевыми элементами.

Дальность применения управляемых авиабомб обычно составляет до 30 км, планирующих УАБ и УАБ модульной конструкции – до 80 км, управляемых ракет – до 200 км, а крылатых ракет – до 2000-3000 км.

Общая классификация ВТО по данным работ [336, 340] приведена на рис. 4.13.

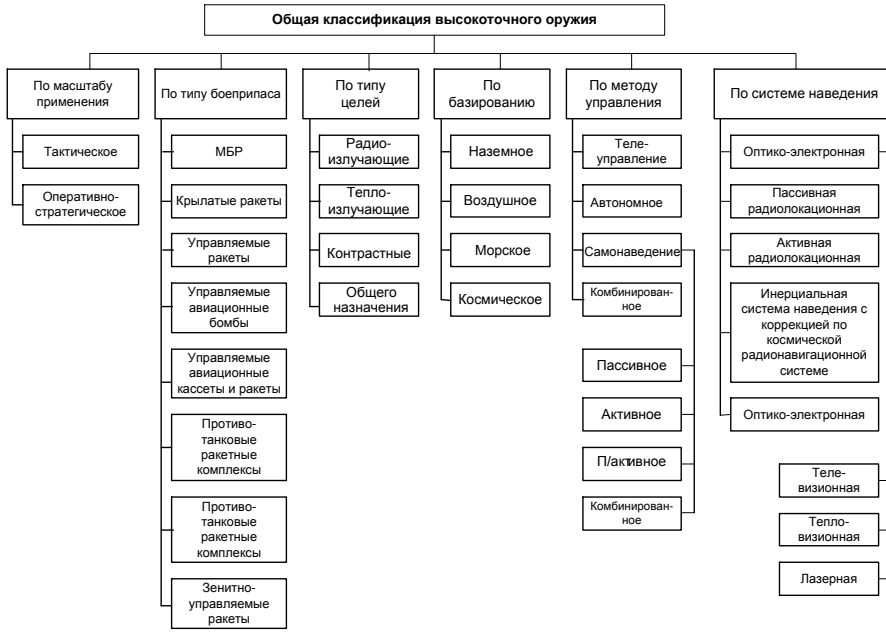


Рис. 4.13. Общая классификация ВТО [336, 340]

По масштабам применения ВТО подразделяют [336]:

- на оперативно-стратегическое;
- на тактическое.

К оперативно-стратегическому ВТО относятся наиболее мощные системы оружия, применение которых позволит стороне конфликта нанести решающее поражение противнику [336]:

- крылатые ракеты:
  - наземного базирования;
  - морского базирования;
  - воздушного базирования;

- управляемые ракеты (типа Lance-2);
- баллистические ракеты, наводимые на конечном участке траектории (типа Pershing II);
- разведывательно-ударные комплексы типа PLSS (Precision Location Strike System) и JSAK (Joint State Area Command);
- дистанционно пилотируемые летательные аппараты.

К тактическому высокоточному оружию относятся [336]:

- авиационные управляемые бомбы;
- управляемые авиационные кассеты и ракеты;
- противотанковые ракетные комплексы (ПТРК) и танки, способные применять управляемые ракеты.

Наиболее распространенным видом ВТО являются крылатые ракеты, основными достоинствами которых являются следующие показатели [300]:

- возможен пуск с земли, воды и воздуха на удалении в несколько тысяч километров от границы территории и зон ПВО противника;
- благодаря малой эффективной площади рассеивания и способности осуществлять полет с огибанием рельефа местности на малых и предельно малых высотах снижается эффективность огневого поражения средствами ПВО противника;
- большая масса боевой части крылатой ракеты определяет ее значительную разрушительную мощь.

Исходя из характера излучения поражаемых объектов, ВТО можно классифицировать по типу поражаемых целей [336]:

- на радиоизлучающие;
- на теплоизлучающие;
- на контрастные.

Для поражения объектов (целей) общего назначения применяются баллистические и крылатые ракеты, управляемые ракеты, при наведении которых энергетический контакт между боеприпасами и целью отсутствует. Эти же объекты могут поражать артиллерия и самолеты с применением управляемых и самонаводящихся боеприпасов. К оружию, поражающему радиоизлучающие цели (командные пункты, радиолокационные станции, узлы связи, центры управления и наведения авиации, ПВО и т.д.), относят средства поражения типа РУК PLSS, противорадиолокационные ракеты AGM-88 HARM, AGM-78 Standard-ARM, AGM-45 Shrike и др. Теплоизлучающие цели могут быть поражены управляемыми авиационными бомбами GBU-15,

AGM-130 управляемыми ракетами AGM-65 Maverick, AGM-650 F и G, а также суббоеприпасами РУК JSAC [336].

К оружию, поражающему цели, обладающие контрастом (радиолокационным, тепловым, фотометрическим) с фоновой поверхностью, относятся РУК JSAC, а также артиллерийские и авиационные управляемые или самонаводящиеся боеприпасы [336].

В зависимости от типа носителя ВТО может быть [300, 340]:

- авиационного базирования;
- морского базирования;
- наземного базирования.

При этом в ближайшие 10 лет возможно появление ВТО космического базирования.

В современных серийных образцах ВТО используются комбинированные системы наведения в составе инерциального блока управления с коррекцией по данным космической радионавигационной системы и различных головок самонаведения (ГСН): тепловизионных; активных, полуактивных, пассивных радиолокационных; лазерных – которые обеспечивают применение оружия в любых метеорологических условиях и при любой помеховой обстановке.

В зависимости от характера аппаратуры, обеспечивающей точное наведение оружия на цель, места ее размещения, особенностей энергетического контакта с целью различают четыре метода управления [336]:

- телеуправление;
- автономное;
- самонаведение;
- смешанное (комбинированное).

В зависимости от типа установленной на борту системы наведения ВТО подразделяется [341, 340]:

- на ВТО с оптико-электронными системами наведения (телевизионной, тепловизионной, лазерной);
- на ВТО с пассивной радиолокационной системой наведения;
- на ВТО с активной радиолокационной системой наведения;
- на ВТО с инерциальной системой наведения и коррекцией с использованием данных космической радионавигационной системы (КРНС);
- на ВТО с комбинированной системой наведения (различные комбинации вышеперечисленных систем наведения).

Основные научно-технические программы в области развития ВТО направлены на увеличение скорости и дальности полета боеприпаса, повышение точности стрельбы, снижение радиолокационной и оптической заметности, использование комбинированных систем наведения, которые позволяют применять оружие в любых метеорологических условиях. Особое внимание уделяется оснащению ВТО различными типами боевых частей, что значительно расширяет спектр решаемых боевых задач и избирательность воздействия [340].

Основными направлениями совершенствования средств ВТО являются:

- разработка новых средств и способов доставки ВТО к цели;
- разработка новых боеприпасов ВТО;
- разработка новых средств информационного обеспечения применения ВТО.

К разрабатываемым перспективным средствам и способам доставки высокоточного оружия к цели можно отнести [300]:

- гиперзвуковые аэрокосмические ракеты;
- гиперзвуковые крылатые ракеты;
- разведывательно-ударные комплексы на основе БПЛА.

Наибольшее воздействие на этот процесс технологического совершенствования средств ВТО и процессы его боевого применения окажут факторы, представленные в работе [340].

1. Рост количественного состава ВТО в общем арсенале средств поражения. Удешевление стоимости производства ВТО за счет глобальной унификации на всех уровнях (функциональная, аппаратурная, конструктивно-технологическая, элементная унификации).

2. Возможность применения ВТО с рубежей, находящихся не только вне зон действия активных средств ПВО, но и вне зон информационных средств ПВО. Это достигается путем разработки ВТО большой дальности стрельбы, а также путем реализации различных траекторий полета ВТО, позволяющих производить его пуски с носителей из-за радиогоризонта.

3. Расширение диапазона высот и скоростей применения ВТО от воздушной сферы до воздушно-космической. В настоящее время в США и НАТО открыт ряд программ по созданию гиперзвуковых управляемых и крылатых ракет. Отличительными особенностями данных типов средств будут являться высокая оперативность и гибкость боевого применения, малая уязвимость, повышенная внезапность и скрытность ударов за счет возможности их применения с любых

направлений, в любых погодных условиях и независимо от времени суток.

4. Резкий рост уровня «интеллекта» ВТО, связанный с появлением новых поколений высокопроизводительных многоядерных процессоров с малым энергопотреблением и совершенствованием программного обеспечения в части применения ВТО, его управления на этапах преодоления зоны ПВО и распознавания цели.

5. Придание ВТО «всепогодных» свойств, позволяющих эффективно применять его в любой обстановке, независимо от метеорологических условий и времени суток. В результате в ближайшем будущем точность стрельбы основных типов ВТО не будет зависеть от метеорологических условий. Этот фактор получил свое развитие в результате разработки для ВТО различных систем наведения. В настоящее время многие типы средств поражения оснащены инерциальной системой наведения с коррекцией с использованием данных КРНС NAVSTAR, а также комбинированными системами наведения, работающими на разных физических принципах.

6. Расширение перечня типов объектов, поражаемых ВТО, и появление возможности реализации принципа избирательности воздействия по объектам. Этот фактор получил свое развитие благодаря разработкам различных типов боевых частей для ВТО. Первые образцы ВТО были способны поражать только слабо защищенные в инженерном отношении точечные объекты. В настоящее время для ВТО разработаны проникающие бетонобойные боевые части, способные эффективно поражать высокозащищенные углубленные объекты.

Активно ведутся работы по созданию ВТО так называемого нелетального воздействия. К ним относятся ЭМИ боеприпасы для поражения электромагнитным импульсом различных типов РЭС, а также боеприпасы, снаряженные наэлектризованной графитовой смесью для вывода из строя систем электроснабжения.

7. Возможность создания в США и НАТО на рубеже 2015-2020 г. «Перспективной интегрированной системы применения ВТО». Предусматривается, что в состав данной системы будут интегрированы ударные средства, оснащенные ВТО (авиация, надводные корабли и подводные лодки, наземные комплексы, ударные БПЛА), и информационно-управляющая инфраструктура, единая для всех видов ВТО (система глобального наблюдения и разведки, система связи и передачи данных, система контроля и управления). Данной системе отводится решающая роль в разрабатываемой в США концепции сетецентрической войны.

Вследствие массового принятия на вооружение новых типов ВТО формы и способы боевого применения СВКН приобретут иной характер и существенно пополнят свое содержание. Это проявится, прежде всего, в том, что все боевые действия приобретут явно выраженный воздушно-космический характер и будут вестись в единой воздушно-космической сфере. Появится ряд новых особенностей, обусловленных качественным совершенствованием ВТО, к которым относятся [340]:

1. Значительно возрастут пространственные параметры боевых действий и увеличится объем решаемых задач оперативно-стратегического и стратегического масштаба. Эта тенденция связана с увеличением дальности применения ВТО и возможностью эффективного его использования для нанесения ударов по объектам, находящимся в глубоком тылу противостоящей стороны.

2. В результате повышения избирательности применения ВТО появится возможность комплексного и одновременного решения главных задач операций (боевых действий) уже на начальном этапе военного конфликта.

3. Существенно возрастут динамичность и интенсивность боевых действий и, следовательно, повысятся требования к срокам выполнения основных боевых задач.

4. Появится реальная возможность для достижения тактической внезапности, особенно при нанесении первого ракетно-авиационного удара воздушной наступательной операции. Эта тенденция обусловлена, с одной стороны, значительным ростом боевого потенциала группировок СВКН, что позволяет начать боевые действия существующими группировками без предварительного их усиления, а с другой – возможностью применения ВТО с рубежей, находящихся за пределами зон контроля информационных средств противостоящей стороны, а также с неожиданных направлений.

5. При нанесении массированных ударов произойдут изменения в оперативно-тактическом построении СВКН, связанные с увеличением количества сил, действующих в эшелоне беспилотных средств поражения. Эта тенденция обусловлена количественным увеличением такого типа ВТО, как крылатые ракеты воздушного и морского базирования, которые будут способны самостоятельно решать практически весь спектр боевых задач.

Кроме того, произойдут изменения в тактическом построении боевых порядков пилотируемой авиации, действующей в эшелоне подавления ПВО и в ударных эшелонах. Это найдет свое выражение в

переходе к одновременным действиям большого количества небольших по составу ударных групп и даже одиночных самолетов, решающих конкретные задачи по поражению объектов. Эта тенденция обусловлена высокими точностными характеристиками средств поражения, что позволяет решать боевые задачи меньшим составом сил [340].

Количество самолето-вылетов, необходимое для поражения одних и тех же малоразмерных объектов с помощью ВТО, значительно сократится по сравнению с применением неуправляемых средств поражения. Поэтому такое понятие, как «массированный авиационно-ракетный удар», приобретет совсем иной смысл, а именно будет рассматриваться не с точки зрения массированных налетов авиации в плотных боевых порядках, а с точки зрения одновременных действий большого количества небольших по составу авиационных групп. Переход к таким действиям уже явно обозначился в военных конфликтах последних лет, где авиация США и НАТО одновременно наносила удары по большому количеству объектов, используя при этом небольшие по составу ударные группы и даже одиночные самолеты [340].

Необходимо также отметить неординарное влияние, которое перспективное авиационное ВТО может оказать на тактику действий самолетов-носителей. Эта тактика существенно упростится, поскольку главными задачами самолетов-носителей останутся выход на установленные рубежи применения ВТО, расположенные вне зон действия активных средств ПВО противостоящей стороны (а в некоторых случаях и вне зон информационных средств ПВО), и проведение согласованных по времени пусков ВТО [340].

Учитывая это обстоятельство, а также возможность создания вышеупомянутого «интеллектуального ВТО» при прогнозировании действий СВКН в будущих военных конфликтах, целесообразно рассматривать не столько тактику действий самолетов-носителей ВТО, сколько тактику применения самого ВТО. Эта тактика будет определяться, прежде всего, типом системы наведения, установленной на конкретном образце ВТО, характером объекта поражения, а также степенью его защищенности активными и пассивными средствами ПВО [340].

В качестве основных средств информационно-разведывательного обеспечения применения ВТО используются космические и, в меньшей степени, воздушные системы видовой разведки. Группировка космической видовой разведки включает в себя спутники оптоэлектронной и радиолокационной разведки, спутники-ретрансляторы

и развитую высокопроизводительную наземную инфраструктуру. Данная группировка позволяет с высокой точностью вскрывать оперативное построение войск противника, состав его сил и средств, в том числе элементы системы боевого управления, а также определять координаты наиболее важных объектов. Значительные усилия предпринимаются в области разработки аппаратуры гиперспектральной съемки, РЛС обнаружения движущихся целей и методов высокоточного определения их координат. В ближайшее десятилетие возможно создание орбитальной системы на базе большого количества малогабаритных спутников видовой разведки с аппаратурой гиперспектральной съемки и РЛС с синтезированием апертуры антенны. Такая система обеспечит всепогодное обнаружение мобильных замаскированных целей при высокой частоте просмотра заданного района и вне зависимости от технического состояния отдельных спутников [29].

В ряде технологически развитых стран (прежде всего в США) финансируются программы создания на основе ВТО оружия глобального действия нового поколения, в том числе [269]:

- средств нападения на основе гиперзвуковых технологий, полет которых будет проходить в диапазоне высот от 35-40 км до 100-120 км на скоростях от 3 М до 15-20 М. Полетное время таких средств на межконтинентальную дальность соизмеримо с полетным временем МБР, а параметры траектории полета не позволяют эффективно обнаруживать их существующими средствами разведки;
- космических платформ для размещения на них гиперзвуковых летательных аппаратов;
- МБР и ПЛАРБ, обладающих высокой точностью и эффективностью поражения объектов за счет оснащения их маневрирующими ГЧ, в том числе в неядерном исполнении;
- ядерных боезарядов глубокого проникновения, малой мощности и ядерных боезарядов четвертого поколения – термоядерных, для поражения командных пунктов и ракетных шахт БР.

Применение боезарядов, упомянутых в последним пункте не должно привести к экологической катастрофе. Первый тип боеприпаса подрывается на глубине 30-70 м, при этом компоненты ядерного взрыва практически не выходят на поверхность. Второй – термоядерный, реакция синтеза в нем инициируется альтернативной реакцией деления источником энергии. Это позволяет избежать традиционного, при

применении ядерных боезарядов предыдущих поколений, радиоактивного заражения местности [269].

Таким образом, доминирующее влияние на формирование характера вооруженной борьбы в воздушно-космической сфере в военных конфликтах начала XXI века будет оказывать ВТО, которое станет главным средством огневого воздействия практически на все объекты, независимо от степени их защищенности и мобильности. Можно с уверенностью утверждать, что войны будущего – это войны высокоточных технологий [340].

4.3.1.2. Образцы и тенденции развития высокоточного оружия (на примере оружия ВС США)

За последние годы наивысший приоритет в программах военного строительства США получили именно те системы вооружения, которые отличаются высокой точностью, трудностью их обнаружения и повышенной дальностью. К таким системам, в частности, относятся крылатые ракеты морского и воздушного базирования (для нанесения ударов с рубежей, недоступных для средств обороны противника), самолеты, выполненные по технологии Stealth (стратегические и тактические), беспилотные средства поражения (прежде всего, для ударов по РЛС и космическим аппаратам воздушно-космической обороны), разведывательно-ударные комплексы (для поражения групповых бронетанковых, а также точечных высокозащищенных целей в глубине обороны противостоящей стороны). Новым этапом в развитии этих средств стали активные работы в области гиперзвуковых средств доставки, что к уже упомянутым качествам ВТО добавляет еще одно важнейшее для воздействия на ядерный потенциал противника качество – минимальное подлетное время [10, 29].

Анализ применения ВТО в конфликтах последних десятилетий показывает, что решающую роль в современной войне играют именно ВТО из-за его большой ударной мощи и радиуса действия, гибкости боевого применения, мобильности его боевых платформ и почти абсолютной точности поражения целей. При этом следует заметить, что оба класса управляемого оружия – управляемые авиабомбы и крылатые ракеты (КР) – взаимно дополняли друг друга по дальности применения: КР имеют ограничение по минимальной, а авиабомбы – по максимальной дальности боевого применения. Кроме того, инфракрасное излучение реактивного двигателя КР делает ее уязвимой для средств

ПВО противника, а управляемые авиабомбы двигателей не имеют и легко преодолевают ПВО объекта удара.

Опыт военных конфликтов последнего десятилетия показал, что ВС США и их союзников в качестве основного средства ВТО используют КРМБ Tomahawk. Ракета имеет несколько алгоритмов атаки и различные типы боевых частей (фугасные/кассетные/проникающие). В настоящее время основной модификацией, применяемой в ВМФ США, является Tactical Tomahawk (TacTom). Данная модификация явилась продуктом ряда доработок, направленных на то, чтобы сделать ее более пригодной для тактической поддержки войск, то есть для применения в непосредственной близости от линии фронта. Были приняты меры по снижению стоимости ракеты в сравнении с предшествующими образцами за счет использования более легких материалов и более дешевого двигателя Williams F415-WR-400/402. Ракета оснащена совмещенной инерциально-спутниковой системой наведения, рельефометрической системой коррекции траектории TERCOM, а также системой оптико-электронного распознавания целей DSMAC (Digital Scene Matching Area Correlation), которая позволяет ракете распознавать наземные цели, сопоставлять их с имеющимися в памяти бортового вычислителя их изображениями и выполнять наведение с КВО до 10 м. Масса боевой части 340 кг, дальность действия ракеты 1600 км. Ракета имеет спутниковую систему передачи данных, что дает возможность перенацеливать ее в полете на любую из 15 заранее запрограммированных целей. Установленная на борту ТВ-камера позволяет оценивать состояние цели при приближении к ней и принимать решение о продолжении атаки или перенацеливании ракеты на другую цель [350].

На смену ракетам Tomahawk со временем должно прийти новое поколение ракет типа Fasthawk. Эти ракеты при достаточно высокой дальности стрельбы (740 км в режиме Surface Skimming и 2200 км в режиме баллистического полета) имеют существенно более высокие скоростные показатели (3000 км/ч и 5600 км/ч соответственно) по сравнению с устаревающими уже КР Tomahawk. Кроме того, они обладают возможностью получения уточненных целеуказаний в полете к цели или при барражировании в безопасной зоне. Прогноз-анализ показывает, что к 2020 г. количество кораблей – носителей ракет данной системы может составить не менее 70 единиц, а к 2030 г. – 100 единиц с общим боекомплектом на борту до 200 тыс. высокоточных крылатых ракет [269].

В настоящее время в интересах реализации концепции «Мгновенный глобальный удар» (PGS – Prompt Global Strike) предусматривается обеспечить военное ведомство средством нанесения быстрых и точных неядерных ударов по любой цели на планете в ответ на угрозы национальной безопасности США. При этом речь идет о реагировании на возникновение таких угроз в минимальные сроки или без предупреждения вообще [95].

С целью совершенствования боевых возможностей стратегических сил в США реализуется комплекс программ модернизации, направленный на продление сроков эксплуатации ПЛАРБ типа Ohio и находящихся на их борту БРПЛ Trident II до 2040 г., а также доработку системы управления ракетами с целью повышения оперативности их перенацеливания и точности стрельбы. Кроме того, предусматривается существенно увеличить количество полетных заданий ракет, что расширит возможности планирования ракетных ударов по поражению критичных по времени целей. Ведется разработка твердых видов топлива для ракетных двигателей. Осуществляется переоборудование четырех ПЛАРБ типа Ohio под носители КРМБ Tomahawk. При этом, вместо 16-20 БРПЛ на одной ПЛАРБ развертывается более 150 КРМБ [335, 337].

К 2040 г. планируется принять на вооружение новую ракету морского базирования и развернуть ПЛАРБ нового поколения. Проводятся исследования по определению общей конфигурации перспективной высокоточной БРПЛ средней дальности (3000 км), способной поражать цели в течение 10-15 мин после пуска. Параллельно ведутся работы по модернизации боевых частей БРПЛ и совершенствованию их тактико-технических характеристик [335].

Сторонники оснащения БРПЛ неядерными боеголовками отмечают ряд их достоинств по сравнению с МБР [338]:

- БРПЛ могут быть развернуты ближе к потенциальным целям, чем МБР, что потребует меньшего подлетного времени;
- в отличие от МБР траектории БРПЛ могут быть выбраны таким образом, чтобы не вызвать международного резонанса из-за их пролета в воздушном пространстве недружественных государств;
- гибкость в выборе траектории позволит минимизировать попутный ущерб, связанный с падением ступеней ракет;

- БРПЛ по сравнению с МБР в меньшей степени подвержены ограничениям в соответствии с международными договорами.

В настоящее время в США продолжается процесс совершенствования ВТО. К сверхэффективным высокоточным неядерным вооружениям Пентагон относит [300]:

- модифицированные баллистические ракеты (БРПЛ) Trident II (D5), оснащенные вместо ядерных боеголовок обычными;
- разрабатываемые гиперзвуковые аэрокосмические ракеты с дальностью действия 6 тыс. км;
- гиперзвуковые крылатые ракеты со скоростью полета около 6500 км/ч;
- ракеты SJX61, принятие которых планируется в 2017 г.

В целях непрерывного информационного обеспечения ВТО ВС США дополняют космические системы разведки воздушными средствами. Вместе с разведывательными самолетами используют стратегические разведывательные БПЛА – высотный RQ-4A Global Hawk и средневысотный MQ-1B Predator. В настоящее время в связи с необходимостью ведения воздушной разведки с больших высот аппараты Global Hawk в силу своей экономичности и эффективности могут заменить пилотируемые высотные разведывательные самолеты U-2 [29, 37, 80, 95].

4.3.2. Гиперзвуковое высокоточное оружие

4.3.2.1. Общая характеристика гиперзвукового оружия

Гиперзвуковые летательные аппараты (ГЗЛА), по мнению аналитиков, вне зависимости от дислокации в перспективе смогут достигать любой точки земного шара в течение одного часа и тем самым служить альтернативой МБР, оснащенных ядерными боеприпасами [95]. По мнению ряда экспертов, гиперзвуковые управляемые ракеты будут способны наносить молниеносные точные удары по пунктам управления вооруженными силами, базам подводных лодок и шахтным установкам межконтинентальных баллистических ракет, местам дислокации дальних бомбардировщиков на территории противника, который, даже обладая стратегическими ядерными силами, просто не

успеет ответить. С помощью таких гиперзвуковых крылатых ракет США могут получить практически неуязвимые для ПВО средства ВТО и еще более развить концепцию «обезоруживающего удара» [346].

ГЗЛА – это летательный аппарат (самолет или ракета), способный разгоняться и маневрировать в атмосфере со скоростью, многократно превышающей скорость звука. Говоря о гиперзвуке, надо иметь в виду, прежде всего долговременный полет в атмосфере со скоростями, превышающими 4-5 М (М – число Маха, равное скорости звука в атмосфере 331 м/с). Такая скорость давно доступна МБР, но они достигают ее только в космосе, в безвоздушном пространстве, на высотах, где отсутствует сопротивление воздуха и соответственно возможность аэродинамического маневрирования и управления полетом. Применительно к ГЗЛА речь идет об управляемом полете в атмосфере со скоростями 6-7 М, а в перспективе – 10-12 М [346, 347].

Военные самолеты сегодня могут эффективно применяться лишь на высотах до 20-25 км, а космические аппараты – на высоте не менее 140 км. Промежуток же высот от 20-25 до 140-150 км оказывается недоступным для военного использования. Вместе с тем именно этот диапазон высот, доступный исключительно для ГЗЛА, является очень перспективным с точки зрения их использования [347].

Тематика ГЗЛА очень важна для развития ВТО, так как позволяет обеспечить его высокие показатели по скорости, точности и неуязвимости. Гиперзвуковые ракеты, когда их удастся создать, будут способны поразить любую цель на земном шаре в течение часа. Причем благодаря своей способности маневрировать, корректировать курс на протяжении всего полета – поразить с высочайшей точностью, буквально до метра, стартуя при этом с воздушных или воздушно-космических носителей, отследить которые крайне сложно. Двигаясь в атмосфере, в плазменном облаке, они будут максимально скрытными и сложно доступными для системы обнаружения ПРО. Помимо сложности обнаружения гиперзвуковые цели чрезвычайно сложны для перехвата [347].

Таким образом, ГЗЛА имеют ряд только им присущих особенностей, существенно затрудняющих решение задач по их обнаружению, сопровождению, опознаванию и поражению, возложенных на средства системы ПВО-ПРО (воздушно-космической обороны) государства, против которого они будут применяться [300]:

- возможность использования ранее не освоенного диапазона высот от 25 до 140 км от земной поверхности;

- способность ГЗЛА осуществлять полет на ранее не достижимых для средств воздушно-космического нападения скоростях (от 5 до 30 М) как в атмосфере, так и за ее пределами – в околоземном космическом пространстве;
- использование смешанных труднопрогнозируемых траекторий полета к объекту поражения (аэродинамическая – на начальном этапе полета, эллиптическая – при полете в околоземном космическом пространстве, баллистическая – на конечном этапе полета во время атаки объекта поражения);
- сочетание в одном ГЗЛА боевых свойств как аэродинамических средств воздушного нападения, так и космического аппарата.

По данным зарубежных источников информации широкое поступление ГЗЛА на вооружение ожидается не ранее 2020 г. [300].

Классификация ГЗЛА приведена на рис. 4.14 [269].

Рис. 4.14. Классификация ГЗЛА [269]

4.3.2.2. Проекты гиперзвукового оружия различных стран

Кратко рассмотрим информацию о ведущихся в странах Запада и США разработках ГЗЛА, способных действовать как в воздухе, так и в космосе, переходя из одной сферы в другую.

Существенный объем НИОКР в этой области выполняется в США. Ради скорейшей разработки ГЗЛА сегодня различными ведомствами разрабатывается сразу несколько перспективных гиперзвуковых проектов. Это X-43A (его курирует космическое агентство NASA), X-51A и Falcon HTV-2 (проекты ВВС), AHW (Сухопутные войска), ArcLight (Военно-морские силы) и другие. Такой массированный штурм гиперзвука, по мнению специалистов, позволит американ-

цам уже к 2018-20 гг. создать серийные образцы ГЗЛА большой дальности воздушного и морского базирования [269, 347, 288].

Аналогичные исследования по ГЗЛА проводятся в Великобритании, Франции, Германии, Японии и Китае, общая стоимость их национальных программ оценивается в 11-13 млрд долл. Учитывая значительную стоимость работ, эти государства принимают меры по кооперации, а также заимствованию технологических решений друг друга при реализации разработок [269].

В августе 2014 г. был осуществлен пуск ракеты Х-43А с полигона Кодьяк (Kodiak) на Аляске. Эта ракета разрабатывалась как совместный проект американской армии и лаборатории Sandia National в рамках концепции «Быстрого глобального удара». Предполагалось, что в ходе испытаний она, набрав скорость около 6500 км/ч, поразит учебную цель на тихоокеанском атолле Кваджалейн (Kwajalein), однако аппарат проработал всего 7 с, после чего сгорел в атмосфере. Тем не менее в США назвали этот полет успешным, т.к. ракета продемонстрировала способность двигаться с требуемым ускорением [347].

К тематике ГЗЛА относится и разработка воздушно-космических самолетов, способных действовать как в безвоздушном пространстве, так и в атмосфере, совершая при этом стремительные гиперзвуковые «нырки» с околоземной орбиты в воздушную среду для применения высокоточного оружия [347].

В США проекты воздушно-космических самолетов реализуются по программам Falcon и Х-37 [347].

Автономный аппарат Х-37 был отправлен в первый полет 22 апреля 2010 г. и вернулся на Землю 3 декабря 2010 г. Посадка в автоматическом режиме была осуществлена на взлетно-посадочную полосу базы ВВС США Ванденберг. Ряд экспертов высказывают предположение, что за 225 суток, проведенных в космосе, воздушно-космический самолет провел реальные пуски боевого оружия. Именно в это время был сбит российский спутник, что официально объяснили возможным попаданием в него метеорита. До сих пор руководство ВВС США не публикует никаких подробностей о целях и задачах полета Х-37В [96].

Боевые аппараты, которые создаются по программе Х-37, уже сегодня позволяют выводить на орбиту до трех боеголовок и доставлять их к цели, минуя систему предупреждения о ракетном нападении и другие средства контроля. В перспективе американский воздушно-космический самолет, выведенный на орбиту с гиперзвуковыми ракетами на борту, будет способен нести там боевое дежурство в течение

нескольких лет – в постоянной готовности к мгновенному применению оружия по сигналу с земного командного пункта. Орбитальная группировка из нескольких десятков таких аппаратов будет способна обеспечить поражение любой цели на земной поверхности в течение буквально нескольких минут [347].

В ноябре 2011 г. в США прошли первые удачные испытания тестового летательного аппарата по проекту Falcon HTV-2 (HTV – Hypersonic Technology Vehicle), в ходе которых он был запущен ракетой-носителем, затем разогнан ракетным ускорителем до скорости 20 М – около 23 000 км/ч. Обычная боеголовка после этого летит по баллистической траектории, а HTV-2 скользил в верхних слоях атмосферы на гиперзвуке [300].

Falcon представляет собой маневрирующий возвращаемый космический аппарат, способный действовать на гиперзвуковых скоростях в околоземном пространстве и в приграничной зоне «космос-стратосфера» и доставлять к назначенным объектам ударов набор вариантов оружия общим полезным весом не менее полутоны, включая мощные проникающие боезаряды для поражения заглубленных и защищенных объектов или пакет до 6 единиц боеприпасов WAASM (Wide-Area Airborne SurveillanceSystem) широкозонального автономного поиска и поражения подвижных и стационарных целей, или пакет из 4 «интеллектуальных бомб» SBWS (Smart Bomb Weapon System) для избирательного поражения целей, или пакет из 6 беспилотных разведывательных аппаратов UAV (Unmanned aerial vehicles) для разведки поля боя [269].

В июле 2014 г. представители DARPA (Defense Advanced Research Projects Agency) анонсировали первую фазу реализации нового проекта по созданию беспилотного космического корабля XS-1 (Experimental Spaceplane). В долгосрочных планах агентства добиться того, чтобы беспилотный космический корабль мог совершить 10 полетов за 10 дней, хотя бы в одном полете достигнув скорости 10 М. Стоимость каждого совершенного рейса не должна будет превышать 5 млн долларов. При этом аппарат должен будет нести на борту полезную нагрузку массой от 1,36 до 2,37 т. Совершение гиперзвуковых полетов экспериментальным американским космическим беспилотником XS-1 намечено на начало 2018 г. Автономный гиперзвуковой космолет XS-1, который будет совершать полеты как обычный самолет, при этом сможет также выводить спутники на низкую орбиту на отделяемой от аппарата ступени. Предполагается, что вторая ступень ракеты-носителя будет осуществлять выпуск полезного груза на суборби-

тальной высоте полета, как только она сможет отсоединиться от основного корпуса. Сам беспилотный аппарат вернется назад на Землю и практически сразу же начнет готовиться к совершению следующих полетов. Представители агентства DARPA отмечают, что они собираются финансировать работы трех компаний, которые будут работать над созданием собственных демонстраторов беспилотного космолета XS-1. Денежные средства будут выделены компании Northrop Grumman Corporation, сотрудничающей с Virgin Galactic, Masten Space Systems, XCOR Aerospace, и компании Boeing, работающей с Blue Origin [263].

Таким образом, воздушно-космические самолеты как система оружия будут обладать значительными стратегическими преимуществами, что позволит им выполнять боевые задачи на качественно новом уровне. Предполагается, что основными задачами этих систем оружия будут [269]:

- поражение стратегически важных объектов, включая критичные по времени, в том числе мобильные наземные цели в глубине территории противника;
- ведение стратегической воздушной разведки;
- перехват воздушно-космических целей;
- вывод на околоземные орбиты КА различного назначения;
- переброска войск и военной техники на трансконтинентальную дальность.

Помимо США обширную программу в области гиперзвука успешно развивает и Китай. Так, по сообщениям СМИ со ссылкой на китайского военного эксперта Лу Сяодуна в Китае недавно совершил свой первый испытательный полет гиперзвуковой самолет. Этот ГЗЛА по своей скорости обошел все существующие современные сверхзвуковые самолеты, в том числе и знаменитый SR-71 Blackbird – американский стратегический сверхзвуковой разведчик. Лу Сяодун отметил, что в «США уже достаточно давно занимаются созданием гиперзвукового самолета нового поколения, который мог бы достичь скорости полета 5 М, но планы американцев так и остаются на бумаге. В этот раз КНР, можно сказать, сумела превзойти все ожидания международных наблюдателей» [293].

Таким образом, развитие технологий ГЗЛА в ближайшее время позволит получить высокоскоростное глобальное оружие, которое выведет эффективность применения ВТО на принципиально новый уровень.

4.3.3. Перспективные боевые части высокоточного оружия (на примере оружия ВС США)

Помимо совершенствования средств доставки ВТО развитые страны уделяют большое внимание развитию боевых частей (БЧ) этого оружия.

В США особое внимание уделяется совершенствованию существующих и разработке новых самонаводящихся боеприпасов для снаряжения кассетных БЧ КР морского и воздушного базирования, УР классов «воздух – земля» и «корабль – берег», управляемых и неуправляемых кассет, а также УАБ [338].

4.3.3.1. Малогабаритные высокоточные боеприпасы

В целях повышения эффективности выполнения задач по уничтожению малоразмерных целей, расположенных, главным образом, в населенных пунктах, при минимальном побочном ущербе в состав снаряжения кассетных БЧ КР, а также применяемого вооружения боевых самолетов и ударных БПЛА планируется включить новые малогабаритные высокоточные боеприпасы (например, Viper Strike). Эти боеприпасы оснащены осколочно-фугасной БЧ с 20-30 поражающими элементами, автономной системой управления с коррекцией по данным КРНС NAVSTAR и полуактивной лазерной ГСН. Наведение боеприпаса на конечном участке траектории может осуществляться бортовым дальномером-целеуказателем носителя или системой подсвета цели передовых авианаводчиков [338].

4.3.3.2. Самоприцеливающиеся боевые элементы

Совершенствуются малогабаритные относительно дешевые самоприцеливающиеся боевые элементы, предназначенные, прежде всего, для поражения бронетанковой техники. При этом предпочтение отдается БЧ, построенным по принципу ударного ядра. Отличием этих БЧ от традиционных кумулятивных является применение кумулятивной выемки большого радиуса, а также значительная дальность действия (более 100 м) [338].

В качестве основных направлений развития самоприцеливающихся боевых элементов в США определены [338]:

- существенное снижение массогабаритных показателей;

- повышение поражающего действия БЧ благодаря применению облицовок из тяжелых металлов, например, из обедненного урана, германия и др. при одновременном снижении закупочной стоимости;
- создание всепогодных помехозащищенных прицельных датчиков, выполненных на современной элементной базе;
- совершенствование алгоритмов обнаружения цели, исключающих ее пропуск и ложное срабатывание;
- разработка новых систем и методов рассеивания элементов, обеспечивающих максимальную площадь накрытия и высокую эффективность поражения целей;
- унификация боевых элементов по носителям.

Основными американскими самоприцеливающимися боевыми элементами с БЧ являются боевые элементы (БЭ) SADARM и SKEET, которые входят в состав кассетных БЧ крылатых ракет и авиационных кассет. Первый из них, представляющий собой готовый БЭ, оснащен инфракрасным датчиком. Стабилизация БЭ в полете осуществляется асимметричным парашютом, благодаря чему обеспечивается круговой поиск цели. Четыре самоприцеливающихся БЭ SKEET входят в состав суббоеприпаса BLU-108/B. Данные боеприпасы могут применяться как самостоятельно (главным образом, с многоцелевых БПЛА), так и входить в состав кассетных БЧ авиационного оружия. При боевом применении снижение и стабилизация боеприпаса обеспечиваются парашютом. После его сброса на заданной высоте с помощью встроенного в корпус твердотопливного ракетного двигателя осуществляется вертикальный набор высоты и раскрутка боеприпаса вокруг своей оси для поиска целей. В случае их обнаружения происходит отстрел боевых элементов. Впервые для поражения легкобронированной военной техники и живой силы противника БЭ были применены в ходе боевых действий в Ираке в 2003 г. Суббоеприпасами BLU-108/B снаряжаются неуправляемые (CBU-97) и управляемые (CBU-105) авиационные кассеты (по десять боеприпасов) [338].

4.3.3.3. Кинетические боевые элементы

Для поражения расположенных на открытой местности или в легких укрытиях личного состава, техники, складов ГСМ и вооружения, а также для расчистки минных заграждений широко применяются кинетические боевые элементы [338].

Например, в состав снаряжения управляемого авиационного комплекса (УАК) CBU-107PAW (Passive Attack Weapon) входят более 3700, выполненных из высокопрочной стали стреловидных оперенных кинетических бронебойных элементов различных массогабаритных размеров. В их число входят до 350 элементов длиной около 0,36 м, более 1000 длиной 0,17 м и около 2500 длиной 0,06 и 0,05 м. Для обеспечения наибольшей площади поражения их укладка выполнена таким образом, чтобы в первую очередь разбрасывались более тяжелые, а затем – более легкие элементы [95, 338].

4.3.3.4. Унифицированные боевые части

Для оснащения управляемого авиационного оружия класса «воздух – земля» в ВС США широко применяются унифицированные боевые части. К ним, в частности, относятся БЧ калибров 500, 1000 и 2000 фунтов: унитарные осколочно-фугасные (серии Мк) и проникающие (серии BLU). Эти БЧ изготавливаются, хранятся и транспортируются в зависимости от калибра в связках (по две, три, четыре или шесть единиц). Фактически они являются готовыми модулями авиационных бомб. Кроме того, некоторые боевые части без конструктивных доработок устанавливаются в планеры управляемых ракет. Такой принцип модульного построения конструкции авиационного оружия позволяет снизить затраты на производство, эксплуатацию и техническое обслуживание БЧ, а также сократить время подготовки АСП к боевому применению [338].

Сборка конкретного типа авиационной бомбы, которая производится после получения боевой задачи, включает установку стабилизатора заданного типа, а при переоборудовании в управляемый вариант – соответствующей системы наведения. Согласно действующим нормативам в боевых условиях любая БЧ не более чем за 5 мин должна быть оснащена блоком управления серии JDAM (Joint Direct Attack Munitions), а также комплектом системы управления и наведения серии Paveway [338].

4.3.3.5. Проникающие боевые части

По оценкам американских специалистов, до 90% типовых наземных целей, назначаемых к уничтожению в ходе ракетно-бомбовых ударов, представляют собой защищенные укрепленные либо заглубленные объекты со средней или высокой степенью защиты. В

этой связи американские специалисты уделяют особое внимание как совершенствованию существующих, так и разработке новых проникающих БЧ. Для поражения шести основных типов объектов со средней степенью защищенности американские разработчики в дополнение к существующим создали новые унитарные бетонобойные БЧ весом 2000, 1000 и 500 фунтов с повышенной проникающей способностью [338].

В частности, в рамках программы AUP-3 конструкторы фирмы Lockheed Martin создали проникающую БЧ BLU-116/B калибра 2000 фунтов, которой оснащаются УАБ GBU-24, GBU-31 и крылатые ракеты воздушного базирования (КРВБ) AGM-86D. Корпус БЧ BLU-116/B выполнен из никель-кадмиевой стали и при сходных с БЧ BLU-109/B (масса 890 кг, масса ВВ 243 кг, толщина пробиваемого бетонного перекрытия до 2,5 м) массогабаритных характеристиках обладает почти вдвое большей проникающей способностью. Кроме того, БЧ снаряжена меньшим, чем в BLU-109/B, количеством взрывчатого вещества [338].

Для авиации ВМС на базе осколочно-фугасной БЧ Мк-83 калибра 1000 фунтов благодаря снижению массы ВВ и увеличению толщины стенок корпуса для УАБ GBU-32 создана проникающая БЧ BLU-110/B (масса 450 кг, тип ВВ – тритонал или Н6, масса ВВ 190 кг, толщина пробиваемого бетонного перекрытия около 2 м) [338].

Разработана также новая, аналогичная по массогабаритным показателям и проникающей способности БЧ J-1000 (масса 435 кг, масса ВВ – 109 кг) для УАБ GBU-35 и управляемых авиационных ракет AGM-158. Обе БЧ оснащаются высотомером DSU-33 и программируемым взрывателем FMU-152/B с установками на мгновенный взрыв (высота от 1,5 до 11 м) или с временной задержкой (от долей секунды до 24 ч) [338].

Для управляемой авиационной кассеты AGM-154C на базе осколочно-фугасной БЧ Мк-82 калибра 500 фунт разработана проникающая БЧ BLU-111/B такого же калибра (масса 227 кг, тип ВВ – тритонал или Н6, масса ВВ 80 кг, толщина пробиваемого бетонного перекрытия до 1,5 м) [338].

Командование ВВС США проводит мероприятия, направленные на повышение боевой эффективности и пополнение запаса израсходованных во время последних военных конфликтов авиационных бомб с проникающими БЧ, предназначенных для поражения высокозащищенных объектов [338].

К данным БЧ относятся, прежде всего, УАБ GBU-28B/B серии Paveway-3 с полуактивной лазерной головкой самонаведения (носитель – тактический истребитель F-15E Strike Eagle) и GBU-37/B серии JDAM с ИСУ, корректируемой по данным КРНС NAVSTAR (носитель – стратегический бомбардировщик B-2A Spirit), оснащенные наиболее мощной из современных проникающих БЧ BLU-113/B (калибр 5000 фунтов, толщина пробиваемого бетонного перекрытия – 6 м, грунта средней плотности – около 30 м) [338].

В рамках программы модернизации БЧ BLU-113/B создана боевая часть BLU-122/B такого же калибра. Она изготовлена из высокопрочного стального сплава марки ES-1, отличается массивной головной частью корпуса с усовершенствованной формой и снаряжена ВВ повышенной мощности AFX-757, малочувствительным к внешним воздействиям. Эти боевые части комплектуются донными взрывателями FMU-143 или FMU-152, обеспечивающими немедленный подрыв либо подрыв с задержкой по времени, и боковым инерционным предохранительным механизмом. Результаты проведенных стендовых и летных испытаний показали, что по сравнению с боевой частью BLU-113/B новая БЧ имеет увеличенные на 20-25% проникающую способность (толщина пробиваемой железобетонной преграды 7-7,5 м) и на 70% фугасное воздействие. Кроме того, более прочный к механическим воздействиям корпус обеспечивает повышенную на 30% надежность его срабатывания [338].

4.3.3.6. Объемно-детонирующие боевые части

В ряде стран ведутся масштабные работы по совершенствованию оружия объемного взрыва, к которому относятся системы термобарического и вакуумного оружия, обладающие высокими поражающими возможностями [300].

Большую эффективность имеет и вакуумное оружие, в основном пока в виде объемно-детонирующих авиационных бомб (ОДАБ). Принцип их действия в следующем. В носовой части бомбы находится сложное электромеханическое устройство, предназначенное для боевого взвода и распыления взрывчатого вещества. После сброса устройства через установленное время начинается распыление боевого вещества. Полученная аэрозоль преобразуется в газовоздушную смесь, которую потом подрывает взрыватель [300].

ОДАБ предназначены для поражения целей, расположенных в складках местности или в полевых фортификационных сооружениях открытого типа, а также для проделки проходов в заграждениях [300].

В настоящее время в ходе работ, ведущихся по совершенствованию вакуумного оружия, созданы вакуумные бомбы, по своей эффективности и возможностям соизмеримые с ядерными боеприпасами. Достаточно сказать, что такие ОДАБ создают ударную волну с избыточным давлением около 3000 кПа (30 кгс/см). В результате в эпицентре взрыва образуется фактически полностью лишенная воздуха вакуумная среда. Этот перепад давления буквально разрывает изнутри все: личный состав, технику, здания, сооружения и др. При этом действие ОДАБ не загрязняет окружающую среду по сравнению с ядерными боеприпасами [300].

4.3.3.7. Термобарические боевые части

Поражающее воздействие термобарического боеприпаса определяется образованием при его взрыве огненного шара и ударной волны. Термальное поражение при взрыве термобарического боеприпаса в открытом пространстве происходит обычно вблизи взрыва с летальным исходом от ожогов на расстоянии, определяемом размером огненного шара. Летальная зона от ударных ранений превышает зону термальных ранений, но, поскольку воздействие давления снижается с увеличением расстояния от места взрыва, снижаются и летальные ударные воздействия [300].

Целевой эффект применения термобарических боеприпасов изменяется кардинально, когда они используются в ограниченном пространстве. Огненный шар и ударная волна могут огибать углы и проникать туда, куда не могут проникнуть осколки, которые могут быть остановлены стенами, мешками с песком и средствами личной защиты. В связи с этим личный состав, находящийся в ограниченном пространстве, подвергается воздействию давления значительно большего уровня, чем на таком же расстоянии от взрыва в открытом пространстве. Вот почему это оружие наиболее эффективно применяется для поражения бункеров, строений, пещер, тоннелей и т.п. [300].

Высокая эффективность поражающего воздействия термобарического оружия учитывается при разработке новых, более эффективных взрывчатых композиций, переходе от жидких рецептур к твердым, созданию новых термобарических систем (бомб, гранатометов, реактивных установок, ракет и др.) [300].

Так, в целях обеспечения более эффективного поражения живой силы противника, находящейся в высокозащищенных и заглубленных фортификационных или естественных укрытиях, в США создана термобарическая боевая часть BLU-118/B [338].

Основными отличиями термобарической БЧ от объемно-детонирующей являются сниженное потребное количество атмосферного кислорода для детонации заряда и повышенная стойкость к ударным внешним воздействиям, что позволяет применять их в проникающих корпусах. В снаряжение термобарической БЧ входят порошкообразная металлизированная смесь, взрывчатое вещество с пониженной скоростью детонации, а также окислительные компоненты [338].

4.3.3.8. Боевые части для поражения объектов по производству и хранению химического и биологического оружия

В зарубежных СМИ отмечается, что в США особое внимание уделяется созданию проникающих БЧ, предназначенных для поражения объектов, связанных с производством и хранением химического и биологического оружия.

Так, в рамках программы Vulcan Fire, реализуемой командованием ССО ВВС США, разработана высокотемпературная зажигательная смесь, которой будет снаряжаться БЧ J-1000. При пробитии боевой частью преграды в зависимости от времени установки программируемого взрывательного устройства происходит выброс зажигательных контейнеров. В результате химической реакции, сопровождаемой повышением температуры до 1500°С в течение 15 мин, выделяются атомарные хлор и фтор, а также хлор- и фтороводородные кислоты. Предполагается, что в условиях высокой температуры выделяемые продукты способны нейтрализовать химическое или биологическое оружие, а относительно малое избыточное давление исключает выброс веществ на поверхность. Разрушение контейнеров с ОВ или агентами биологического оружия обеспечивается входящими в состав БЧ специально разработанными осколочными элементами [338].

4.3.3.9. Тандемные боевые части

Специалистами франко-германской фирмы TDA/TDW по заказу министерства обороны Германии была разработана тандемная бе-

тонобойная БЧ Effector для авиационных УР KEPD 350. Ее конструкция включает следующие основные элементы: кумулятивный заряд, проникающую боевую часть, оптоэлектронный неконтактный датчик и взрывательные устройства для обоих зарядов. Использование кумулятивного заряда обеспечивает начальную фазу поражения бетонной преграды. Его подрыв осуществляется на установленном от поверхности преграды расстоянии при помощи взрывательного устройства по данным входящего в его состав оптоэлектронного неконтактного датчика. Корпус проникающей БЧ выполнен из высокопрочного сплава на основе вольфрама. Детонация размещенного в нем заряда взрывчатого вещества производится после попадания внутрь объекта при помощи программируемого взрывательного устройства PIMPF (Programmable Intelligent Multi-Purpose Fuze). Оно распознает преграды разного типа путем сравнения данных, имеющихся в его базе данных, с поступающими от акселерометра, измеряющего ускорение с момента удара. Это позволяет определить время подрыва с учетом пробития заданного количества преград (перекрытий) различной плотности и твердости, а также пройденного расстояния. Взрывательное устройство может быть запрограммировано до вылета самолета или непосредственно перед применением боеприпаса на наземный (для уничтожения площадных целей) или подземный подрыв [338].

Подобные боеприпасы, BROACH (Bomb Royal Ordnance Augmented Charge) и Lancer, разработаны также британскими фирмами British Aerospace и Thomson Torn соответственно. В частности, создано несколько вариантов боеприпаса BROACH диаметром 450 мм (для оснащения франко-британских авиационных УР SCALP/Storm Shadow), 300 мм (планировалось к оснащению УАК AGM-154C) и 127 мм (под 155-мм артиллерийский снаряд) [338].

Главными преимуществами тандемных проникающих БЧ перед унитарными такой же массы считаются вдвое-втрое повышенная энергия, из которой до 70% приходится на кумулятивную БЧ, и меньший занимаемый объем. Однако на основе анализа результатов испытаний британских тандемных БЧ в корпусах американских КРВБ AGM-86 и УАК AGM-154, а также боевого применения британской УР Storm Shadow выявлено, что боевая эффективность таких БЧ ниже, чем унитарных. Это обусловлено, в первую очередь, недостаточной надежностью срабатывания существующих оптоэлектронных неконтактных датчиков и взрывательных устройств для обоих зарядов [338].

Таким образом, вышеприведенный анализ показал, что совершенствование существующих и создание новых, относительно деше-

вых высокоэффективных боевых частей со сниженными массогабаритными показателями позволит улучшить тактико-технические характеристики ВТО.

4.3.4. Системы противоракетной обороны (на примере систем ВС США)

4.3.4.1. Общая характеристика системы ПРО США как основного элемента защиты от высокоточного оружия

Развитие ВТО идет параллельно с созданием эффективных систем ПВО и ПРО, превращая их в единый комплекс. Опыт войны Израиля против «ХАМАС» в ноябре 2012 г. показал, что с помощью ВТО можно уничтожить политико-военное руководство и наступательные вооружения даже в защищенных объектах, а с помощью систем ПРО – перехватить до 90% средств нападения, достигнув в итоге главной военной цели – «разоружения» противника. Это, конечно, не означает всегда политической победы, которая определяется не только военными результатами (как и в случае палестино-израильской войны 2012 г.), но, очевидно, предопределяет такую политическую победу [337].

Противоракетная оборона (ПРО) – комплекс мероприятий разведывательного, радиотехнического и огневого характера, предназначенный для защиты объектов от ракетного оружия, в том числе и ВТО. ПРО очень тесно связана с ПВО и часто осуществляется одними и теми же комплексами.

ПРО включает в себя защиту от ракетной угрозы, однако, говоря о ПРО, как правило, имеют в виду «стратегическую ПРО» – защиту от массированного применения МБР и ВТО в рамках реализации стратегии быстрого глобального удара.

В настоящее время работы по созданию стратегической ПРО активно ведутся в США. Цель этих работ – обезопасить территорию США от внезапного массового применения МБР и ВТО. Пентагон продолжает реализовывать программу создания многоэшелонной глобальной системы ПРО с размещением ее составляющих и в европейской части (так называемый «поэтапный адаптивный подход» к региональной ПРО, или ПРО на ТВД).

Система национальной ПРО США – это комплексная система обнаружения, отслеживания и перехвата баллистических ракет раз-

личных классов, предназначение которой – защита территории США, а также их союзников и передовых военных баз от ракетных ударов ограниченной мощности – таких, которые потенциально могли бы нанести как Россия и Китай, так и «страны-изгои», к которым в США относят: КНДР, Иран и Сирию (ранее также Ирак и Ливию).

Система ПРО США представляет собой комплекс, состоящий:

- из РЛС раннего предупреждения о ракетном нападении;
- из спутников слежения за запусками ракет;
- из пусковых установок и станций наведения ракет- перехватчиков наземного и морского базирования, предназначенных для уничтожения боевых блоков баллистических ракет малого, среднего и межконтинентального радиуса действия как в космическом пространстве, так и в атмосфере на разных участках траектории.

Основные мероприятия по развертыванию ПРО изложены в директиве президента США «Национальная политика США в области противоракетной обороны». В соответствии с данным документом и общей концепцией стратегической ПРО ее основными боевыми составляющими являются [95]:

- наземный компонент GBMD;
- морской (корабельный) компонент SBMD – Aegis combat system;
- противоракетный комплекс сухопутных войск THAAD;
- войсковой компонент объектовой ПВО/ПРО «Пэтриот-3» (Patriot PAC-3);
- лазерные воздушные компоненты (в настоящее время работы по созданию лазерных средств ПРО на основе Boeing B-747 прекращены в связи с их низкой перспективностью).

Освоение программы создания многоэшелонной системы ПРО, по мнению аналитиков США, позволит осуществлять заатмосферный перехват и уничтожение боеголовок баллистических ракет наземного, воздушного и морского базирования, оснащенных средствами преодоления противоракетной обороны, а так же недопущение конечного поражения стратегически важных целей на территории США и их союзников [95].

Принцип эшелонирования, заложенный в основу системы ПРО, предусматривает разработку и развертывание (рис. 4.15) [286]:

- средств перехвата баллистических целей на конечном участке траектории;

- средств перехвата баллистических целей на среднем участке траектории;
- средств перехвата баллистических целей на активном участке траектории;
- системы боевого управления и связи;
- информационно-разведывательных средств.

Рис. 4.15. Перехват ракет на различных участках ее траектории [396]

В настоящее время ведется поэтапный подход к развертыванию системы ПРО (рис. 4.16). По заявлению официальных лиц Пентагона, элементы глобальной системы ПРО развернуты в Азии (Япония, Южная Корея, Австралия), на Ближнем Востоке (Израиль, Турция), в районе Персидского залива (государства – участники Совета сотрудничества арабских государств). По сообщениям зарубежной печати рассматривается вопрос о размещении РЛС в интересах ПРО на территории Турции или Азербайджана.

Кроме того, ведется развертывание системы ПРО в Европе, которое предусматривает реализацию мероприятий в течение четырех этапов [95].

1. На первом этапе (2011-2016 гг.) планируется постоянно иметь в европейских водах на боевом дежурстве 3 боевых корабля с серийно выпускаемыми морскими противоракетами Standard Missile 3 (SM-3), а для обнаружения ракет – новые мобильные РЛС большой дальности.
2. В течение второго этапа (с 2016 г.) намечается заменить существующие противоракеты более эффективными, а также развернуть на Европейском континенте наземные комплексы ПРО с использованием противоракет SM-3 и более совершенные системы обнаружения.
3. К третьему этапу намечено приступить в 2018 г. При этом планируется принять на вооружение морских и наземных

комплексов ПРО новую противоракету SM-3 Blok IIA, способную поражать широкий спектр баллистических целей, включая баллистические ракеты средней дальности. Предполагается, что применение SM-3 Blok IIA и наращивание количества комплексов позволит, начиная с 2018 г., обеспечить полную защиту всей территории Европы от гипотетических иранских ракет.

4. На четвертом этапе (ориентировочно 2020 г.) планируется поставить на вооружение разработанную к тому времени еще более эффективную противоракету SM-3, которая должна обладать способностью поражать даже межконтинентальные баллистические ракеты.

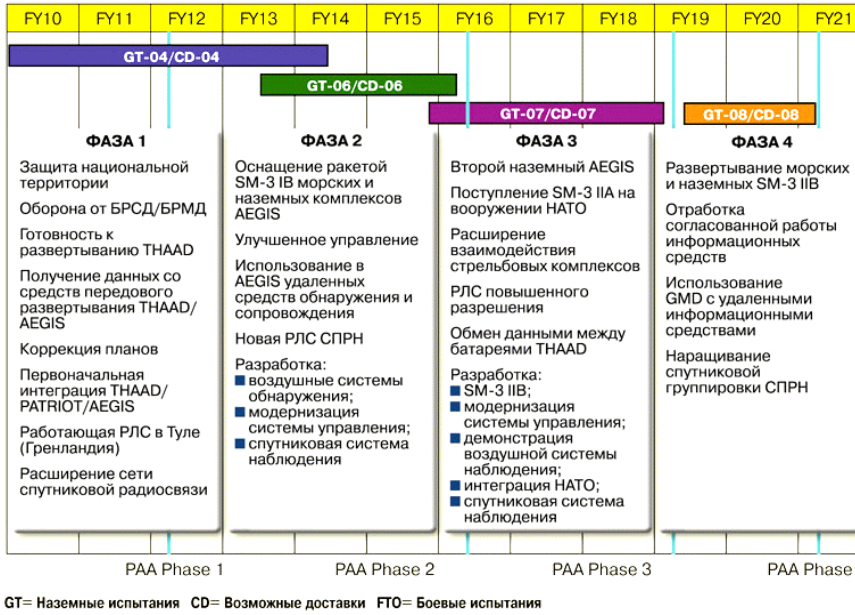


Рис. 4.16. Поэтапный подход к развертыванию системы ПРО [365]

Ниже боле подробно представленны составляющие стратегической ПРО.

4.3.4.2. Наземная система GBMD

Наземная система противоракетной обороны на среднем участке траектории GBMD (Ground-Based Midcourse Defense) – американский комплекс ПРО, введенный в строй в 2005 г. Предназначен для перехвата межконтинентальных баллистических ракет и их боевых частей в космическом пространстве за пределами атмосферы Земли.

Комплекс стратегической ПРО США, исходно получивший название NMD (National Missile Defense), был предназначен для решения технически наиболее сложной задачи – перехвата боевых частей МБР за пределами атмосферы на основном участке их траектории. Так как МБР движутся наиболее быстро по сравнению с другими видами баллистических ракет, для гарантии эффективной защиты требовалось обеспечить поражение боевых блоков до входа в атмосферу, на среднем (проходящем в космическом пространстве) участке траектории. В 2002 г., в связи с интеграцией в NMD других элементов, в том числе системы ПРО на базе флотской БИУС Aegis, комплекс был переименован в GBMD.

Основной задачей комплекса GBMD является перехват в космическом пространстве моноблочных МБР. Комплекс должен решать задачи своевременного обнаружения стартующих баллистических ракет, отслеживания их в космосе, наведения на цель противоракет и поражения боеголовок за пределами атмосферы. В качестве средства поражения был избран кинетический перехватчик, уничтожающий цель лобовым столкновением. Американскими специалистами было доказано, что кинетический перехват более эффективен для целей ПРО, чем предлагавшиеся в 1970-х противоракеты с ядерными зарядами, так как при кинетическом перехвате не образуется электромагнитная вспышка, мешающая работе наземных радаров.

Элементы комплекса GBMD:

- наземная система РЛС ракетного обнаружения PAVE PAWS (Precision Acquisition Vehicle Entry Phased Array Warning System);
- ракеты-перехватчики GBI (Ground-Based Interceptor).

Кроме того, комплекс GBMD в ближайшем будущем предполагается дополнить информационной поддержкой от развертываемой космической системы раннего обнаружения пусков баллистических ракет SBIRS (Space-Based Infrared System).

Три стационарных РЛС PAVE PAWS являются основой информационного обеспечения системы GBMD, осуществляющей обна-

ружение и отслеживание угрожающих территории США космических объектов. Расположенные на стратегически важнейших направлениях, радары осуществляют непрерывный контроль аэрокосмического пространства, отслеживание перемещающихся в космосе объектов и вторичное предупреждение о ракетном нападении на подступах к Северной Америке.

Каждая РЛС представляет собой тетраэдрическое сооружение с двумя установленными на нем неподвижными фазированными антеннами. Угол обзора РЛС составляет порядка 240° по горизонтали и от 3° до 85° по вертикали. Сектора обзора радарных станций пересекаются на флангах и обращены от континентальной территории США. Радиус действия радаров составляет порядка 2000 км, что позволяет им эффективно отслеживать в космическом пространстве приближающиеся цели.

Сектора обзора станций системы PAVE PAWS (выделены синим) и более ранней системы предупреждения о ракетном нападении BMEWS [Ballistic Missile Early Warning System] (выделены красным) представлены на рис. 4.17.

Рис. 4.17. Сектора обзора станций системы PAVE PAWS

Несмотря на широкие возможности системы станций PAVE PAWS, у этих РЛС есть существенный недостаток. Их радиус действия составляет не более 2000 км, что не позволяет им обнаруживать и сопровождать ракеты на ранних участках траектории. Это не дает возможности в полной мере реализовать оборонительный потенциал системы GBMD, технически способной (при наличии целеуказания) поражать цели в космическом пространстве над любой точкой Земли. Чтобы решить эту проблему, была разработана мобильная РЛС морского базирования (на основе буровой платформы MOSS CS-50Mk II «Полярная звезда»), работающая в X-диапазоне, способная отслеживать цели в околоземном пространстве на расстоянии в 2000-4700 км. Основной функцией данной РЛС является перемещение в случае возникновения конфликтной ситуации в район потенциального запуска МБР. Эта РЛС морского базирования может отследить запуск ракет на самом раннем участке траектории и выполнить наведение против них противоракет GBI, базирующихся на наземных базах на континентальной территории США. Дальность перехвата, таким образом, становится почти неограниченной – развернутая в соответствующей точке платформа может навести противоракету на космический объект в любой точке мира.

Дополнительно к наземным РЛС PAVE PAWS в США ведутся работы по развертыванию двухкомпонентной комплексной космической системы раннего обнаружения пусков баллистических ракет SBIRS. Она должна сменить систему раннего оповещения о пусках МБР дальнего действия DSP (Defense Support Program), которая создавалась еще в 1970 г. как система стратегического наблюдения. Система SBIRS использует для определения запусков инфракрасные датчики, настроенные на параметры стартов ракет. Кроме контроля запусков ракет она предназначена для определения траектории их полета, идентификации боевых частей и ложных целей, выдачи целеуказания для перехвата, а также ведения разведки над территорией военных действий в инфракрасном диапазоне. Первоначально предполагалось, что система будет состоять из двух компонентов:

- SBIRS High – группировки космических аппаратов с инфракрасным оборудованием на борту на геостационарной (SBIRS-GEO) и высокоэллиптической (SBIRS-HEO) орбитах;
- SBIRS Low – группировки космических аппаратов на низкой околоземной орбите.

Однако, несмотря на то, что работы по созданию SBIRS были начаты еще в середине 90-х гг. и должны были завершиться в 2010 г., на 2013 г. на орбиту выведены только 2 спутника верхнего эшелона на эллиптических орбитах и 2 геостационарных спутника.

В рамках программы SBIRS Low предполагалось создать группировку из 24 низкоорбитальных спутников, предназначенных для отслеживания баллистических ракет, выявления боеголовок, ложных целей на различных участках полета. Программа должна была начать развертывание в 2010 г., но была досрочно свернута. В 2001 г. на основе системы SBIRS Low была создана новая программа – космическая система слежения и видеонаблюдения STSS (Space Tracking and Surveillance System). В рамках этой программы в 2009 г. для демонстрации предложенных технологий были запущены 3 спутника.

Основным оружием комплекса GBMD является ракета-перехватчик наземного базирования GBI, размещаемая в подземных шахтах. Противоракета GBI представляет собой трехступенчатую твердотопливную ракету, размещаемую в подземных шахтах. Максимальная высота запуска 2000 км. Расчетная дальность действия ракеты варьируется в зависимости от высоты траектории и составляет от 2000 до 5500 км. Противоракета разгоняется до скорости 8,3 км/с и выбрасывает в космическое пространство перехватчик EKV (Exoatmospheric Kill Vehicle) – искусственный спутник массой 64 кг и длиной 1,4 м [95].

Следует особо отметить, что, так как скорость выводимого в космическое пространство перехватчика может превысить первую космическую, традиционный термин «дальность действия» для GBI неприменим в полной мере – теоретически перехватчик может перехватить цель в любой точке орбиты. Практически дальность действия перехватчика ограничена временем реакции системы GBMD на приближающиеся баллистические ракеты [95].

При этом, по оценкам специалистов, загрузка ракет GBI в шахты занимает 24-26 ч, а замена боеголовок на этих ракетах, превращающая их из оружия обороны (противоракет) в наступательное ядерное оружие, – еще меньший промежуток времени [95].

Основным поражающим элементом ракеты-перехватчика GBI является заатмосферный кинетический перехватчик EKV. Он оснащен электронно-оптической системой наведения, защищенной от посторонней засветки особым кожухом и автоматическими фильтрами. Получая целеуказание с наземной части системы GBMD, перехватчик EKV обнаруживает с помощью инфракрасного телескопа цель и, ма-

неврируя жидкостным двигателем, начинает разгон для ее поражения. Поражение боеголовки осуществляется лобовым тараном на встречном курсе, при этом в момент столкновения с целью скорость EKV составляет порядка 7 км/с, таким образом, кинетической энергии удара вполне хватает, чтобы полностью уничтожить боевой блок [95].

В отличие от шрапнельных зарядов кинетический перехватчик при попадании полностью уничтожает боеголовку. То есть при его применении невозможна неопределенная ситуация, когда боеголовка, выведенная из строя шрапнельным снарядом, остается единым целым и продолжает полет по прежней траектории. Кроме того, кинетическое поражение не создает значительных облаков обломков, способных нанести вред другим космическим аппаратам [140].

Рис. 4.18. Планируемое размещение ракет SM-3
на территории Румынии и Польши и перехват ими МБР

Первоначально в рамках программы GBI планировалась разработка кластерного перехватчика, предназначенного для поражения головок от МБР с разделяющимися боеголовками. Согласно проекту противоракета GBI должна была выводить на орбиту несколько ком-

пактных миниатюрных перехватчиков MKV (Multiple Kill Vehicle), наводящихся одновременно на несколько целей. Однако в связи с рядом технологических трудностей и необходимостью сокращения бюджета США программа GBI с MKV была закрыта в 2009 г.

С июня 1997 г., когда начались первые тестовые пуски GBI, и по 2016 г.было осуществлено 37 тестовых запусков. 17 из них были предприняты с целью перехвата учебных мишеней (остальные – для отработки различных компонентов и проверки оборудования). Из 17 пусков, осуществлявшихся по учебным целям, полностью успешными были 8, что составляет порядка 47%. Однако в одном случае провал испытаний произошел по вине вышедшей из строя учебной цели. Из 16 же случаев, когда цель отработала нормативно, было осуществлено 8 успешных перехватов, что составляет 50%, а это близко к расчетной эффективности комплекса [284].

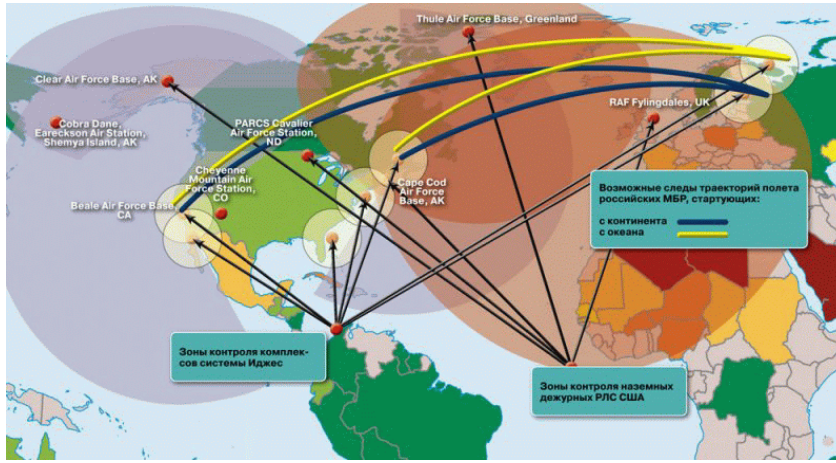


Рис. 4.19. Вариант перехвата МБР,
запускаемых из европейской части России

В настоящее время размещение 30 противоракет GBI осуществлено в двух позиционных районах – на Аляске (Fort Greely) и в Калифорнии (авиабаза Vandenberg). Третий позиционный район Пентагон планировал создать на территории Польши, разместив на территории площадью около 275 га позиции (подземные шахтные установки) для 10 противоракет, а также в Чехии, где на территории в 30 га предполагалось разместить РЛС ПРО. РЛС в Чехии, по заключению экспертов, давала возможность контролировать пуски МБР из России

в направлении Восточного побережья США с последующим их перехватом противоракетами GBI, а безопасность Западного побережья обеспечивали противоракеты, размещенные на Аляске.

Однако в 2009 г. под давлением России планы развертывания системы GBMD в Польше были отменены и заменены планами развертывания наземной версии системы ПРО Aegis. В 2013 г. США заявили о переориентации своих усилий в области ПРО на Азиатско-Тихоокеанский регион. В конце 2014 г. на саммите АТЭС президент США Б. Обама предлагал развернуть ПРО коалиции стран АТР в качестве сдерживающего фактора для КНДР и Китая [285].

4.3.4.3. Морская система SBMD на основе боевой информационно-управляющей системы «Aegis»

Aegis («Иджис») – американская корабельная многофункциональная боевая информационно-управляющая система (БИУС), представляющая собой интегрированную сеть корабельных средств освещения обстановки, средств поражения, таких как зенитные управляемые ракеты SM-2 (Standard Missile-2) и более современные SM-3 (Standard Missile-3), а также автоматизированные системы боевого управления. Aegis является составной частью системы SBMD (Sea-Based Midcourse Defens) стратегической ПРО США [95, 227].

Система Aegis предназначена для поражения самолетов, противокорабельных ракет и баллистических ракет малой дальности. Aegis считается морским компонентом американской национальной системы ПРО, которая дополняет систему GBMD в противоракетных операциях действиями с морских и океанских позиционных районов и оценочно перекрывает высоты в диапазоне 150-1000 км от поверхности Земли [95, 227].

Система Aegis позволяет принимать и обрабатывать информацию с датчиков других кораблей и летательных аппаратов соединения и выдавать целеуказания на их пусковые установки. Наименование Aegis носит также ЗРК, применяемый в составе этой БИУС.

Работы по созданию Aegis, предназначенной для уничтожения самолетов и ракетного оружия классов «воздух-корабль» и «корабль-корабль», начались в декабре 1969 г. Первый корабль, оснащенный системой Aegis, – ракетный крейсер типа Ticonderoga (CG-47), который зачислен в списки флота в январе 1983 г. В последующие годы система неоднократно подвергалась глубокой модернизации с целью

повышения эффективности ее информационно-разведывательной и ударно-боевой составляющих.

Основным элементом системы Aegis является РЛС кругового обзора AN/SPY-1 модификаций A, B или D с четырьмя фазированными антенными решетками общей средней излучаемой мощностью 32-58 кВт и пиковой мощностью 4-6 МВт. РЛС способна осуществлять автоматический поиск, обнаружение, сопровождение 250-300 целей и наведение по наиболее угрожающим из них до 18 ЗУР. Компьютерные системы управления и поддержки принятия решения являются ядром Aegis. Они позволяют одновременно решать задачи противовоздушной, противолодочной обороны и наносить удары по кораблям противника. Это позволило системе Aegis устойчиво сопровождать и поражать некоторые низколетящие цели, а также ВТО, пикирующее на АУГ с углами до 85-90 градусов. При этом решение на поражение угрожающих кораблю целей может приниматься автоматически. Пуск ракет может производиться универсальными установками вертикального пуска Mk 41, располагаемыми под основной палубой крейсеров и эсминцев [227].

Основным вооружением системы Aegis являются корабельные трехступенчатые ракеты SM-3 (Standard Missile-3) компании Boeing. Две маршевые ступени ракеты состоят из блоков-ускорителей, что позволяет ей развивать более высокую скорость. Третья ступень ракеты SM-3 – разгонная [95].

Если более старые ракеты-перехватчики SM-2 Block IV используются для поражения баллистических ракет в атмосфере на заключительном этапе их полета, и их боевая часть оснащается осколочным боезарядом с обычным взрывчатым веществом, то ракета-перехватчик SM-3 уничтожает баллистические ракеты, находящиеся в средней части траектории и летящие за пределами атмосферы, с помощью кинетической боеголовки, путем ударно-контактного взаимодействия [95].

Обнаружив цель, РЛС AN/SPY-1 непрерывно сопровождает ее, передавая данные боевой информационной системе Aegis, которая вырабатывает решение на поражение и дает команду на запуск ракеты. Противоракета SM-3 запускается из ячейки с помощью твердотопливного стартового ускорителя Aerojet, устанавливает двусторонний канал цифровой связи с кораблем-носителем и непрерывно получает от него поправки по курсу. Текущее положение противоракеты устанавливается с высокой точностью при помощи системы GPS. Работа трех ступеней SM-3 позволяет вывести ракету на встречную траекторию и

обеспечивает набор достаточной скорости для поражения цели. На конечной фазе полета отделяется заатмосферный малогабаритный кинетический перехватчик (Lightweight Exo-Atmospheric Projectile), который начинает самостоятельный поиск цели с помощью данных с корабля-носителя и собственной инфракрасной ГСН. Цели могут обнаруживаться на дальностях до 300 км, а коррекция траектории может составлять до 3-5 км. Кинетический перехватчик имеет собственные двигатели для корректировки полета и космического маневрирования, которые осуществляют точное выведение перехватчика на встречный курс. При столкновении энергия удара перехватчика составляет 130 МДж, что более чем достаточно для уничтожения любой баллистической цели [229].

Морская система Aegis на испытаниях противоракет SM-3 показала способность успешно перехватывать баллистические ракеты, крылатые ракеты воздушного базирования и групповые цели (баллистические ракеты средней дальности в сочетании с крылатыми ракетами воздушного базирования) не только на конечном, но и на среднем участке их траектории [95].

Всего в 4 испытательных пусках SM-3, проведенных в 2001-2002 гг., был достигнут успешный перехват имитатора боевого блока баллистической ракеты в космосе на высотах 240-250 км. 11 декабря 2003 г. с эсминца USS Lake Erie была сбита цель на высоте 137 км при общей скорости сближения 3,7 км/с, вся операция от обнаружения до перехвата заняла 4 мин. 21 февраля 2008 г. ракета SM-3 была выпущена с крейсера Lake Erie в Тихом океане и через 3 мин после старта поразила находящийся на высоте 247 км аварийный разведывательный спутник USA-193, двигающийся со скоростью 7580 м/с. Очередное пробное тестирование модернизированной SM-3, проведенное 16 апреля 2011 г., показало высокую эффективность комплекса по перехвату ракет средней дальности [95].

В 2018 г. корабельные противоракеты SM-3 следующего поколения предусматривается адаптировать к наземному способу базирования. Эти ракеты будут предназначены для перехвата баллистических ракет на восходящем (до начала разделения боеголовок) и нисходящем участках траектории полета на дальности до 1000 км и высотах 70-500 км. В апреле 2011 г. агентство ПРО США объявило о подписании контрактов по разработке более совершенной модификации ракеты-перехватчика SM-3, предназначенной для перехвата и уничтожения на активном участке траектории МБР с дальностью пуска до 12 000 км. Развертывание новых противоракет намечено на 2020 г. Для повыше-

ния эффективности применения противоракет SM-3, в том числе наземного базирования, предполагается использовать разрабатываемые авиационные инфракрасные средства обнаружения и сопровождения целей, установленные на средневысотных многоцелевых БПЛА MQ-9 Reaper. В качестве пунктов управления огнем разработчики предусматривают использовать командный пункт противоракетного комплекса сухопутных войск THAAD (дальность перехвата до 200 км на высотах от 40 до 150 км), который включает в себя размещенные на шасси многоцелевых автомобилей повышенной проходимости типа Humvee кабины боевого управления и управления пуском [95, 228].

По мнению ряда аналитиков, именно такие модернизированные противоракеты SM-3 наземного и морского базирования наряду с противоракетными комплексами сухопутных войск THAAD составят основу боевых элементов так называемого поэтапного адаптивного подхода США по созданию европейского сегмента системы ПРО. В связи с тем, что, по мнению американских специалистов, государства, несущие угрозу США (Иран, КНДР и др.), в отдаленной перспективе смогут обладать МБР, а широкое распространение баллистических ракет малой и средней дальности признано реальной угрозой, основное внимание уделено массовому развертыванию мобильных противоракетных средств, способных эффективно им противодействовать. В данных условиях предполагается осуществлять массовое развертывание модернизированных компактных и легких противоракет SM-3, имеющих значительный потенциал, а также системы Aegis в вариантах морского и наземного базирования. Главное преимущество этого оружия, по утверждению экспертов, – это мобильность. Именно высокая мобильность SM-3 как в корабельной, так и в наземной модификациях в сочетании с размещением РЛС системы предупреждения о ракетном нападении на плавучих платформах позволит Пентагону оперативно реагировать на обстановку, перенося усилия с одного ТВД на другой [95].

В конце 2011 г. ВМС США имели в общей сложности 24 корабля, оснащенных БИУС Aegis, в том числе пять ракетных крейсеров типа Ticonderoga и 19 эсминцев типа Arleigh Burke. В процессе реализации долгосрочной программы развития системы Aegis ею планируют оснастить 22 ракетных крейсера и практически все эсминцы с ракетным вооружением – 62 единицы. Долгосрочная кораблестроительная программа ВМС, которая будет реализована до 2041 г., предусматривает модернизацию под указанную систему до 84 таких кораблей [287].

К 2015 г. в Румынии на территории военно-воздушной базы Deveselu на юге страны планировалось разместить около 200 американских военнослужащих и развернуть три мобильные батареи с 24 пусковыми установками SM-3, по поводу чего 14 сентября 2011 г. был подписан соответствующий межгосударственный договор между США и Румынией. Кроме того, в качестве мест вероятного развертывания стартовых позиций рассматриваются также территории Польши, Чехии и Турции. Возможность включения данных противоракет в систему своей национальной ПРО изучает и Израиль [95].

4.3.4.4. Комплекс ПРО сухопутных войск THAAD

Для решения задач в интересах ПРО на ТВД предназначен усовершенствованный зенитный ракетный комплекс Patriot PAC-3 (Patriot Advanced Capability-3) и противоракетный комплекс мобильного наземного базирования высотного перехвата сухопутных войск THAAD [95].

THAAD (Terminal High Altitude Area Defense) – комплекс ПРО подвижного наземного базирования для высотного заатмосферного перехвата ракет средней дальности.

Комплекс THAAD, является авиатранспортабельным, он предназначен для поражения оперативно-тактических ракет на дальностях до 1000 км, баллистических ракет средней дальности (БРСД) на расстоянии до 3500 км на высотах от 40 до 150 км. Следует отметить, что комплексы THAAD также предполагалось использовать в системе национальной ПРО США для уничтожения тех целей, которые прошли рубеж обороны GBI, однако их возможности по перехвату МБР значительно ниже [95].

В комплексе THAAD так же, как и в других американских системах ПРО, применена концепция кинетического перехвата – для поражения цели используется кинетическая энергия аппаратного блока. Отдельно выделенной боевой части нет. Благодаря высокой кинетической энергии аппаратного блока, комплекс THAAD должен быть существенно более эффективным против устаревших баллистических ракет (типа Р-17), чем ЗРК Patriot вариантов PAC-1 и PAC-2. При этом одной ракетой возможно уничтожение лишь одиночной цели, траектория которой известна с заданной точностью.

Некоторые специалисты отмечают, что концепция прямого попадания ограничивает возможность противодействия комплекса THAAD сложным баллистическим целям, а возможность противодей-

ствия скоростным маневрирующим целям является сомнительной. Также сомнительной является возможность прямого попадания в цель в условиях активного применения средств РЭБ и в сложной помеховой обстановке.

РЛС комплекса THAAD на основе АФАР имеет дальность обнаружения 1000 км.

Противоракета THAAD является одноступенчатой твердотопливной и снабжена неохлаждаемой ИК ГСН, работающей в среднем (3,3-3,8 мкм) и дальнем (7-10 мкм) участках ИК-диапазона, а также командно-инерциальной системой управления. Дальность ракеты – до 200 км, высота перехвата 150-200 км, скорость ракеты 3 км/с, дальность пуска перехватываемой баллистической ракеты – до 3500 км.

НИОКР по созданию комплекса ПРО THAAD были начаты в 1992 г. корпорацией Lockheed Martin. Было проведено эксплуатационное испытание системы с перехватом ракет на большой высоте на заключительном этапе их траектории. Были успешно перехвачены одна ракета малой дальности и одна баллистическая ракета средней дальности.

4.3.4.5. Зенитно-ракетный комплекс ПВО-ПРО Patriot PAC-3

Комплект MIM-104 Patriot – американский ЗРК, используемый армией США в качестве основной платформы воздушной защиты на средних и больших высотах. В дополнение к этому, Patriot играет роль платформы перехвата баллистических ракет, причем эта роль сегодня является ключевой задачей комплекса. ЗРК Patriot состоит из ракеты воздушного перехвата и высокопроизводительной радарной системы. В настоящий момент эксплуатируется усовершенствованная версия системы – Patriot PAC-3.

Наведение ракеты MIM-104 на цель осуществляется стандартным способом – радиокомандным управлением с земли, с помощью метода «слежения через ракету». Летящая ракета принимает отраженный от цели сигнал наземной РЛС и ретранслирует его по одностороннему каналу связи на командный пост. Управляющий компьютер сопоставляет данные, полученные от наземной РЛС и от самой ракеты, и вырабатывает поправки к траектории, направляя ракету на цель.

Особенностью режима ПРО в PAC-3 является необходимость в специальном спутнике, который находится на орбите. Этот спутник

должен заранее сообщать на локационную станцию РАС-3 координаты ракеты и траекторию ее полета, что занимает порядка 90 с.

Таким образом, США активно наращивают возможности и численный состав стратегической ПРО. По сведениям СМИ США, в начале 2010 г. отдельные элементы системы ПРО были развернуты [95]:

- в сухопутных войсках – от 575 до 600 подвижных пусковых установок РАС-3 и 24 наземные ракеты-перехватчики GBI, в том числе 21 – в штате Аляска и 3 – в штате Калифорния;
- в военно-воздушных силах – радиолокационные станции на 3 постах (в Великобритании, штатах Калифорния и Аляска);
- в военно-морских силах – радиолокационные станции и противоракеты SM-3 на 18 ракетных крейсерах и эсминцах управляемого ракетного оружия.

Подводя итоги анализа путей развития ВТО и средств ПРО, можно сделать вывод, что роль высокоточного оружия в решении задач военных конфликтов последнего десятилетия заметно увеличилась. Учитывая перспективы его развития в начале XXI века, можно с уверенностью утверждать, что оно будет оказывать определяющее влияние на формирование характера вооруженной борьбы не только в воздушной, но и в воздушно-космической сфере [300].

4.4. Космические средства и оружие

4.4.1. Общая характеристика тенденций развития космических систем и средств

Недавние войны в Югославии, Афганистане и Ираке наглядно продемонстрировали асимметричное преимущество, предоставляемое космическими средствами на поле боя, независимо от того, ведутся ли боевые действия в пустыне, в горных районах или в крупных городах. Космические средства предоставляли вооруженным силам возможность применять ударные системы ВТО с высокой точностью и при минимальных сопутствующих разрушениях, сводя к минимуму необходимость применения ядерного оружия (рис. 4.20).

Ведущие технически развитые государства, прежде всего США, рассматривают космические средства как важнейший элемент

обеспечения боевых действий и применения современного оружия, в том числе и ВТО.

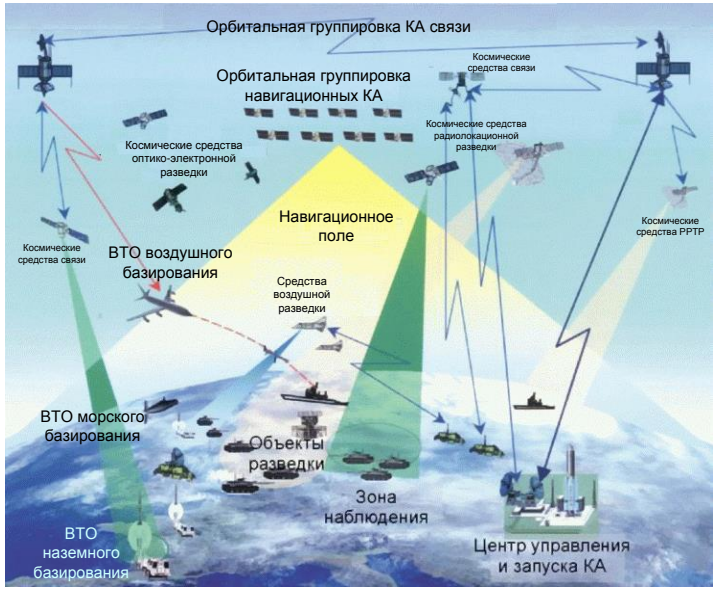


Рис. 4.20. Космическое обеспечение применения средств ВТО

Активное использование космического пространства в военных целях может обеспечить [126, 269]:

- контроль использования другими странами космического пространства, а также суши, акваторий морей и океанов Земли;
- получение полной и достоверной информации о противнике в масштабе времени, близком к реальному, и оперативное доведение ее до всех органов управления и элементов войск (сил);
- развертывание сил и систем ВТО, способствующих достижению военных целей с минимальными потерями и минимальным ущербом для гражданского населения и окружающей среды;
- защиту национальной территории и развернутых группировок войск от оружия массового поражения и ударов средств воздушно-космического нападения, в первую очередь баллистических и крылатых ракет (рис. 4.21 и 4.22).

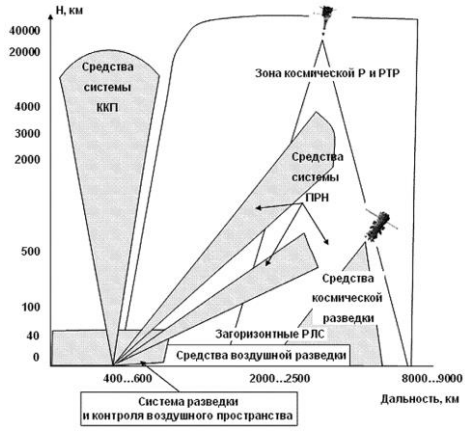


Рис. 4.21. Зоны обнаружения воздушно-космических целей различными системами и средствами разведки [269]

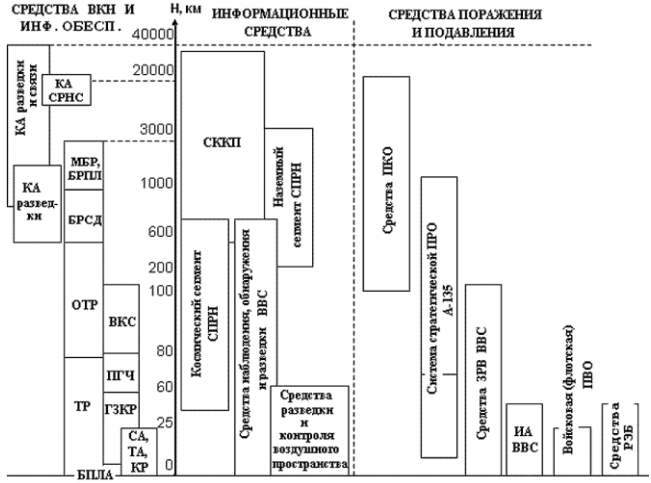


Рис. 4.22. Системы и средства, привлекаемые к решению задач обнаружения и борьбы с воздушными и космическими средствами противника [269]

Операции космических сил по обеспечению боевых действий в космосе и других средах, в соответствии с принятой в США терминологией, подразделяются на следующие группы (рис. 4.23) [230]:

- разведывательные;
- навигационные;
- обеспечения связи;

- предупреждения о ракетном нападении;
- контроля воздушно-космического пространства.

Рассмотрим более подробно роль космических систем в процессах добывания, сбора, обработки и передачи информации в рамках оперативного обеспечения войск (сил) по информации из работы [233].

Рис. 4.23. Классификация операций космических сил по обеспечению боевых действий [230]

Разведка как вид оперативного обеспечения классифицируется по ряду признаков, один из которых – способ размещения добывающих средств. В соответствии с этим признаком различают наземную, воздушную, морскую и космическую разведки. Космическая разведка, в свою очередь, подразделяется на:

- фотографическую;
- оптико-электронную;
- радио- и радиотехническую;
- радиолокационную.

В качестве космических средств разведки можно рассматривать также орбитальные группировки космических аппаратов и соответствующие наземные комплексы системы предупреждения о ракетном нападении.

Топогеодезическое обеспечение – комплекс мероприятий по подготовке и доведению до штабов и войск топогеодезических данных, необходимых для успешного решения поставленных задач. Включает подготовку и доведение до войск исходных астрономогеодезических и гравиметрических данных; создание, периодическое обновление, накопление запасов и обеспечение штабов и войск картами и фотодокументами местности; топографическую разведку. Здесь, так же как и в случае с разведкой, следует различать наземные, морские, воздушные и космические средства, способы получения необходимых данных.

Навигационное обеспечение – обеспечение потребителей данными о собственном местоположении на поверхности Земли, в воздушном и космическом пространстве.

Гидрометеорологическое обеспечение – комплекс мероприятий по сбору, обработке и доведению до войск и сил флота информации о гидрологических и метеорологических условиях в районах боевых действий. В интересах данного вида обеспечения могут использоваться как отдельные орбитальные группировки, так и космические аппараты разведки и дистанционного зондирования Земли (ДЗЗ), например, в целях разведки ледовой обстановки и др.

Оперативная маскировка – комплекс взаимосвязанных организационных военно-технических мероприятий и практических действий штабов, а также сил (войск), проводимых по единому замыслу и плану и направленных на достижение внезапности действий, повышение живучести и сохранение боеспособности сил (войск) и военных объектов в любых условиях обстановки.

По сути, маскировка есть предоставление или навязывание противнику ложной информации. Способами выполнения задач оперативной маскировки являются скрытие, имитация, демонстративные действия и дезинформация.

Космические средства разведки позволяют получать собственные (а также подтверждать полученные с помощью других средств) данные, свидетельствующие о выполнении либо невыполнении требований по скрытности своими войсками (силами). Имитация характерных действий войск (сил), равно как и демонстративные действия, могут осуществляться формированиями наземной группировки космиче-

ских сил. Для дезинформации противника в полной мере могут и должны быть использованы космические средства связи.

Радиоэлектронная борьба представляет собой совокупность согласованных действий и мероприятий по радиоэлектронному поражению радиоэлектронных объектов противника, радиоэлектронной защите своих радиоэлектронных объектов и радиоэлектронно-информационному обеспечению. Выявление радиоэлектронных объектов противника и контроль функционирования своих радиоэлектронных средств и применяющих их сил (вскрытие радиоэлектронной обстановки) достигается ведением радиоэлектронной разведки, в том числе с помощью КА радиолокационной, радио- и радиотехнической разведки. Принятие на вооружение средств радиоэлектронного подавления космического базирования позволит обеспечить возможность глобальности РЭП всех наземных, морских, воздушных и орбитальных объектов, а, следовательно, влиять на информационные потоки противника. Космические средства в рамках РЭБ могут применяться и для выдачи целеуказания на средства подавления каналов связи противника.

Инженерное обеспечение – комплекс инженерных мероприятий по созданию условий, необходимых для своевременного и скрытного развертывания сил (войск), обеспечению защищенности сил (войск) и объектов от воздействия средств поражения противника, ликвидации последствий его огневых и ядерных ударов, затруднению действий противника на берегу, ликвидации последствий чрезвычайных ситуаций природного и техногенного характера. Космические средства видовой разведки, равно как и КА ДЗЗ, могут быть задействованы при выполнении задач инженерной разведки противника, местности, акваторий водных участков земной поверхности и объектов системы базирования войск (сил); для вскрытия и освещения процесса подготовки ТВД, выявления последствий воздействия противника и чрезвычайных ситуаций различного характера, а также для оперативного контроля состояния инженерных объектов.

Контроль из космоса результатов ядерных ударов позволит оперативно получать информацию о ядерных взрывах с точностью, достаточной для определения факта поражения цели. Указанная информация поможет более обоснованно принимать решения с учетом складывающейся обстановки и о нанесении при необходимости повторных ядерных ударов своими СЯС.

Космические аппараты связи также могут быть использованы в качестве основных либо дополнительных средств обмена информа-

цией на необорудованных ТВД, равно как и при выходе из строя штатных средств управления и связи, размещенных на стационарных пунктах управления.

Радиационная, химическая и биологическая защита представляет собой совокупность согласованных действий и мероприятий сил (войск), направленных на обеспечение выполнения боевых задач в условиях применения противником ОМП, высокоточного и других видов оружия, а также крупномасштабных разрушений (аварий) радиационно, химически и биологически опасных объектов. Для выполнения ряда мероприятий РХБЗ, а именно засечки ядерных взрывов, сбора данных о радиационной обстановке, оповещения своих сил о применении противником ядерного оружия, а также оперативного предоставления соответствующей информации органам военного и государственного управления, применяются космические средства СПРН, разведки и связи. Размещение на КА датчиков, регистрирующих изменение радиационного фона, позволит расширить спектр средств, применяемых для засечки ядерных взрывов и тем самым повысить полноту и достоверность выявления радиационной обстановки.

Возможности космических систем позволяют также применять их и для решения задач, присущих специфическим видам оперативного (боевого) обеспечения отдельных родов войск (сил). Примером могут служить задачи поисково-спасательного обеспечения в ВВС и ВМС.

Для выполнения ряда задач *морально-психологического обеспечения*, а также задач информационно-психологических операций группировок ОВС НАТО в ходе войны в Югославии в 1999 г. и многонациональных сил в ходе войны в зоне Персидского залива в 2003 г. широко использовались космические системы телевидения и радиовещания Intelsat и Eutelsat, имеющие в своем составе КА на геостационарной орбите.

Представленные выше виды оперативного обеспечения с учетом приоритета использования их информационной составляющей, а также применения для этой цели космических средств правомерно рассматривать в качестве составных частей информационно-космического обеспечения [233].

Информационно-космическое обеспечение – совокупность действий (мероприятий), выполняемых как самостоятельно, так и во взаимодействии с потребителями, а также другими средствами видов ВС и средствами двойного назначения по [233]:

- поддержанию устойчивого функционирования каналов космической связи;
- формированию навигационного поля;
- созданию на борту КА изображений (в виде записи радиоголограммы, записи оптико-электронного изображения с ПЗС-матрицы и др.);
- доведению до приемных пунктов наземных специальных комплексов специальных материалов и сигналов с требуемым качеством;
- контролю фоноцелевой обстановки и космической деятельности иностранных государств в стратегической космической зоне;
- контролю пусков ракет;
- измерению, записи и передаче значений параметров космического пространства (радиационной обстановки, магнитного поля и др.) в интересах информационного обеспечения применения вооруженных сил.

В некоторых случаях информационно-космическое обеспечение целесообразно рассматривать как составную часть более широкого понятия *космического обеспечения* (или *военно-космического обеспечения*) [233].

При этом под космическим обеспечением предлагается понимать комплекс мероприятий, проводимых в ВС с участием оборонно-промышленного комплекса государства в целях [233]:

- создания, развертывания, наращивания и восполнения орбитальных группировок космических сил и средств военного и двойного назначения;
- предоставления гарантированного доступа космическим и иным средствам (например, гиперзвуковым летательным аппаратам, суборбитальным средствам, баллистическим ракетам и др.) в стратегическую космическую зону;
- использования космического пространства для решения задач военного характера (как обеспечивающего, так и боевого);
- контроля космического пространства (а в перспективе – разведки космической обстановки и выдачи целеуказаний);
- осуществления информационно-космического обеспечения применения войск (сил).

Представленное выше определение предполагает равнозначное возрастание роли новых сфер противоборства (в том числе и воору-

женного) – космической и информационной, диалектическую связь деятельности в этих сферах, а также важность совместного применения всего спектра используемых средств [233].

С учетом вышеизложенного можно сделать вывод о том, что эффективность выполнения стоящих перед вооруженными силами задач как в мирное, так и в военное время радикально зависит от возможности добывать и доставлять потребителю (в оперативные штабы, управляющие КП и т.д.) требуемую информацию. Данная информация должна позволять оценивать текущую политическую, военную, экономическую обстановку и состояние сред пространства во всех интересующих командование районах. Это, в конечном итоге, должно обеспечить эффективное применение группировок сил (войск). Такие задачи по добыванию, обработке и доставке информации с высокой оперативностью способны успешно решать только космические системы [233].

4.4.2. Системы информационно-космического обеспечения (на примере систем ВС США)

Рассмотрим возможности систем информационно-космического обеспечения боевых действий на примере орбитальной группировки США.

Развернутая в настоящее время орбитальная группировка КА военного назначения США, а также их функции представлены в табл. 4.3 [230, 261, 262].

Таблица 4.3. Развернутая в настоящее время орбитальная группировка КА военного назначения США, а также их функции [230, 261, 262]

Системы	**Количество и тип КА (дислокация)**
Разведывательные системы	
Видовой оптоэлектронной разведки	2 KH-11, TacSat-3, ORS, KestrelEye
Видовой радиолокационной разведки	3 Lacrosse, 4 Ferret-D, 20 SSU, Shale, Vortex,
Радиотехнической разведки	Ferret-D, SSU, SSU-2, SSU-3, SSU-4
Радио- и радиотехнической разведки	Vortex, Mercury Magnum, Orion, Mentor, Intruder, Jumpseat-2, Jumpseat-3, TacSat-4

Продолжение табл.4.3.

Системы	Количество и тип КА (дислокация)
Космическая система обнаружения пусков баллистических ракет Irish Maternity Early Warning System (IMEWS)	8 IMEWS (из них 5 находятся в оперативном использовании)
Система обнаружения ядерных взрывов	В качестве космического компонента используются установленные на борту спутников различного назначения (например, NAVSTAR) специальные комплексы датчиков и аппаратуры передачи данных
Космическая навигационная система	
Космическая радионавигационная система NAVSTAR	В состав космического компонента входят 29 КА (из них 24 в оперативном использовании)
Топогеодезическая, метеорологическая и контроля окружающей среды системы	
Система контроля окружающей среды	В состав космической группировки входят 6 КА Block-5D, 6 КА NOAA, 4 КА GOES
Топогеодезическая система министерства обороны	Развернута на базе КА GOES-3, LAGEOS-1
Океанографическая система	Развернута на базе КА OrbView-2, SiStar. Также задействованны метеорологические КА
Система разведки природных ресурсов Земли	Развернута на базе 3 КА Landsat-7
Спутниковые системы связи	
Система стратегической связи министерства обороны	DSCS-3, WGS
Объединенная система стратегической и тактической связи	MilStar-1, MilStar-2
	AEHF
Система связи ВВС (AFSatCom)	Использует каналы связи через КА типов FLTSATCOM, UFO, MilStar, SDS, DSCS, WGS
Система тактической узкополосной связи ВМС, ВВС и СВ	UFO, MUOS, TacSat-4
Система передачи данных SDS	7 КА SDS

Окончание табл.4.3.

Системы	Количество и тип КА (дислокация)
Система слежения и ретрансляции данных TDRSS	7 КА TDRS
Коммерческие космические системы связи	Геостационарные КА типов SATCOM, GStar, Telexy, PanAm Sat, Aurora, Iridium и др. (часть каналов в ретрансляторах арендуется МО США у различных американских фирм)
Системы контроля космического и воздушного пространства	
Система контроля космического пространства ВВС Spacetrack. Система контроля космического пространства ВМС SPASUR. Радиолокационная станция контроля космического пространства СВ ALTAIR. Вспомогательные средства	
Контрольно-измерительные комплексы и управление космическими средствами	
Контрольно-измерительные комплексы в составе ВВС (обеспечивают управление 80% КА), ВМС, СВ. Национального управления США по аэронавтике и исследованию космического пространства (NASA) и Национального управления по океанографии и метеорологии (NOAA)	

Ниже более подробно представлены отдельные системы информационно-космического обеспечения в соответствии с их функциональным предназначением.

4.4.2.1. Космические системы ведения разведки

Космические разведывательные системы используются для слежения за повседневной деятельностью и районами сосредоточения вооруженных сил потенциального противника, районами военных конфликтов, выявления и уточнения характеристик объектов критической инфраструктуры, наблюдения за их состоянием и особенностями функционирования, для вскрытия фактов использования РЭС и выявления по ним местоположения войск и сил. Космические разведывательные системы является основой информационного обеспечения для систем ВТО.

Анализ работ [237, 238, 241, 242, 244, 246, 258, 259, 260, 261, 262] показал, что в США разведка из космоса ведется следующими системами:

- системы оптико-электронной разведки (КА КН-11, ORS TacSat-3);
- система радиолокационной разведки (КА Lacrosse);
- системы радиотехнической разведки (КА Ferret, SSU, SSU-2, SSU-3, SSU-4);
- системы радио- и радиотехнической разведки (КА типов Vortex, Mercury Magnum, Orion, Mentor, Intruder, TacSat-4, Jumpseat-2, Jumpseat-3,).

Система оптико-электронной разведки KeyHole развернута на высотах 298-443 км на основе КА КН-11, которые оснащены длиннофокусными оптическими телескопами и фотоприемниками, позволяющими вести разведку днем в видимом диапазоне волн (с получением стереоизображений), а также ночью в ИК-диапазоне. Оптическая система КА КН-11 обеспечивает беспропускной просмотр всей земной поверхности в течение суток в полосе обзора 1250-3600 км с разрешающей способностью до 0,15 м в панхроматическом режиме [259]. В орбитальной группировке предусмотрено от 2 до 4 КА КН-11 [262].

Совместно с системой KeyHole для оптико-электронной разведки используются КА TacSat-3 и ORS (Operationally Responsive Space). В 2013 г. в интересах наращивания возможностей орбитальной группировки оптико-электронной разведки запущен КА KestrelEye [259].

КА TacSat-3 оснащен гиперспектральной оптико-электронной камерой для съемки в видимом, а также в ИК-диапазоне. Сброс полученных изображений осуществляется по радиоканалам потребителям на ТВД и на подвижные наземные станции. Дополнительно этот КА оснащен оборудованием в интересах ВМС для сбора данных с океанских буев, наземных датчиков и кораблей. КА ORS производит съемку в панхроматическом и многоспектральном режимах с разрешением лучше 1 м. КА Kestrel Eye может делать снимки с разрешением 1,5 м в панхроматическом режиме. В случае дальнейшей востребованности данной системы в планах США вывести на орбиту около 30 КА Kestrel Eye [237, 259].

Дополнительно к системам военного назначения США разведка из космоса также ведется с помощью КА двойного назначения, таких как: WorldView, GeoEye, LandSat. Аппаратура этих КА позволяет обеспечить получение панхроматических (разрешением 0,4-0,3 м) и многоспектральных (1,6-1,8 м) изображений [237, 238, 241, 242, 259].

В рамках дальнейшего развития системы оптико-электронной разведки США планируется создание системы космической оптико-электронной разведки SEE ME (Space Enabled Effects for Military Engagements). Основным предназначением данной системы станет разведывательное обеспечение подразделений ВС США, действующих на ТВД и в зонах вооруженных конфликтов. Предположительно, орбитальная группировка будет насчитывать 24 КА, которые будут развернуты после 2020 г. на низких орбитах высотой от 200 до 350 км. SEE ME позволит вести непрерывный мониторинг стратегически важных регионов и обеспечивать американские войска достоверными разведданными практически в любой точке мира в срок не более 90 мин [260].

Кроме того, в США ведутся разработки КА оптико-электронной разведки на геостационарной орбите. Планируется разработать КА с диаметром мембранно-оптической линзой до 20 м, который будет передавать видеоизображения в масштабе времени, близком к реальному, с линейным разрешением на местности не менее 1 м, при этом ширина полосы съемки составит не менее 10 км. Размещение на геостационарной орбите позволит одному КА охватить 1/3 поверхности Земли [260].

Система радиолокационной разведки функционирует на основе КА Lacrosse, развернутых на высоте 680 км. На данных КА устанавливаются однопозиционные многолучевые РЛС с синтезированной апертурой в сантиметровом диапазоне и однопозиционные однолучевые РЛС бокового обзора с синтезированной апертурой в дециметровом диапазоне. Это обеспечивает наблюдение в радиодиапазоне в полосе обзора 4000 км с разрешающей способностью 1-6 м. Максимальная разрешающая способность бортовой аппаратуры КА Lacrosse – 0,3-0,9 м. Данные с КА Lacrosse передаются по радиоканалам в масштабе времени, близком к реальному, через КА-ретрансляторы SDS и TDRS в центр сбора и обработки разведывательной информации на территории США [236, 246, 258].

В орбитальной группировке системы радиолокационной разведки предусмотрено 2-4 КА Lacrosse, 3 КА-ретранслятора SDS и 3-4 КА-ретранслятора TDRS [262].

Основной тенденцией развития КА радиолокационной разведки является расширение возможностей бортовой аппаратуры КА главным образом путем реализации многоспектральной оптико-электронной съемки и режима слежения за движущимися целями при радиолокационной съемке. Одним из основных направлений совер-

шенствования КА является проведение предварительной обработки получаемых данных на борту КА в интересах повышения качества получаемых изображений и снижения объема данных для передачи по радиоканалу [262].

Система космической радиотехнической разведки построена на основе КА Ferret-D, SSU и SSU-2.

КА Ferret-D позволяет вести разведку РЭС в диапазоне частот от 30 МГц до 80 ГГц с точностью определения координат 5-10 км в полосе сканирования шириной около 5800 км. Данные КА обеспечивают выявление дислокации и режимов работы РЭС. В составе орбитальной группировки системы радиотехнической разведки используются не менее 2 активных и 1-2 резервных КА Ferret-D. Система из 2 КА Ferret-D обеспечивает одновременное наблюдение района разведки на средних широтах с различных ракурсов с минимальным интервалом повторной разведки экваториального района 5,5 ч. Такое же время требуется для осуществления обзора всей поверхности Земли [262].

Система морской радиотехнической разведки NOSS (Naval Ocean Surveillance System) на основе КА SSU-1, SSU-2 и Intruder предназначена для обнаружения, опознавания, определения местоположения и курса движения кораблей и подводных лодок по излучению их РЭС. Орбитальное построение и возможности КА SSU и SSU-2 обеспечивают обнаружение корабельных РЭС в диапазоне частот от 50 МГц до 40 ГГц в полосе обзора около 7000 км и позволяют определять координаты кораблей и подводных лодок интерферометрическим методом с точностью до 1-5 км. Возможности орбитальной группировки позволяют производить беспропускной просмотр акватории Мирового океана за 1,5-2,5 ч [244, 246, 258, 261, 262, 337].

В орбитальной группировке NOSS предусмотрено 3-6 групп КА SSU-1 и SSU-2 (по 3 КА в группе), развертываемых на высотах 830-1200 км [262].

Система космической радио- и радиотехнической разведки построена на основе КА Vortex, Mercury (в ряде источников указывается как Advanced Vortex), Magnum, Orion, Mentor (в ряде источников указывается как Advanced Orion). Данная система предназначена для перехвата информации наземных средств, а также переговоров по УКВ-линиям связи в диапазоне частот 45 МГц – 20 ГГц. Ее орбитальное построение позволяет вести разведку круглосуточно и непрерывно. Данные от спутников передавались через КА сбора и передачи данных SDS на наземные пункты приема информации. В дальнейшем

планируется расширить возможности космической системы радио- и радиотехнической разведки с целью обеспечения перехвата сообщений в каналах правительственной и военной связи [261, 262]. Так, в 2011 г. был запущен КА TacSat-4, одной из задач которого является перехват сообщений в УВЧ каналах правительственной и военной радиосвязи.

Система радио- и радиотехнической разведки на высокоэллиптических орбитах над северным полушарием на основе КА Jumpseat-2 и Jumpseat-3 обеспечивает обнаружение, определение местоположения РЭС и их характеристик, перехват переговоров по УКВ-линиям связи в диапазоне 50 МГц – 40 ГГц. В орбитальной группировке предусмотрено 5-6 КА [261, 262].

4.4.2.2. Система обнаружения стартов МБР и ядерных взрывов

Система обнаружения стартов МБР и ядерных взрывов предназначена для обнаружения стартов МБР противника и предупреждения о них, обнаружения ядерных взрывов на поверхности Земли, в атмосфере и в космическом пространстве. Орбитальная группировка состоит из 6-8 КА типа IMEWS (Integrated Missile Early Warning Satellite), IMEWS-2, а также КА SEWS. Оборудование этих КА работает в двух инфракрасных диапазонах, что позволяет более точно классифицировать запускаемые ракеты и определять параметры их движения. Оно позволяет иметь по долготе глобальную зону обзора, по широте – от 83° с.ш. до 83° ю.ш. и время поступления информации на КП NORAD – 1-4 мин после обнаружения старта МБР спутниками системы. При этом максимальная ошибка определения координат старта МБР – около 3 км, а ошибка определения районов падения головных частей – до 1000 км. Продолжаются работы по развертыванию перспективной системы обнаружения стартов МБР SBIRS взамен существующей [261, 262].

4.4.2.3. Космическая навигационная система

Космическая навигационная система NAVSTAR, обеспечивающая измерение расстояния, времени и определяющая местоположение во всемирной системе координат WGS 84, позволяет в любом месте Земли (исключая приполярные области) почти при любой погоде, а также в околоземном космическом пространстве определять местопо-

ложение и скорость объектов с точностью 1 м (в высокоточном режиме) и 5-25 м [261, 262].

4.4.2.4. Космическая топогеодезическая система

Космическая топогеодезическая система США состоит из КА типа GEOS-3, LAGEOS-1 и LAGEOS-2, которые используются для уточнения данных о форме, размерах Земли и ее гравитационном поле, слежения за перемещением материков и отдельных участков земной поверхности. Кроме того, для получения топогеодезической информации используется КА GFO-1.

Бортовая аппаратура КА GEOS-3 и LAGEOS-1 позволяет измерять расстояние от спутника до земной поверхности с точностью до 0,2 м. Это обеспечивает возможность определять абсолютную высоту от центра поверхности Земли с точностью до 5 м.

В дальнейшем данные космических топогеодезических систем лягут в основу подготовки полетных заданий для крылатых ракет, осуществляющих полет с огибанием рельефа местности.

4.4.2.5. Космическая система метеорологии и контроля окружающей среды

Метеорологическую информацию и данные контроля окружающей среды вооруженные силы США получают от военной и коммерческих метеорологических систем на основе КА: Block-5D, NOAA, GOES. Эти КА обеспечивают интервал связи с метеостанциями 5-15 мин, обзор одним КА поверхности Земли полосой 2700-3000 км и разрешающей способностью 0,55-1,1 км, определяющий температурный профиль атмосферы до высоты 30-40 км от уровня моря с точностью 0,5-1,5 гр С [261, 262].

4.4.2.6. Спутниковые системы связи и ретрансляции данных

Большое значение для обеспечения устойчивости и глобальности управления вооруженными силами связи ВС США имеет использование систем спутниковой связи. Основное их назначение – это предоставление органам управления на ТВД надежных, защищенных каналов связи (передачи данных) с группировками вооруженных сил, тактическими соединениями, отдельными воинскими частями и каждым солдатом. Основными качествами спутниковой связи, которыми

не обладают другие виды связи, являются глобальный охват и способность предоставлять каналы связи из любой точки мира в очень короткое время.

Анализ работ [130, 261, 262, 266, 320] показал, что военные спутниковые системы связи вооруженных сил США делятся на:

- стратегические;
- оперативные;
- тактические.

Кроме того, в условиях военных конфликтов для восполнения требуемой высокой пропускной способности космической связи вооруженные силы США активно используют ресурс коммерческих спутниковых систем связи – Iridium, GlogalStar, Satcom, и др.

Система спутниковой связи стратегического звена управления DSCS (Defense Satellite Communication System) обеспечивает связью высшее военно-политическое руководство и органы вооруженных сил практически с любой воинской частью, размещенной вне территории США, или с авианосными соединениями, находящимися в акватории Мирового океана.

В составе системы используются 12-13 КА DSCS-3 и WGS (Wideband Global Satcom) на геостационарных орбитах, а также сеть наземных и корабельных станций ретрансляции. Геостационарное построение системы позволяет обеспечивать глобальную связь на всей территории Земли, за исключением полярных районов. В настоящее время производится постепенный переход орбитальной группировки с КА DSCS на КА WGS [266].

Ретрансляционная аппаратура КА DSCS-3 обеспечивает связь по 3900 телефонным каналам в X-диапазоне: 7900-8400 МГц - на прием, и 7250-7750 МГц – на передачу. Мощность транспондеров – 50 Вт. Полоса пропускания каналов – от 50 до 85 МГц. Для управления космическим аппаратом и передачи телеметрии используются S- и X-диапазоны. Кроме того, на КА установлен ретранслятор, работающий в диапазоне 225-400 МГц. Пропускная способность одного КА составляет от 100 до 900 Мбит/с. КА серии DSCS-3 обеспечены надежной защитой от ЭМИ ядерного взрыва и имеют на борту широкополосную, помехозащищенную аппаратуру связи. Кроме того, они оснащены защищенной системой телеметрии, слежения и передачи команд, которая рассчитана на быструю перестройку в случае постановки преднамеренных помех [320, 266].

Для увеличения общей пропускной способности и предоставления услуг магистральной связи для зон Тихого, Атлантического,

Индийского океанов и континентальной части США с начала 2001 г. ведется разработка новой широкополосной системы спутниковой связи WGS (Wideband Global Satcom). Основная задача этой системы состоит в увеличении пропускной способности каналов связи, для чего при разработке аппаратуры связи применялись следующие технические решения, предполагавшие [266]:

- развертывание дополнительных ретрансляторов миллиметрового диапазона;
- применение гибкого полосового фильтра и возможность переключения каналов на борту для переноса в ретранслятор другого диапазона;
- одновременное использование номиналов частот за счет пространственного и поляризационного разделения.

КА WGS оснащены бортовой аппаратурой, которая состоит из нескольких десятков ретрансляторов, работающих в диапазонах, которые используются в ВС США в настоящее время (8/7, 40/20 ГГц), а также еще в нескольких военных и гражданских диапазонах (например, в Ка-диапазоне 30/20 ГГц для обеспечения работы службы глобального вещания), и обеспечивает суммарную пропускную способность 2,2 Гбит/с. Это сравнимо с 10 КА типа DSCS-3 [266].

Антенный комплекс КА WGS может формировать 19 независимых зон покрытия и имеет в своем составе [320]:

- основную антенну Х-диапазона (8/7 ГГц);
- передающие и приемные фазированные антенные решетки, формирующие в Х-диапазоне 8 зон покрытия;
- 8 узконаправленных и 2 зональные параболические приемо-передающие антенны на карданном подвесе для формирования 10 лучей в К- и Ка-диапазонах (40/20 и 30/20 ГГц).

КА WGS оснащен комплектом аппаратуры обработки сигналов на борту и коммутацией каналов с переносом их в ретранслятор другого диапазона. Бортовая аппаратура КА обеспечивает передачу данных со скоростью 311 Мбит/с. Диапазон 30/20 ГГц предназначен для глобальной службы вещания системы GBS (Global Broadcast System). Глобальная спутниковая система широкополосного вещания GBS осуществляет передачу видео, геодезической и картографической информации, а также метеоданных и других сведений для соединений и частей всех видов вооруженных сил США. Спутниковая приемная аппаратура системы GBS работает в Ка-диапазоне (30 ГГц) и имеет 4 канала связи со скоростью передачи данных 24 Мбит/с. Передача данных по линии вниз осуществляется в Ка-диапазоне (20 ГГц). Про-

пускная способность космического аппарата WGS за счет применения устройств коммутации каналов, средств частотного, пространственного и поляризационного разделения сигналов и при использовании аппаратуры GBS составляет от 2,4 до 3,6 Гбит/с [320].

Расчетный срок активного функционирования КА WGS – 10 лет [266].

Для управления целевой нагрузкой КА WGS в вооруженных силах США создано 4 армейских центра управления связью, каждый из которых может одновременно управлять приемом-передачей данных через 3 КА. Центр управления полетом спутников один, а его наземные средства работают в S-диапазоне [320].

После полной замены системы на КА WGS планируется, что орбитальная группировка будет включать в себя только 6 КА WGS [266].

Система спутниковой связи стратегического и оперативно-тактического звена управления ВС США построена на основе КА MilStar и КА AEHF. Система обеспечивает безопасную и помехоустойчивую связь в глобальном масштабе и характеризуется [261, 262]:

- высокой живучестью за счет использования защиты от лазерного и электромагнитного оружия;
- автономностью за счет использования бортовой навигационной системы и малой потребности в управлении с Земли;
- безопасностью и помехозащищенностью за счет использования кодирования, алгоритмов восстановления ошибок, шифрования информации, а также использования лазерной межспутниковой связи.

В составе орбитальной группировки системы используются 5-6 КА MilStar-1, MilStar-2, AEHF.

С целью высокой защищенности линий связи в системе используется Ка-, К- и V-диапазоны частот. Эти диапазоны частот позволяют формировать узкие направленные лучи, которые, наряду с помехозащищенностью каналов, повышают и скрытность линий связи, поскольку сигналы трудно запеленговать, а значит, и подавить. Использование помехоустойчивых алгоритмов кодирования и обработки сигнала позволяет обеспечивать высокую помехозащищенность каналов связи [320].

Через технические средства спутников передаются разведданные и видеоинформация, осуществляется речевой обмен и проводятся видеоконференции.

КА MilStar-1 использовали радиодиапазоны 225-400 МГц, 20-44 ГГц. Эти КА оборудованы аппаратурой низкоскоростной передачи данных, которая обеспечивала организацию 192 низкоскоростных (от 75 до 2400 бит/с) каналов связи (44,5 ГГц – на линии вверх и 20,7 ГГц – на линии вниз) и систему перекрестной связи друг с другом на частоте 60 ГГц. Кроме того, космические аппараты имеют четыре УВЧ- канала связи (300 и 250 МГц) системы AFSATCOM (Air Force Satellite Communications) для ВВС США и один УВЧ-канал вещания (300 и 250 МГц) – для ВМС США [266, 320].

КА следующего поколения MilStar-2 позволяют организовывать 192 низкоскоростных (от 75 до 2400 бит/с) и 32 среднескоростных (от 4,8 кбит/с до 1,544 Мбит/с) защищенных канала связи в расширенной полосе рабочих частот. Расширение полосы рабочих частот, необходимое для осуществления передачи данных в режиме высокой скорости, снижает стойкость к активным преднамеренным помехам, поэтому такой аппарат несет две антенны с обнулением диаграммы направленности в сторону помехи и одну с разнесенными зонами обслуживания. Антенные системы способны засекать направление активных преднамеренных помех и временно блокировать или обнулять диаграмму направленности в направлении помехи, сохраняя обычный режим работы в других направлениях без потери связи [266, 320].

Технические средства КА MilStar реализуют следующие функции [266]:

- бортовая обработка и коммутация сигналов;
- автономное управление бортовыми ресурсами;
- перекрестное использование спектра (прием сигнала через одну антенну в одном диапазоне и ретрансляция его через другую антенну в другом диапазоне);
- межспутниковая связь.

С 2009 г. система связи на основе КА MILSTAR (Military Strategic and Tactical Relay) постепенно заменяется на перспективную систему связи миллиметрового диапазона AEHF – Advanced Extremely-High-Frequency [266].

Космическая система AEHF обеспечивает более безопасную, устойчивую и высокоскоростную, по сравнению с системой MILSTAR, глобальную связь высшего политического и военного руководства США с командованием вооруженных сил, видов и родов войск, командирами стратегических и тактических группировок войск. Система AEHF применяется на всех ТВД, на суше, на море, в воздухе

и в космосе в условиях мирного и военного времени, в том числе в условиях ядерной войны [320].

Система AEHF состоит из трех сегментов: космического, пользовательского и наземного. Космический сегмент представляет собой орбитальную группировку из 4-6 КА на геостационарной орбите с системой межспутниковой связи, обеспечивающей глобальное покрытие. Наземный сегмент управления системой предназначен для управления аппаратами на орбитах, контроля их оперативно-технического состояния и обеспечения планирования и управления системой связи. Этот сегмент строится по схеме многократного резервирования и включает комплекс стационарных и мобильных станций управления [320].

Бортовой ретрансляционный комплекс КА AEHF функционирует на частотах 44 ГГц (каналы «Земля-КА») и 20 ГГц (каналы «КА-Земля»), формируя более 50 каналов суммарной пропускной способностью 430 Мбит/с. КА AEHF совместим с низкоскоростными (от 75 до 2400 бит/с) и среднескоростными (от 4,8 кбит/с до 1,544 Мбит/с) каналами системы MILSTAR, а также поддерживает высокоскоростные каналы связи (до 8,2 Мбит/с). Скорость обмена данными в системе AEFH в 5 раз превышает скорость обмена в системе MILSTAR, что позволяет передавать пользователям целеуказания и видеоизображение высокого разрешения от БПЛА и КА разведки в реальном масштабе времени. Кроме того, КА AEHF имеют развитую и надежную инфраструктуру связи между собой (каждый с двумя соседними) в миллиметровом V-диапазоне частот (60 ГГц) [266, 320].

Антенный комплекс КА AEHF включает следующие элементы [320]:

- основная антенна;
- 2 передающие фазированные антенные решетки (ФАР), формирующие до 24 каналов с временным разделением для работы с портативными терминалами;
- приемная антенна с ФАР;
- 6 параболических приемопередающих антенн на карданном подвесе для формирования региональных лучей;
- 2 остронаправленные антенны для тактической и стратегической связи;
- 2 антенны межспутниковой связи.

Каждый КА AEHF, используя сочетание ФАР и параболических антенн, формирует 194 региональных луча [320].

В КА AEHF реализована обработка сигналов на борту. Это обеспечивает высокую помехозащиту и оптимизацию используемых

бортовых ресурсов, системную гибкость по отношению к различным потребителям в видах вооруженных сил и другим пользователям, использующим терминалы наземного, морского и воздушного базирования [320].

Система AEHF после полноценного развертывания является одним из ключевых звеньев единой информационной системы GIG и системы управления государственных и военных организаций, а также основой космической системы обмена данными между субъектами боевых действий на суше и на море, в воздухе и в космосе [320].

Тактико-технические характеристики систем MILSTAR и AEHF представлены в табл. 4.4 [320].

Таблица 4.4 – ТТХ систем MILSTAR и AEHF [320]

Тип и объем информации	**Время доставки информации потребителю**		
	Система военной связи		
	MilStar 1	MilStar 2	AEHF
Целеуказание (1,1 Мбайт)	1 ч	6 с	1 с
Видеоизображение (24 Мбайт)	22 ч	2 мин	24 с
Радиолокационное изображение от БПЛА (120 Мбайт)	110 ч	12 мин	2 мин
Радиолокационное изображение от КА ДЗЗ (1 Гбайт)	880 ч	90 мин	17 мин
Подвижная связь	нет	нет	140 линий по 32 кбит/с

Ранее в планах США было создание трансформируемой системы спутниковой связи TSAT (Transformational Satellite Communications System) [266], которая должна была обеспечить еще более высокие показатели по пропускной способности. Однако после начального развертывания системы WGS и запуска первого КА AEHF Министерство обороны США приняло решение о свертывании работ по системе спутниковой связи TSAT [320].

Система тактической узкополосной связи на основе КА UFO и MUOS (ранее – FLTSATCOM) создавалась ВМС США для обеспечения связи береговых центров с надводными и подводными объектами, авиацией флота и циркулярного оповещения сил флота по

специальному каналу. В настоящее время система UFO является основной системой тактической мобильной связи вооруженных сил США в дециметровом диапазоне. Она широко используется Министерством обороны, государственным департаментом, Президентом США и стратегическими командованиями для управления подразделениями и частями оперативно-тактического звена всех видов вооруженных сил, в частности, обеспечивая связью подводные лодки, самолеты и стратегическую авиацию США [320].

На начало 2013 г. орбитальная группировка системы включала 9 КА UFO (8 основных и 1 резервный) и 2 КА FLTSATCOM на геостационарной орбите. Рабочая зона системы UFO охватывает всю зону Земли за исключением полярных широт (свыше 76°). Система UFO позволяет постоянно поддерживать связь с кораблями, подводными лодками, находящимися в акватории Мирового океана, и самолетами в полете. С помощью спутников обеспечивается односторонняя связь со всеми мобильными средствами (только передача) и двусторонняя связь с крупными надводными кораблями, подводными лодками и самолетами [266, 320].

КА UFO разработаны на основе платформы BSS-601 компании Boeing. Срок активного существования космического аппарата – 14 лет. На всех КА UFO установлено 11 твердотельных усилителей УВЧ-диапазона. Они обеспечивают 39 каналов связи с суммарной полосой пропускания 555 кГц и 21 узкополосный канал звуковой связи полосой пропускания 5 кГц каждый, 17 ретрансляционных каналов с шириной полосы по 25 кГц и канал флотского вещания с шириной полосы 25 кГц [320].

Последние 3 КА UFO оснащены аппаратурой службы глобального вещания GBS. Эти комплекты состоят из 4 транспондеров мощностью по 130 Вт, работают в Ka-диапазоне (30/20 ГГц) и обладают пропускной способностью 24 Мбит/с. Таким образом, комплект GBS на одном спутнике обеспечивает передачу 96 Мбит/с [320].

На замену системы UFO в настоящее время приходит перспективная система узкополосной связи MUOS – Mobile User Objective System. Разработка и производство спутниковой системы связи MUOS возложены на компанию Lockheed Martin.

В состав первичной конфигурации системы связи вошли наземный комплекс управления и 2 КА MUOS, срок развертывания системы первого этапа – лето 2013 г. Полностью развернутая система MUOS состоит из 5 КА (1 из них резервный) на геостационарной орбите [320].

Спутники MUOS разработаны на основе платформы A2100 компании Lockheed Martin. Срок планируемого активного существования космического аппарата – 14 лет [320].

Система MUOS создана с применением передовых технологий гражданской спутниковой связи, она значительно улучшает возможности военной связи, предоставляя мобильным пользователям (от стратегического звена до отдельного пехотинца) в реальном масштабе времени телефонную связь, услуги по передаче данных и видео. Система ориентирована на совместное применение с создаваемыми едиными пользовательскими терминалами проекта JTRS (Joint Tactical Radio Systems), совместимыми, в том числе и с системой UFO. Важнейшими требованиями, предъявляемыми системе, являются: обеспечение гарантированного доступа, связь в движении, способность формировать различные по назначению и конфигурации сети связи, объединенное взаимодействие сетей связи разнородных сил, глобальный охват, режим вещания и связь в приполярных районах, возможность использования малогабаритных портативных абонентских терминалов [320].

КА MUOS работают в УВЧ-, Х- и Ка-диапазонах. Бортовое оборудование КА MUOS обеспечивает организацию узкополосных каналов связи со скоростью до 64 кбит/с. Скорость каналов связи обеспечиваемая спутником MUOS, – до 5 Мбит/с, что в 10 раз выше, чем у системы UFO (до 400 кбит/с). Каждый КА MUOS обладает пропускной способностью, эквивалентной 8 КА UFO [320].

Бортовое оборудование КА MUOS позволяет более эффективно использовать выделяемый диапазон частот, для чего в системе реализован многостанционный доступ с выделением каналов по требованию. Благодаря использованию современных методов цифровой обработки сигналов, новых способов модуляции и помехоустойчивого кодирования, система связи имеет более высокие надежность, защищенность, помехоустойчивость и эффективность связи [320].

Система тактической узкополосной связи на высокоэллиптических орбитах. В 2005 г. для того чтобы сделать систему военной спутниковой узкополосной связи глобальной (в том числе за счет обеспечения связи в приполярных северных районах), в США было принято решение о создании экспериментальной системы связи на высокоэллиптических спутниках.

В сентябре 2011 г. с этой целью запущен экспериментальный спутник TacSat-4. Орбита космического аппарата – эллиптическая с перигеем 850 км, апогеем 12050 км и наклоном плоскости орбиты –

63,4 град. TacSat-4 – экспериментальный КА разведки и связи, спроектированный научно-исследовательской лабораторией ВМС США при участии компании Boeing, General Dynamics и Raytheon. Масса – 460 кг, диаметр антенны – 3,8 м [320].

Назначение КА TacSat-4 [320]:

- обеспечение глобальной защищенной помехоустойчивой связи с подразделениями на поле боя (реализующих принцип «связь на ходу»);
- радиоразведка и обнаружение подводных лодок противника;
- доведение до подразделений морской пехоты и кораблей ВМС США результатов оценки обстановки и боевых приказов в условиях сильного противодействия радиотехнических средств противника.

Спутник TacSat-4 обеспечивает до 10 каналов узкополосной связи (от 2,4 до 16 кбит/с) в диапазоне УВЧ (300 и 250 МГц). На спутнике TacSat-4 также имеется аппаратура системы MUOS с шириной полосы пропускания 5 МГц для информационного сопряжения с КА MUOS на геостационарных орбитах и приема-передачи данных через них [320].

Испытания и эксплуатация космического аппарата TacSat-4 позволяют ВМС США определять будущую потребность в спутниках на высокоэллиптической орбите, действующих совместно с системами на геостационарной орбите [320].

Система связи ВВС США AFSatCom позволяет постоянно поддерживать связь между штабом стратегического командования США и воздушными командными пунктами со стратегическими бомбардировщиками в полете, постами управления запуском МБР, а также самолетами-ретрансляторами Takamo для связи с ПЛАРБ [261, 262].

Система AFSatCom своих КА не имеет, а использует каналы связи через КА типов FLTSATCOM, UFO, MilStar, SDS, DSCS, WGS, что обеспечивает связь с объектом, находящимся в любом районе Земли [261, 262].

Система сопровождения и ретрансляции данных TDRSS (Tracking and Data Relay Satellite System) обеспечивает слежение за КА разведки и ретрансляцию принимаемой от них информации на наземную станцию управления. Система создана на основе КА TDRS (Tracking and Data Relay Satellite) и способна одновременно получать и передавать данные от 20 низкоорбитальных КА, при этом сами КА

TDRS могут далее ретранслировать информацию на КА, находящиеся на более высоких орбитах. Бортовое оборудование включает в себя транспондеры S- и Ku-диапазонов (КА TDRS-2), кроме того, дополнительно Ka-диапазона. Орбитальная группировка включает 8-10 КА TDRS-1 и TDRS-2 на геостационарных орбитах [236, 258].

Космическая система сбора и передачи данных на базе КА SDS (Satellite Data System) обеспечивает связью самолеты ВВС в районах Крайнего Севера, прием и передачу информации с разведывательных спутников и от расположенных за пределами территории США станций слежения за КА. В состав системы входят 10 КА на высоко эллиптических (с апогеем над северным полушарием) и стационарных орбитах, а также сеть наземных и самолетных станций.

Бортовая аппаратура КА SDS позволяет обеспечивать связь с самолетами ВВС США по 15 радиотелеграфным каналам в метровом диапазоне волн 240-320 МГц. В дециметровом диапазоне 2,2-2,3 ГГц бортовая аппаратура КА SDS обеспечивала ретрансляцию информации от разведывательных КА на пункты сбора и обработки информации, а также от станций слежения за спутниками [236, 258, 261, 262].

4.4.2.7. Перспективные системы информационно-космического обеспечения на основе малых космических аппаратов

При традиционных способах информационно-космического обеспечения КА не может обладать малой массой в силу массогабаритных характеристик бортовой аппаратуры. Однако в настоящее время прорабатывается ряд новых перспективных направлений информационно-космического обеспечения с использованием малых КА (мини-КА и микро-КА).

Первое направление – многоспектральная разведка. Телескопом минимального диаметра можно накрыть цель и сделать снимок с невысоким разрешением. Но если при этом реализовать многоспектральный портрет цели, то с помощью бортового компьютера КА можно получить высококачественное изображение в реальном масштабе времени. Такая система оптической разведки без использования большого телескопа получается достаточно компактной, а скорость обработки сигнала современными средствами высока [265].

Второе направление – развитие радиотехнической разведки. При расстоянии 10-50 км между мини-КА разрешающая способность распределенной космической системы благодаря увеличению базы измерений возрастает в сотни раз. Система из 3-4 таких мини-КА сможет обеспечить мониторинг транспортных средств, территории и целей противника на локальном ТВД [265].

В области радиолокационной разведки специалистами ведутся исследования возможности стороннего радиоподсвета цели или облучения ее с других КА. Проведенные исследования показали, что возможно создание орбитальной группировки, в которой один КА кластера, обладающий мощным передатчиком, облучает поверхность Земли, а находящиеся рядом с ним мини-КА (без передатчиков и мощных систем электропитания) получают ответный сигнал от целей и по нему строят радиолокационные изображения. Причем в кластере получается не одно, а одновременно несколько изображений, что исключает возможность помех и открывает новые возможности вскрытия замаскированных целей [265].

В этом же направлении развиваются работы по радиоподсвету воздушных целей с помощью КА навигационных космических систем. Несмотря на слабый отраженный сигнал, использование разнесенного приема позволит создать глобальную систему пассивного радиолокационного наблюдения за всем воздушным пространством страны. При этом использование пассивной локации повысит живучесть подобной системы в условиях применения противником средств поражения (по опыту боевых действий последних десятилетий, средства активной ПВО поражались в первую очередь) и обеспечит возможность целеуказания для средств ПВО [265].

Третье направление – создание мини-КА связи. При информационном обеспечении войск важно решить не только проблему оперативной связи между подразделениями в районе военного конфликта, но и проблему глобальной оперативной связи удаленных войсковых группировок (групп кораблей ВМФ, авиационных группировок) с центральным военным командованием. Как показывает отечественный и зарубежный опыт, все эти проблемы также сравнительно просто и устойчиво решаются с помощью низкоорбитальных группировок МКА связи [265].

Четвертое направление – совершенствование космического эшелона воздушно-космической обороны. Одним из вариантов удачного применения для мини-КА является развитие системы контроля космического пространства (СККП). На орбите размещается ряд КА с

перекрестными полями наблюдения. Моделирование показывает, что всего 8 КА в группировке позволют уточнять цель любого нового объекта в течение 30 мин. Сейчас в наземных оптико-электронных и радиолокационных системах на это требуется несколько часов. Выигрыш в создании подобного космического эшелона контроля состоит еще и в том, что сейчас отсутствуют наземные средства, которые наблюдали бы КА на орбитах с наклоном менее 30^0. Кроме того, подобный космический сегмент СККП может осуществлять мониторинг гиперзвуковых летательных аппаратов, которые летают на средних высотах от 20 до 40 км со скоростью свыше 5 М [265].

Расширить космический эшелон СККП возможно и за счет размещения средств радиотехнической разведки на малых КА. В результате появляется возможность глобального мониторинга всех геостационарных систем связи, которые ранее были недоступны для контроля. Кроме того, космические системы контроля могут отслеживать такие космические средства, как КА-инспекторы и КА-перехватчики, а в отдаленной перспективе – контролировать использование в космосе средств противоспутниковой борьбы [265].

Пятое направление – создание на основе мини-КА систем противоспутниковой борьбы, в которые входят орбитальные платформы-носители и группировки мини-КА: контроля космического пространства, инспекторы и перехватчики.

Шестое направление – создание группировки оперативного контроля ионосферы, в том числе в приполярной области. Это чрезвычайно важно при решении задач повышения точности космических навигационных систем, а также при уточнении данных загоризонтных РЛС, используемых в системах предупреждения о ракетном нападении [265].

Стратегия развития многоспутниковой системы на малых КА предусматривает создание универсальных КА информационно-космического обеспечения. Таким образом, единая универсальная многоспутниковая группировка малых КА способна решать задачи обеспечения глобальной связи, всеобъемлющей разведки ТВД и околоземного космоса [265].

В настоящее время перспективы использования систем на основе малых КА постоянно расширяются, и в связи с этим появился ряд принципиально новых проектов, связанных с существенным удешевлением и повышением оперативности процесса вывода их на орбиту. Так, испанская компания Celestia Aerospace объявила о начале своего проекта SALS (Sagitarius Airborne Launch System – Воздушная система

запуска «Стрелец»), целью которого является обеспечение сравнительно простого и дешевого запуска микро-КА. В состав комплекса SALS вошли самолеты и ракеты-носители двух типов. В качестве полезной нагрузки системы SALS рассматриваются микро-КА массой до 10 кг. В зависимости от типа используемой ракеты-носителя одновременно на орбиту могут выводиться от 4 до 16 аппаратов. Самым крупным компонентом комплекса SALS должен стать самолет Archer-1 («Лучник-1»). Непосредственная доставка полезной нагрузки на орбиту будет осуществляться при помощи ракет Space Arrow SM и Space Arrow CM («Космическая стрела»). Характеристики этих изделий таковы, что ракеты могут подниматься на достаточную высоту и сбрасывать полезную нагрузку в виде микро-КА. Ракета Space Arrow SM несет 4 КА. Более крупная ракета Space Arrow CM – 16 аппаратов. Предполагается, что данная система позволит выводить микро-КА на орбиту высотой до 600 км. Первый испытательный запуск ракеты Space Arrow состоялся в 2016 г [489].

4.4.3. Перспективы проведения военных операций в космической сфере (на примере доктрины ВС США)

Кроме широкомасштабного использования информационно-космических систем для обеспечения применения ВС, в настоящее время прорабатываются вопросы ведения боевых действий в космической сфере. Так, в специальном документе министерства ВВС США AFDD 2-2 «Space Operations» («Космические операции»), опубликованном в августе 1998 г., были определены доктринальные основы боевого применения (современные, а также на ближне- и среднесрочную перспективу) космических сил США, основу которых составляет 14-я воздушная армия ВВС. В соответствии с этим документом первоочередной задачей любой военной кампании провозглашается завоевание безусловного военного превосходства в космосе [230].

Военное превосходство в космосе – такая ситуация, при которой космические силы будут обладать полной свободой действий, в том числе и по нанесению ущерба противнику, а космические силы противника, наоборот, не будут иметь никакой возможности для причинения вреда государству или его союзникам [230].

Понятие военного космического превосходства распространяется также на недопущение использования противником космической связи, сигналов точной навигации, разведывательных, метеорологиче-

ских и других данных, получаемых с помощью собственных или иностранных (международных) космических средств [230].

Завоевание военного космического превосходства предполагается осуществлять путем выполнения комплекса специальных активных мероприятий, в рамках которого планируется проведение противокосмических операций. При этом сами же противокосмические операции могут быть [230]:

- оборонительными;
- наступательными.

Цель наступательных противокосмических операций – уничтожение или нейтрализация космических систем или средств противника, а также прекращение доступа к обеспечиваемой ими или через них информации [230].

Достижение этой цели планируется осуществлять различными способами, основными из которых являются [230, 231]:

- внесение преднамеренных искажений в циркулирующие через космические системы противника информационные потоки;
- временное нарушение функционирования;
- снижение эффективности боевого применения или уничтожение компонентов космических систем противника;
- лишение доступа противника к собственным космическим системам.

Наиболее широко проработанной формой наступательной противокосмической операции является нанесение авиационных, ракетных и артиллерийских ударов по наземным элементам космической инфраструктуры противника. Вместе с тем возможно и проведение противокосмических операций по схемам «Земля-космос», «космос-космос» и «космос-Земля». В связи с этим создание и развертывание вооружений, предназначенных для применения по указанным схемам, являются важнейшими факторами, обеспечивающими безопасность государства [230].

Оборонительные противокосмические операции – активные и пассивные мероприятия, направленные на защиту космических сил от ударов противника или его попыток нарушить порядок их функционирования [230].

В рамках активных противокосмических операций планируется проводить мероприятия по обнаружению, сопровождению (идентификации) и уничтожению или нейтрализации атакующих средств противника. При этом возможно осуществление маневрирования косми-

ческими аппаратами с целью увода их от возможного воздействия, использования средств РЭБ, а также другие формы противоспутниковой борьбы (ПСБ) [230].

Пассивные противокосмические операции планируется проводить в целях снижения уязвимости космических систем и средств. В ходе таких операций самостоятельно или в различных сочетаниях предполагается применение таких мер, как шифрование, использование техники псевдослучайного перескока несущих частот, повышение прочности конструкций, маскировка, рассредоточение и другие [230].

При рассмотрении возможностей по обеспечению наступательных и оборонительных противокосмических операций можно отметить, что высокие результаты могут быть получены только при наличии развитых и эффективных систем контроля воздушно-космического пространства, наблюдения за его параметрами (радиационный фон, характеристики магнитного поля, интенсивность потоков солнечного ветра и другие), а также предупреждения о ракетном нападении [230].

В результате завоевания военного превосходства в космосе космические силы смогут практически беспрепятственно проводить не только противокосмические, но также и другие операции по применению силы в космосе и из космоса, а также по обеспечению боевых действий в других средах [230].

Нанесение ударов из космоса (операции по применению силы) уже рассматривается как реальная форма боевых действий космических сил, несмотря на то, что даже многие технологически развитые страны еще пока не располагают соответствующими системами вооружения. Ударной космической системой, являющейся наиболее вероятным «кандидатом» на развертывание в ближайшие сроки, называется комплекс лазерного оружия космического базирования [230].

Направления сосредоточения основных усилий при развитии космических сил для придания им способности проводить вышеуказанные «противокосмические операции» [232]:

- формирование, подготовка и обучение высококвалифицированного персонала;
- модернизация стратегических ядерных сил и средств на основе МБР;
- развертывание средств обнаружения и предупреждения об угрозах, защищенных линий связи, систем навигации и заблаговременное оповещение войск в ходе боевых действий об обстановке;

- обеспечение возможности проведения противокосмических операций за счет приобретения новых систем контроля космического пространства и оборонительных средств, а также расширение возможностей космических полигонов;
- совершенствование способности беспрепятственного управления космическими силами в любом регионе (на любом театре войны);
- проведение работ в следующих областях:
    - наступательные противокосмические операции;
    - немедленное нанесение глобальных ударов неядерными средствами;
    - ведение разведки;
    - наблюдение и сопровождение объектов для получения данных, достаточных для выдачи целеуказания;
- разработка технологий для повышения уровня стандартизации конструкций космических аппаратов и порядка проведения космических операций, интенсификация процесса «спиральной» разработки, а также внедрение технологий, обеспечивающих революционные возможности в области управления и связи, двигательных систем, ядерных и обычных средств поражения, планирования и проведения операций.

Приоритетным направлением является повышение эффективности космических сил для максимального обеспечения развединформацией войск на поле боя. Особую важность для проведения космических операций представляют возможности космических сил по управлению и связи, а также плановому выводу на орбиты космических аппаратов. И, наконец, особое значение, наряду с началом работ в области наступательных противокосмических операций и экстренного вывода КА на орбиту, придается возможностям по ядерному сдерживанию, оборонительным противокосмическим операциям и контролю космического пространства. Все это явится первым шагом к развертыванию ударных космических систем в среднесрочной и долгосрочной перспективе [232].

Космические системы и средства должны предоставлять следующие возможности [232]:

- повышение эффективности космических сил (возможности, повышающие эффективность проведения военных операций на суше, на море, в воздухе и космосе);

- противокосмические операции (возможности, позволяющие завоевывать и удерживать превосходство в космическом пространстве, предоставляющие ВС право использовать космос в своих интересах и лишающие этого права противника);
- применение космических сил (возможности, используемые для выполнения задач с применением систем оружия из космоса (через космос), в результате чего наземные цели будут постоянно находиться под угрозой уничтожения);
- космическое обеспечение (возможности по запуску, в случае необходимости, полезной нагрузки и контролю функционирования КА);
- обеспечение операций в других сферах (функциональная область, которая распространяется на все военные задачи и обеспечивает требуемую для этого инфраструктуру).

Отличительной особенностью применения сил в космосе и из космоса является недостаточное правовое урегулирование данного вопроса. Так, понятие воздушно-космического пространства в международном праве отсутствует. Это связано с различными правовыми режимами космического и воздушного пространств. На воздушное пространство распространяется суверенитет государства, который ограничивает его использование иностранными государствами (разрешительный характер), а при использовании космоса в военных целях он существенно ограничен. Так, резолюция Генеральной ассамблеи ООН «Предотвращение гонки вооружений в космосе» особо подчеркнула обязанность всех государств воздерживаться в своей космической деятельности от угрозы силой или ее применения [269].

Поэтому введение понятия единого воздушно-космического пространства несколько противоречит базовым принципам существующих норм международного права, в котором сферы деятельности в воздушном и космическом пространствах четко разграничены [269].

С позиций реализации норм и принципов международного права единое воздушно-космическое пространство означает, например, либо полный запрет несанкционированных полетов любых аппаратов, включая космические, над территориями суверенных государств, либо полное снятие таких запретов, то есть признание права на свободный полет любых иностранных аппаратов, включая воздушные суда, над любой территорией [269].

Существующий термин «отражение воздушно-космической агрессии» с точки зрения международного права также спорен, так как

не определены признаки факта воздушно-космического нападения. Не урегулирован и вопрос о возможности защиты и поражения космических объектов космическими (или воздушными) средствами [269].

Неясно, как понимать с точки зрения международного права термин «отражение воздушно-космического нападения». Например, какое событие в космосе можно считать фактом воздушно-космического нападения или подготовки к нему? Какие космические объекты необходимо защищать и какие можно поражать воздушно-космическими (то есть воздушными и космическими) средствами, не нарушая норм международного права [269]?

Существующие договоры по космосу принципиально не запрещают военную деятельность в космосе. Так, специалисты выделяют следующие основные зоны военно-космической деятельности, не охватываемые этим договорами [269]:

- развертывание в космосе оружия противоспутниковой борьбы, систем ПРО космического базирования;
- развертывание средств оптико- и радиоэлектронного подавления;
- развертывание оружия, основанного на новых физических принципах (не относящегося к оружию массового уничтожения).

Существует совместная инициатива России и Китая (выдвинутая в 2002 г.) по неразмещению оружия в космосе и неиспользованию силы в отношении космических объектов. По результатам рассмотрения данной инициативы в 2003 г. Генеральная ассамблея ООН приняла резолюцию «Предотвращение гонки вооружений в космическом пространстве». Однако конкретные меры в рамках этой резолюции не обсуждались [269].

В 2005 г. в США была принята военно-космическая стратегия (Space Strategy), задачами которой определены [269]:

- непрерывное управление обстановкой в космическом пространстве и контроль глобальной обстановки космическими средствами США;
- активное обеспечение свободного доступа США в космическое пространство для ведения там военной и другой деятельности (в космосе, из космоса и через космос). Эта задача включает пресечение любых попыток вероятных противников препятствовать доступу США в открытый космос;

- защита и оборона космических средств и систем США от любого воздействия со стороны космических и иных средств противников;
- стратегическая противоракетная и другие виды обороны США космическими оборонительными средствами;
- развертывание и боевое применение в космосе и из космоса обычных (неядерных) наступательных и оборонительных космических средств (ядерные средства некосмического базирования используются через космос);
- развертывание и использование космических средств и систем военного и государственного управления мирного и военного времени, обеспечивающих эффективную реализацию концепции сетецентрической войны военными силами страны и операциями объединенных вооруженных сил в войнах нового облика;
- воспрепятствование военному доступу в открытый космос вероятных противников и развертыванию ими в космосе военных наступательных средств, а также применению таких средств в космосе и из космоса против США.

Данная стратегия предусматривает действия по долгосрочному планированию наращивания возможностей США в космической сфере (рис. 4.24) [230].

Перспективная программа США «Космические ударные системы и средства ПРО» предусматривает развертывание в космосе и в воздушном пространстве обычных (неядерных) боевых ударных систем, способных поражать КА и МБР противника. Предполагается, что вокруг Земли будет создана сеть спутников, которые станут отслеживать все ракетные пуски и поражать стартующие ракеты лазерным лучом из космоса или с борта самолета. Если же ракета с боеголовкой выйдет в космос, то она будет поражена кинетическим оружием. Кроме того, можно говорить о принципиальной возможности применения противоракет дальнего перехвата нового поколения, так называемых нестратегических систем ПРО или ПРО на ТВД, по космическим аппаратам противника в ближнем космосе [269].

Таким образом, США вступили на путь всестороннего развития своих возможностей по использованию космоса в военных целях. Подобные действия, а также создание инновационных образцов космического оружия могут спровоцировать гонку космических вооружений за господство в околоземном пространстве и в конечном итоге, существенно трансформировать способы ведения войн между техно-

логически развитыми странами за счет расширения возможностей высокоточного применения силы на всей территории Земли.

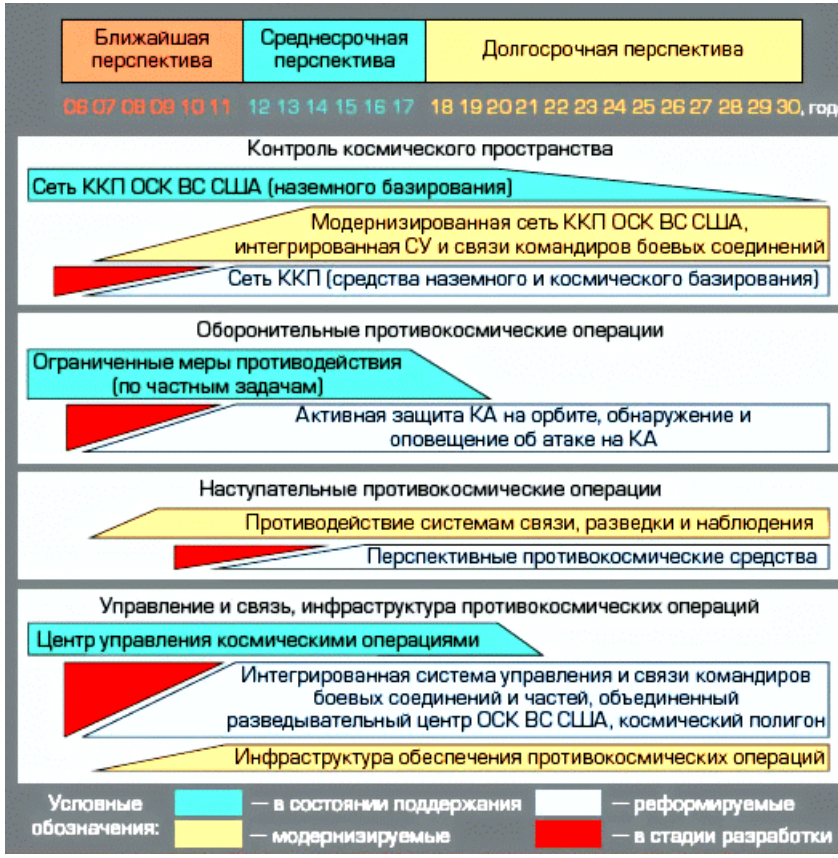


Рис. 4.24. Планы США по наращиванию своих возможностей в космической сфере [230]

4.4.4. Оружие в космической сфере (на примере вооружений ВС США)

Сегодняшний этап разработки средств противоспутниковой борьбы можно определить как начало второго рождения этой тематики, но уже на новой технической и концептуальной базе. После затишья в несколько десятков лет космические державы вновь проводят в космическом пространстве эксперименты по уничтожению, функциональному подавлению и уводу с орбиты космических аппаратов [269].

В настоящее время в мире отсутствуют развернутые системы на основе оружия противоспутниковой борьбы. Однако в той или иной степени подобным потенциалом будут обладать следующие перспективные средства США, находящиеся в различных степенях разработки [347, 262]:

- противоракеты прямого попадания воздушного (типа ASAT), наземного (типа GBI) и морского базирования (типа SM-3);
- лазерное оружие воздушного, наземного и космического базирования;
- воздушно-космические самолеты (подобные тем, что реализуются по программам Falcon и X-37);
- КА-перехватчики и КА-инспекторы (в том числе и малые КА).

В более отдаленной перспективе – противоракеты и лазеры космического базирования.

Ниже представлены основные разработки США, которые могут быть уже на современном этапе использованы для ведения боевых действий в космосе и через космос.

4.4.4.1. Противоспутниковые ракеты

Противоспутниковая ракета ASAT (Anti-Salellile) воздушного базирования разрабатывалась с 1977 по 1985 г и предназначалась для поражения ИСЗ на низких орбитах. В состав комплекса перехвата КА входит самолет-носитель (модернизированный истребитель F-15) и 2 ступенчатая ракета ASAT. Масса ракеты 1200 кг, длина 6,1 м, диаметр корпуса 0,5 м. Ракета подвешивается под фюзеляжем самолета-носителя. В качестве двигательной установки первой ступени применяется ракетный ТТДУ тягой 4500 кг, второй – ТТДУ тягой 2720 кг. Полезная нагрузка – малогабаритный самонаводящийся перехватчик MHIV (Miniature Homing Intercept Vehicle) массой 15,4 кг, длиной 0,46 м и диаметром около 0,3 м [262].

Выведение ракеты ASAT в расчетную точку пространства после ее отделения от самолета-носителя производится инерциальной системой, установленной на 2-й ступени [262].

Перехватчик MHIV состоит из нескольких десятков небольших двигателей, инфракрасной системы самонаведения, лазерного гироскопа и бортового компьютера. На его борту нет взрывчатого веще-

ства, поскольку поражение космической цели осуществляется за счет кинетической энергии при прямом попадании в нее [262].

К моменту завершения работы второй ступени ASAT перехватчик MHIV раскручивается до 20 об/с с помощью специальной платформы. Это необходимо для нормальной работы инфракрасной системы самонаведения и обеспечения стабилизации перехватчика в полете. К моменту отделения перехватчика его инфракрасные датчики, ведущие обзор пространства с помощью восьми оптических систем, должны захватывать цель. Двигатели перехватчика позволяют ему перемещаться в трех плоскостях [262].

Пуск ракеты ASAT с самолета-носителя предполагался осуществлять на высотах 15-21 км как в горизонтальном полете, так и в режиме набора высоты. Для превращения серийного истребителя F-15 в носитель ASAT требовалась установка специального под фюзеляжного пилона и связного оборудования. В пилоне размещается мини-ЭВМ, оборудование для связи самолета с ракетой, система коммутации, резервная батарея питания и газогенератор, обеспечивающий отделение ASAT [262].

Первый пуск экспериментальной ракеты ASAT с самолета F-15 по условной космической цели был произведен в начале 1984 г., а первый успешный перехват – 13 сентября 1985 г. Запущенная ракета ASAT уничтожила американский спутник Soluind на высоте 450 км. В начале 1990-х гг. работы по системе ASAT в США прекращены, однако полученные результаты в процессе реализации программы были использованы в разработке ракет GBI и SM-3 [262].

Противоракета GBI – трехступенчатая твердотопливная противоракета дальнего радиуса действия наземного шахтного базирования – предназначается для заатмосферного перехвата высокоскоростных целей за счет кинетической энергии прямого соударения [262]. Максимальная высота запуска – 2000 км. Расчетная дальность действия ракеты варьируется в зависимости от высоты траектории и составляет 2000-5500 км. Противоракета разгоняется до скорости 8,3 км/с и выбрасывает в космическое пространство перехватчик – спутник массой 64 кг и длиной 1,4 м [95].

Следует особо отметить, что, скорость выводимого в космическое пространство перехватчика может превысить первую космическую, поэтому традиционный термин «дальность действия» для GBI неприменим в полной мере, теоретически перехватчик может перехватить цель в любой точке орбиты. Так как высота перехватываемых це-

лей не превышает 2000 км, то целями перехвата могут быть КА на низких и средних орбитах [95].

Основным поражающим элементом ракеты-перехватчика GBI является заатмосферный кинетический перехватчик EKV (Exoatmospheric Kill Vehicle). Он оснащен электронно-оптической системой наведения, защищенной от посторонней засветки особым кожухом и автоматическими фильтрами. Получая целеуказание с наземной части системы GBMD, перехватчик EKV обнаруживает с помощью инфракрасного телескопа цель и, маневрируя жидкостным двигателем, начинает разгон для ее поражения. Поражение боеголовки осуществляется лобовым тараном на встречном курсе, при этом в момент столкновения с целью скорость EKV составляет порядка 7 км/с. Таким образом, кинетической энергии удара вполне хватает, чтобы полностью уничтожить боевой блок [95].

В отличие от шрапнельных зарядов, кинетический перехватчик при попадании полностью уничтожает цель. Таким образом, при его применении невозможна неопределенная ситуация, когда КА, выведенный из строя шрапнельным снарядом, остается единым целым и продолжает полет по прежней траектории. Кроме того, кинетическое поражение не создает значительных облаков обломков, способных нанести вред другим космическим аппаратам.

Первоначально в рамках программы GBI планировалась разработка кластерного перехватчика, предназначенного для поражения головок от МБР с разделяющимися боеголовками. Согласно проекту, противоракета GBI должна была выводить на орбиту несколько компактных миниатюрных перехватчиков MKV (Multiple Kill Vehicle), наводящихся одновременно на несколько целей. Однако в связи с рядом технологических трудностей и необходимостью сокращения бюджета США программа GBI с MKV была закрыта в 2009 г.

Более подробная информация о ракете GBI в составе системы ПРО США GBMD представлена в подразделе 4.3.4 «Системы противоракетной обороны».

Противоракета Standard Missile 3 (SM-3) – корабельная трехступенчатая ракета компании Boeing, являющаяся основным оружием системы ПРО морского базирования Aegis. Две маршевые ступени ракеты состоят из блоков ускорителей, что позволяет ей развивать более высокую скорость. Третья ступень ракеты SM-3 – разгонная [95].

Ракета-перехватчик SM-3 может уничтожать баллистические ракеты, находящиеся в средней части траектории и летящие за преде-

лами атмосферы, а также КА на низких орбитах с помощью кинетической боеголовки путем ударно-контактного взаимодействия [95].

Работа трех ступеней SM-3 позволяет вывести ракету на встречную траекторию и обеспечить набор достаточной скорости для поражения цели. На конечной фазе полета отделяется заатмосферный малогабаритный кинетический перехватчик LEAP (Lightweight Exo-Atmospheric Projectile), который начинает самостоятельный поиск цели с помощью данных с корабля-носителя и собственной инфракрасной ГСН. Цели могут обнаруживаться на дальностях до 300 км, а коррекция траектории может составлять до 3-5 км. Кинетический перехватчик имеет собственные двигатели для корректировки полета и космического маневрирования, которые осуществляют точное выведение перехватчика на встречный курс. При столкновении энергия удара перехватчика составляет 130 МДж, что более чем достаточно для уничтожения любой баллистической цели [229].

Высота перехватываемых целей до 250 км, а дальность до 300 км применительны к космическим целям – КА на низкой орбите [262].

Всего в 4 испытательных пусках SM-3, проведенных в 2001-2002 гг., был осуществлен успешный перехват имитатора боевого блока баллистической ракеты в космосе на высотах 240-250 км. 11 декабря 2003 г. с эсминца USS Lake Erie была сбита цель на высоте 137 км, при общей скорости сближения 3,7 км/с, вся операция от обнаружения до перехвата заняла 4 мин. 21 февраля 2008 г. ракета SM-3 была выпущена с крейсера Lake Erie в Тихом океане и через 3 мин после старта поразила находящийся на высоте 247 км аварийный разведывательный спутник USA-193, двигающийся со скоростью 7580 м/с. Очередное пробное тестирование модернизированной SM-3, проведенное 16 апреля 2011 г., показало высокую эффективность комплекса по перехвату ракет средней дальности [95].

До 2018 г. корабельные противоракеты SM-3 следующего поколения предусматривается адаптировать к наземному способу базирования. Эти ракеты будут предназначены для перехвата баллистических ракет на восходящем (до начала разделения боеголовок) и нисходящем участках траектории полета на дальности до 1000 км и высотах 70-500 км [95, 228].

Более подробная информация о ракете SM-3 в составе системы ПРО США морского базирования Aegis представлена в подразделе 4.3.4 «Системы противоракетной обороны».

Противоракеты космического базирования типа Brilliant Pebbles. Первоначальные оценки предлагаемого проекта были весьма оптимистичными как по массогабаритным и стоимостным параметрам подобных перехватчиков, так и по их эффективности. Приводились такие данные [262]:

- масса снаряда-перехватчика (без ракетного ускорителя) – 1,5-2,5 кг;
- высота орбиты – 400-500 км;
- количество ракет-перехватчиков – 4000-5000;
- ракеты-перехватчики способны перехватывать БР, дальность полета которых превышает 2000 км, а также низкоорбитальные КА.

Однако учитывая целый ряд трудностей как технического, так и юридического порядка, можно полагать, что работы по перехватчикам космического базирования типа Brilliant Pebbles вряд ли в ближайшее время завершатся разработкой образца, который будет принят на вооружение и включен в систему перехвата. Поэтому центр тяжести работ по перехвату КА сместился в сторону высокоскоростных перехватчиков наземного и морского базирования [262].

Помимо США, созданием оружия противоспутниковой борьбы занимаются и другие технологически развитые страны. Так, например, 11 января 2007 г. кинетическим перехватчиком, запущенным баллистической ракетой, Китай успешно уничтожил свой собственный, уже выведенный из эксплуатации метеорологический спутник Feng Yun 1C (FY-1C), находившийся на полярной орбите высотой около 850 км. При этом кинетический перехватчик, по всей видимости, двигался по суборбитальной траектории [269, 267].

4.4.4.2. Лазерные противоспутниковые системы

За последнее время произошли существенные изменения уровня технической и технологической базы создания лазерного оружия космического базирования. Построены и испытаны мощные химические лазеры, которые могут работать в условиях космоса; создана система наведения и точного сопровождения целей, с помощью которой предполагается решать задачу нацеливания лазерного оружия космического базирования [250].

Эксперименты по исследованию воздействия лазерных лучей на различные материалы целей в вакууме показали, что при определенных условиях облучения лазерным лучом с плотностью энергии на

поверхности цели порядка 10 Дж/см^2 механические повреждения могут получить солнечные батареи, оптические датчики, обтекатели антенн, а при плотности энергии на цели порядка 1000-5000 Дж/см^2 в вакууме уязвимым оказывается и алюминиевый корпус ускорителя баллистической ракеты [250].

Программа лазерной системы ABL (Airborne Laser) воздушного базирования. В США с 1996 г. дочерней фирмой Boeing Defense and Space Group велись разработки лазерного оружия авиационного базирования с целью создание воздушного лазера ПРО, способного сбивать баллистические ракеты на дальности 400-460 км. В результате проекта был разработан химический лазер Chemical Oxygen Iodine Laser (COIL) на основе переохлажденного жидкого кислорода и металлического йода, генерирующий волну 1,3 мкм. Лазер этого типа способен вырабатывать очень узкий, хорошо сфокусированный луч мощностью 1 МВт с низким затуханием в атмосфере. В качестве носителя лазера ПРО выбрали самый большой на то время транспортный самолет Боинг-747-400F стартовой массой 340 т, из которых 72 т заняты лазерным оборудованием. В фюзеляж удалось вместить только 6 химических модулей COIL общей мощностью 6 МВт вместо запланированных 14. Это сразу снизило проектную дальность действия лазера до 250 км. Запаса жидкого переохлажденного кислорода и мелкодисперсного порошкообразного йода на борту хватало для осуществления 20-40 лазерных «выстрелов». В 2005 г. лазерную ПРО испытали в полете, после чего Пентагон собирался заказать 7 таких машин. Но вскоре обнаружились два непреодолимых технологических препятствия. Во-первых, на каждый 1 Вт электроэнергии вырабатывается 4 Вт тепловой энергии, которую невозможно отвести в полном объеме и которая идет на нагрев самого оборудования и самолета-носителя. При мощности в 6 МВт перегрев самолета становиться катастрофическим, тем более что на борту находятся еще и емкости с жидким кислородом. Второй барьер плавление линз с расфокусировкой луча лазера. Температура излучения такова, что кварцевое стекло не выдерживает. В результате в июне 2009 г. Пентагон прекратил финансирование проекта Airbome Laser в связи с его бесперспективностью [316].

Противоракетные лазерные комплексы космического базирования Space Based Laser (SBL). В качестве одного из перспективных ударных средств разрабатываемой в США системы перехвата космических целей в течение многих лет рассматривается лазерное оружие космического базирования SBL (Space Based Laser). Работы в рамках данного проекта ведутся с участием компаний Boeing,

Lockheed Martin и TRW. Несмотря на чрезвычайную сложность проблем, связанных с созданием космического лазерного оружия, работа над ним в США продолжается. Значительные усилия США по созданию комплексов лазерного оружия космического базирования, предпринимавшиеся несмотря на сложность достижения поставленных целей, объясняются огромными преимуществами, получаемыми в случае создания космической системы, оснащенной лазерным оружием. Поскольку лазерное излучение распространяется в космосе почти без потерь энергии, то потенциальная дальность действия таких лазеров будет чрезвычайно большой. Таким образом, лазерные комплексы космического базирования позволяют воздействовать на космические цели практически мгновенно и на больших расстояниях. Однако достижение требуемых ТТХ для такого комплекса представляется исключительно трудной научно-технической задачей. Кроме того, для создания боеспособной системы, обладающей требуемой эффективностью, необходимо развертывание большой космической группировки.

Считается, что система из четырех КА с лазерами мощностью 5 МВт и управляющими зеркалами диаметром 4 м сможет выводить из строя каждый одиночный стратегический бомбардировщик дальнего действия, значительную часть баллистических ракет, запускаемых с подводных лодок, и 50% МБР. Система из 24 КА с лазерами мощностью 10 МВт и зеркалами 10 м в диаметре сможет обеспечить поражение почти всех баллистических ракет, запускаемых с подводных лодок, подавляющую часть МБР и еще некоторое число единиц других видов вооружения. Такая система сможет обеспечить поражение баллистических ракет темпом 2 ед/с, даже если они будут иметь удвоенную по сравнению с современной защиту от лазерного излучения [250].

Однако проведенный американскими специалистами анализ задач первого эшелона системы ПРО для КА с лазерным оружием (с химическим лазером мощностью 5 МВт и управляющим зеркалом 4 м) по перехвату всех стартующих баллистических ракет на участке выведения привел к следующим выводам. Чтобы обеспечить наблюдение за ракетоопасными районами потенциального противника с целью своевременного обнаружения старта средствами такой системы и чтобы при этом хотя бы один КА находился в пределах прицельной дальности, необходимо иметь группировку из 50 КА на орбитах высотой порядка 1000 км. Тогда в условиях массового пуска 1000 баллистических ракет, стартующих в интервале около 8 мин, каждая лазер-

ная установка КА должна иметь потенциал в 1000 «выстрелов». При этом на каждый «выстрел» затрачивается 0,5 с, поскольку такой короткий промежуток времени взаимодействия лазерного луча химического лазера с материалом цели (в перспективе защищенной от лазерного излучения) является недостаточным для поражения цели (для этого необходимы десятки и сотни секунд) [250].

Дополнительные трудности состоят в доставке топлива на орбиту. При достигнутом энергосъеме химического лазера на один «выстрел» требуется порядка 660 кг топлива. Доставка на орбиту топлива, требующегося для производства 1000 «выстрелов», – невыполнимая задача для существующих транспортных средств, поэтому в проектах перспективных систем ПРО для КА с лазерным оружием отводятся ограниченные функции. Ожидается, что такие КА смогут поражать цели темпом в 2 с на расстоянии около 1600 км в любой стадии полета баллистической ракеты [250].

В настоящее время после того, как на проект SBL было потрачено несколько миллиардов долларов, он официально закрыт, стенды законсервированы, а исследования переведены в разряд технологических [14, 316].

4.4.4.3. Ускорительные (пучковые) противоспутниковые системы

Помимо лазерного оружия, разрабатываются концепции космического ускорительного (пучкового) оружия.

Основным элементом такого оружия должны быть ускорители нейтральных и заряженных частиц. Устройства ускорителей электронов и атомов водорода, и возможные области их применения в оружии существенно отличаются. Электронный пучок может распространяться только в специально созданном в атмосфере канале сильно разреженного и ионизированного воздуха, который его ослабляет, нейтрализуя при этом объемный заряд, который приводит к рассыпанию пучка. Магнитное поле Земли сильно искривляет траекторию электронного пучка в вакууме, что исключает возможность создания ускорительного оружия большой дальности и, прежде всего, космического. Прямолинейно распространяться может только пучок нейтральных атомов водорода, причем в ускорителе разгоняются отрицательные ионы водорода, которые на выходе нейтрализуются в специальной газовой ячейке. Однако даже небольшие остатки атмосферы (на высотах

до 200 км) легко ионизуют нейтральные атомы, а образующиеся при этом протоны сильно отклоняются магнитным полем Земли [14].

Действие на цель ускорительного оружия носит как поверхностный, так и объемный характер в силу большой глубины проникновения частиц, причем основные планы создания ускорительного оружия связывались, в первую очередь, именно с его уникальными свойствами. Объемный характер воздействия на цель, обусловленный большой глубиной проникновения ускоренных до околосветовых скоростей частиц, приводит к наблюдаемым внешним вторичным эффектам, пропорциональным массе цели, что позволяет выделить и распознать боевой блок в составе сложной баллистической цели. Именно эта задача и ставилась американцами в программе создания космического ускорительного оружия для национальной системы ПРО. Другим механизмом воздействия пучка частиц является радиационное повреждение полупроводниковых элементов электроники, наступающее, как правило, при уровнях воздействия, существенно меньших, чем необходимо для иных механизмов поражения цели. Такой механизм рассматривается для поражения космических аппаратов, электроники ракет и боевых блоков в космосе. Третий механизм воздействия, основанный на радиационных эффектах, обусловлен разложением под действием частиц химических соединений с образованием активных радикалов или свободных электронов, что инициирует в веществе химические реакции. При воздействии на взрывчатое вещество или твердое топливо начинается процесс горения [14].

Основной упор в работах по ускорительному оружию в США был сделан на создание космических комплексов ПРО, решающих попутно и задачи противокосмической обороны. Наибольший размах эти работы получили в рамках программы СОИ, однако они не вышли из стадии фундаментальных и прикладных исследований по изысканию путей создания такого оружия. Возможное принятие на вооружение космического пучкового оружия возможно не ранее 2020 г. Оно может найти применение для нарушения устойчивости орбитальной космической группировки, поражения одиночных баллистических ракет на заатмосферном участке без срабатывания аппаратуры ядерного подрыва, а также уничтожения других средств воздушно-космического нападения и разведки [14, 300].

4.4.4.4. Воздушно-космические самолеты

В 1999 г. NASA совместно с компанией Boeing начали программу создания беспилотного воздушно-космического самолета X 37B. Стоимость его разработки составила 173 млн долларов, а его использование предусматривалось в качестве средства фото- и радиолокационной разведки, перехватчика космических целей или ударного самолета с ракетой класса «космос – Земля». По имеющимся данным, космолет обладает следующими характеристиками: взлетная масса около 5 т, масса полезного груза 900 кг, время пребывания в космосе до 270 дней. Первый экспериментальный полет, а именно его испытание путем сбрасывания, был совершен 7 апреля 2006 г. В дальнейшем, 22 апреля 2010 г., X-37B ушел в первый полет, задачи которого и ход их решения были засекречены [95].

Ряд экспертов высказывают предположение, что за 225 суток, проведенных в космосе, космолет провел реальные пуски боевых ракет. Именно в это время был сбит российский военный спутник, что официально объяснили возможным попаданием в него метеорита. Вместе с тем до сих пор руководство ВВС США не публикует никаких подробностей о целях и задачах полета X-37B [95].

Принимая во внимание достаточный объем грузового отсека космического аппарата, можно предположить, что X-37B способен нести любую разведывательную аппаратуру и, безусловно, некоторые системы вооружения. Наблюдения, сделанные с помощью оптической аппаратуры, подтверждают высокую маневренность аппарата. За все время его нахождения на орбите было произведено четыре резких изменения траектории движения. Таким образом, аппарат может использоваться для перехвата и захвата спутников. Несмотря на столь явную боевую ориентацию аппарата X-37B, американские военные продолжают настаивать на том, что он является всего лишь летающей в космосе лабораторией [95].

Космолет X-37B вернулся на Землю 3 декабря 2010 г. после семи месяцев беспилотного полета. Посадка в автоматическом режиме была осуществлена на взлетно-посадочную полосу базы ВВС США Ванденберг, штат Калифорния. В период пребывания на орбите X-37B получил семь повреждений обшивки, по официальной версии, в результате столкновения с космическим мусором [95].

Таким, образом, первый космический полет X-37B состоялся 22 апреля 2010 г. и продолжался 225 дней, второй космический полет

начался 5 марта 2011 г. и продолжался 468 дней, третий космический полет – 11 декабря 2012 г., с продолжительностью полета 674 дня.

Боевые аппараты, которые создаются по программе X-37, уже сегодня позволяют выводить на орбиту до 3 боеголовок и доставлять их к цели, минуя систему предупреждения о ракетном нападении и другие средства контроля. В перспективе американский воздушно-космический самолет, выведенный на орбиту с гиперзвуковыми ракетами на борту, будет способен нести там боевое дежурство в течение нескольких лет – в постоянной готовности к мгновенному применению оружия по сигналу с земного командного пункта. Орбитальная группировка из нескольких десятков таких аппаратов будет способна обеспечивать поражение любой цели на земной поверхности и в космосе в течение нескольких минут [347].

В июле 2014 г. представители DARPA анонсировали первую фазу реализации нового проекта по созданию беспилотного космического корабля XS-1 (eXperimental Spaceplane 1). В долгосрочных планах агентства – добиться того, чтобы беспилотный космический корабль смог совершить 10 полетов за 10 дней, хотя бы в одном полете достигнув скорости 10 М. Стоимость каждого совершенного рейса не должна превышать 5 млн долларов. При этом аппарат должен будет нести на борту полезную нагрузку массой от 1,36 до 2,37 т. Гиперзвуковые полеты экспериментального американского космического беспилотника XS-1 намечены на 2018 г. Автономный гиперзвуковой космолет XS-1 будет совершать полеты как обычный самолет, но при этом сможет также выводить спутники на низкую орбиту Земли на отделяемой от аппарата ступени. Предполагается, что вторая ступень ракеты-носителя будет осуществлять выпуск полезного груза на суборбитальной высоте полета, как только она сможет отсоединиться от основного корпуса. Сам беспилотный аппарат вернется назад на Землю и практически сразу же начнет готовиться к следующим полетам. Представители агентства DARPA отмечают, что они собираются финансировать три компании, которые будут работать над созданием собственных демонстраторов беспилотного космолета XS-1. Денежные средства будут выделены компаниям Northrop Grumman Corporation, сотрудничающей с Virgin Galactic, Masten Space Systems, сотрудничающей с XCOR Aerospace, и компании Boeing, работающей с Blue Origin [263].

В последнее время в США к разработке космолетов подключается все большее количество частных компаний. Так, ведется разработка космического беспилотного корабля Dream Chaser, который бу-

дет выводиться на орбиту при помощи ракеты-носителя Atlas V, при этом корабль должен размещаться в верхней части ракеты, в отличие от расположения сбоку, как это было с кораблями Space Shuttle. Такое расположение делает невозможным повреждение космического корабля в момент запуска. Посадка будет производиться горизонтально по самолетному. При этом предусмоатривается не просто планирование, как у шаттлов, а полноценный самостоятельный полет с посадкой на любые ВПП длиной не менее 2500 м [264].

Проведенный анализ возможностей воздушно-космических самолетов как систем оружия показывает, что они будут обладать значительными стратегическими преимуществами, позволяющими выполнять боевые задачи на качественно новом уровне. Предполагается, что основными задачами этих систем оружия будут [269]:

- поражение стратегически важных объектов, включая критичные по времени, в том числе мобильные наземные цели в глубине территории противника;
- ведение стратегической воздушной разведки;
- перехват воздушно-космических целей;
- долговременное хранение и оперативное развертывание группировок малых КА;
- вывод на околоземные орбиты КА различного назначения;
- инспекция, перехват и захват спутников;
- переброска войск и военной техники на трансконтинентальную дальность.

4.4.4.5. Космические аппараты инспекторы и перехватчики

Как известно, США отвергли российско-китайское предложение о заключении договора о неразмещении в космосе оружия и приступили к разработке боевых КА. Планируют создать орбитальную группировку боевых КА нового поколения для ведения вооруженной борьбы в космосе и из космоса, которая будет состоять из следующих систем [269]:

- КА наблюдения Brilliant Eyes (50-70 аппаратов) для сопровождения целей в космосе, селекции боеголовок и ложных целей, выдачи целеуказаний на перехватчики наземного базирования и орбитальные перехватчики. Для точного измерения дальности и определения траектории полета цели будут использоваться лазерные локаторы;

- КА-инспекторы XSS (eXperimental Satellite System), обеспечивающие решение задач инспекции, а возможно, и нейтрализации КА. Предусмотрена ретрансляция получаемых ими данных на Землю через платформу-носитель в реальном масштабе времени;
- КА-перехватчики KEASat для выведения из строя КА противника прямым кинетическим воздействием или дистанционно с использованием лазерных установок.

В апреле 2005 г. ракетой-носителем Minotaur (модифицированный конверсионный вариант МБР Minuteman-2) был выведен на орбиту КА XSS-11. Этот космический аппарат создан по программе «Экспериментальный космический аппарат XSS» и реализуется исследовательской лабораторией ВВС (AFRL) и агентством DARPA в МО США. Цель программы и проекта XSS заключается в создании микроспутника, способного проводить автономные операции вблизи и вокруг других космических объектов, а именно сближение на орбитах, маневрирование вблизи и вокруг них для опознавания и инспектирования, стыковки к космическим аппаратам, перепозиционирование и изменение ориентации и др. [269].

4.4.4.6. Космическая система радиоэлектронной борьбы и мониторинга космического пространства

В настоящее время в США осуществляется программа «Технологии космического пространства», в рамках которой проводятся НИОКР, направленные на создание противоспутниковых систем и средств контроля космического пространства [250].

С 2008 г. ведется разработка систем получения информации о ситуации в локальном космическом пространстве – CSASSA, которые будут иметь комплект средств предупреждения, реагирующих на противоспутниковое оружие и угрозы естественного происхождения [250].

По программе «Противокосмические системы» осуществляется проектирование и создание мобильной системы радиоэлектронного подавления спутниковой связи CCS, представляющей собой наступательную противоспутниковую систему РЭБ, предназначенную для постановки помех спутникам космической связи, и систему RAIDRS быстрого обнаружения и опознавания, а также оповещения о нападении на космический объект [250].

4.4.4.7. Высотные ядерные взрывы

До подписания в 1967 г. Договора о космосе как СССР, так и США успели провести целую серию высотных ядерных взрывов, позволивших сформировать общее представление о воздействии, которое может оказать примененное в космосе ядерное оружие.

В 1958 г. США провели операцию «Аргус», главной целью которой было изучение влияния поражающих факторов ядерного взрыва, который происходит в космическом пространстве, на расположенные на земле средства связи, радиолокаторы, электронную аппаратуру баллистических ракет и спутников. Для испытаний использовались ядерные заряды мощностью 1,4-1,7 кт. Первый ядерный взрыв произошел на высоте 161 км, второй – на высоте 292 км, а последний третий взрыв – на высоте 750 км (по другим данным 467 км) над поверхностью Земли [268].

Результатом высотного ядерного взрыва был очень сильный электромагнитный импульс, обладавший высокой разрушительной силой на расстоянии более 1900 км [268].

Так, при американских испытаниях на острове Охау внезапно погасло уличное освещение, жители перестали принимать сигнал местной радиостанции, нарушилась телефонная связь. Также нарушилась и работа высокочастотных систем радиосвязи [268].

При проведении испытаний в СССР в 1961-1962 гг. электромагнитный импульс высотного ядерного взрыва на высоте 300 км стал причиной помех в радиолокаторах системы ПВО на расстоянии около 1000 км. Подземный силовой кабель, проходящий на глубине 90 см протяженностью 1000 км, соединяющий Целиноград и Алма-Ату, был выведен из строя. Электромагнитный импульс стал причиной возникновения пожаров из-за коротких замыканий в электроприборах. Один из пожаров возник на Карагандинской ТЭЦ-3. Также были выведены из строя более 570 км телефонной линии, проходящей над землей [141].

Во время проведения всех высотных испытаний ядерного оружия в космосе возникало облако заряженных частиц, которые через определенное время деформировались магнитным полем Земли и вытягивались вдоль ее естественных поясов, повторяя их структуру. Эти интенсивные искусственные радиационные пояса стали причиной выхода из строя спутников, которые находились на низких околоземных орбитах [268].

4.5. Робототехнические комплексы

4.5.1. Общие тенденции развития робототехнических комплексов

Анализ опыта военных конфликтов, показывает, что современные боевые действия, ведущиеся в соответствии с концепцией сетецентрической войны, характеризуются следующими основными особенностями: возрастание роли информационного противоборства, использование нетрадиционных форм ведения боевых действий, повышение точности и избирательности действия оружия, внедрение новых систем управления, разведки, компьютерного моделирования. Исходя из этих особенностей, общими технологическими тенденциями развития вооружения является интеллектуализация, миниатюризация, снижение энергопотребления, многофункциональность, автономность, снижение массы и удобство снабжения [13].

По мнению отечественных и зарубежных специалистов, в боевых действиях будущего одним из наиболее перспективных видов вооружения и военной техники, интегрирующим большинство из перечисленных направлений, будут робототехнические комплексы военного назначения. При этом ряд специалистов предполагает, что широкомасштабное внедрение роботов и технологий робототехники изменит способы ведения операций (боевых действий) и технический облик перспективных систем ВВТ, повысит эффективность их применения, а также обеспечит сокращение потерь личного состава [13].

Планируется, что к 2030 г. доля безэкипажных средств составит 52% от количества экипажных боевых машин. При этом, по оценкам американских военных специалистов, боевые возможности подразделений нового типа возрастут в 2-2,5 раза (рис. 4.25) [13].

Создание робототехнических комплексов военного назначения требует существенной проработки наиболее важных технологий, необходимых для создания всей номенклатуры перспективных робототехнических средств. При этом типовой образец робота военного назначения может быть представлен в виде совокупности функционально связанных элементов. В частности [93]:

1. Базовый носитель – это может быть шасси или корпус любой конфигурации, для применения в различных средах.
2. Специализированное навесное (встраиваемое) оборудование в виде набора съемных модулей полезной (целевой) нагрузки.

3. Средства обеспечения и обслуживания, используемые при подготовке к применению и технической эксплуатации робота.

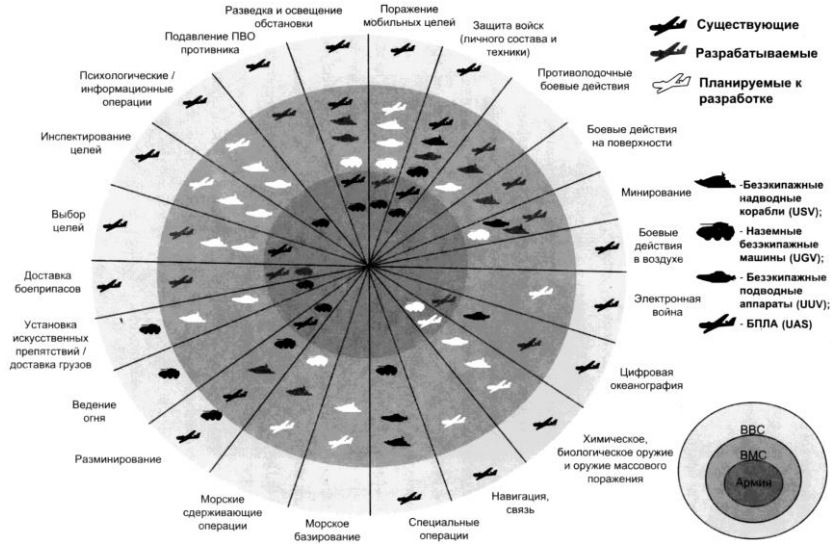


Рис. 4.25. Текущие и перспективные задачи, решаемые военными роботами в различных сферах и в интересах всех видов ВС США [13]

Состав специализированного оборудования устанавливается исходя из функционального предназначения робота и может включать [93]:

- средства разведки;
- средства вооружения;
- навигационные устройства;
- специальное технологическое оборудование;
- средства телекоммуникации;
- специализированные вычислители с программно-алгоритмическим обеспечением;
- средства РЭБ;
- защитные средства.

Помимо этого, робототехника требует обеспечения и обслуживания, то есть в состав комплекса дополнительно включаются [93]:

- диспетчерский пункт управления, контроля и обработки информации;
- средства доставки, транспортировки и запуска;

- средства снаряжения, заправки и зарядки;
- подкомплекс подготовки специалистов;
- комплект руководящих документов;
- комплект запасного имущества и принадлежности (ЗИП).

Такое представление типового робота позволяет выделить технологии, критичные для разработки перечисленных элементов.

Критичные технологии робототехники можно декомпозировать на основные, т.е. разрабатываемые непосредственно для робототехнических комплексов, и вспомогательные, разрабатываемые для широкой номенклатуры образцов вооружения и имеющие перспективу применения при создании роботов военного назначения [13].

К основным могут быть отнесены следующие технологии [13]:

- систем очувствления и обработки сенсорной информации, оценки ситуации и планирования поведения;
- автоматического наведения и управления оружием;
- дистанционного и автономного управления движением;
- автоматического распознавания образов (целей), анализа ситуаций и динамических сцен;
- искусственного интеллекта и обучения;
- человекомашинного интерфейса;
- интеллектуальных систем группового управления.

К числу вспомогательных можно отнести технологии [13]:

- автоматизированного управления;
- создания и функционирования новых перспективных конструкций;
- энергетики;
- создания и применения новых материалов и веществ;
- геоинформационные и точного глобального позиционирования;
- создания перспективных систем датчиков и их элементов;
- создания оптических и оптико-электронных средств.

Обладание такими технологиями – залог успеха в обеспечении необходимой степени автономности и интеллектуальности БПЛА, наземных робототехнических средств и автономных морских аппаратов.

Используя предложенную сотрудниками Оксфордского университета наглядную классификацию, можно систематизировать «способности» роботов по четырем поколениям [90]:

- «уровень ящерицы» – соответствует быстродействию процессоров универсальных роботов первого поколения, кото-

рое составляет от 3 тыс. до 1 млн команд в секунду (MIPS – Million Instructions per Second). Основное назначение таких роботов – получение и выполнение только одной задачи, которая программируется заранее;

- «уровень мыши» – роботы второго поколения, которые могут реализовывать адаптивное поведение, то есть обучение непосредственно в процессе выполнения заданий;
- «уровень обезьяны» – роботы третьего поколения, которые строятся на основе процессоров от 10 млн MIPS. Особенность таких роботов в том, что для получения задания и обучения требуется только показ или объяснение;
- «уровень человека» – четвертое поколение роботов, которое способно мыслить и принимать самостоятельные решения.

В работе [109] представлена классификация боевых роботов по степени их зависимости или, точнее, независимости от человека (оператора):

- роботы 1-го поколения – это устройства с программным и дистанционным управлением, способные функционировать только в организованной среде;
- роботы 2-го поколения – адаптивные, имеющие синтетические органы «чувств» и способные функционировать в заранее неизвестных условиях и приспосабливаться к изменениям обстановки;
- роботы 3-го поколения – интеллектуальные, имеют систему управления с элементами искусственного интеллекта (созданы пока лишь в виде лабораторных макетов).

Западные же специалисты делят роботов на три категории [109]:

- «человек-в-системе-управления» (human-in-the-loop) – беспилотные машины, способные самостоятельно обнаруживать цели и осуществлять их селекцию, однако решение об их уничтожении принимает только человек-оператор;
- «человек-над-системой-управления» (human-on-the-loop) – системы, способные самостоятельно обнаруживать и выбирать цели, а также принимать решения на их уничтожение, но человек-оператор, выполняющий роль наблюдателя, в любой момент может вмешаться и скорректировать или заблокировать данное решение;

- «человек-вне-системы-управления» (human-out-of-the-loop) – роботы способные обнаруживать, выбирать и уничтожать цели самостоятельно без человеческого вмешательства.

Сегодня наиболее распространены боевые роботы первого поколения (управляемые устройства) и быстро совершенствуются системы второго поколения (полуавтономные устройства). Для перехода к использованию боевых роботов третьего поколения (автономных устройств) специалисты разрабатывают самообучающуюся систему с искусственным интеллектом, в которой будут соединены возможности самых передовых технологий в области навигации, визуального распознавания объектов, искусственного интеллекта, вооружения, независимых источников питания, маскировки и др. Такие боевые системы будут значительно опережать человека в скорости распознавания окружающей среды (в любой сфере), а также в скорости и точности реагирования на изменения обстановки [109].

Нынешнее состояние микроэлектроники развитых стран уже позволяет применять робототехнические средства для выполнения полноценных задач с минимальным участием человека. Однако конечной целью является полная замена человека на его виртуальную копию с такими же возможностями для скорости принятия решения, объема памяти и корректного алгоритма действия [90].

Системы на основе искусственных нейронных сетей уже научились распознавать отдельные объекты. По прогнозам специалистов, полностью автономные боевые системы могут появиться уже через 20-30 лет или даже раньше. Ряд экспертов полагает, что будут созданы роботы-андроиды, способные заменить солдата на любом участке боевых действий: на суше, на воде, под водой или в воздушно-космической среде. При этом высказываются опасения, что автономные боевые роботы, каким бы совершенным искусственным интеллектом они ни обладали, не смогут, как человек, анализировать поведение находящихся перед ними людей и, следовательно, будут представлять угрозу для невоюющего населения [109].

Американские специалисты считают, что если попытаться сопоставить способности человека с возможностями компьютера, то такой компьютер должен производить 100 трлн операций в секунду и обладать достаточной оперативной памятью. В настоящее время возможности микропроцессорной техники в 10 раз меньше. В связи с этим принципиально важное значение имеет наращивание быстродействия и миниатюризация разрабатываемых микропроцессоров. Сегодня минимальные размеры процессоров на основе кремниевых полу-

проводников ограничены технологиями их производства, базирующимися на ультрафиолетовой литографии. И, по данным доклада аппарата министра обороны США, эти предельные размеры в 0,1 мкн будут достигнуты уже к 2020 гг. Вместе с тем альтернативой ультрафиолетовой литографии может стать применение оптических, биохимических и квантовых технологий создания переключателей и молекулярных процессоров. По мнению специалистов, процессоры, разрабатываемые с использованием методов квантовой интерференции, могут увеличить скорость вычислений в тысячи раз, а нанотехнологии – в миллионы раз. Кроме того, в интересах создания робототехнических комплексов необходимо уделить серьезное внимание и перспективным средствам связи, которые, по сути, являются критическими элементами успешного применения беспилотных и роботизированных средств [90].

Кроме необходимости развития вычислительных систем и систем связи, развитие робототехники требует использования самых современных технологий создания [90]:

- трансгенных биополимеров, применяющихся при разработке ультралегких, сверхпрочных, эластичных материалов с повышенными характеристиками малозаметности для корпусов БПЛА и других робототехнических средств;
- углеродных нанотрубок, используемых в электронных системах БПЛА. Кроме того, покрытия из наночастиц электропроводных полимеров позволяют на их основе разрабатывать систему динамического камуфляжа для робототехнических и других средств вооруженной борьбы;
- микроэлектромеханических систем, объединяющих в себе микроэлектронные и микромеханические элементы;
- водородных двигателей, позволяющих снизить шумность робототехнических средств;
- «интеллектуальных материалов», выполняющих определенную функцию под влиянием внешних воздействий. Например, для беспилотных летательных аппаратов агентство передовых оборонных исследовательских проектов (DARPA) проводит эксперименты по разработке концепции изменяющегося в зависимости от режима полета крыла, что позволит существенно повысить аэродинамические характеристики БПЛА;
- магнитных наночастиц, способных обеспечить прорыв в разработке устройств хранения информации, существенно

расширив объем памяти робототехнических систем. Потенциал технологии, достигаемый за счет использования частиц размером 10-20 нм, – 400 Гбит на кв. см.

Несмотря на нынешнюю экономическую непривлекательность развития многих проектов и исследований в принципиально новых отраслях, военное руководство ведущих зарубежных стран проводит целенаправленную долгосрочную политику в области разработки перспективных роботизированных и беспилотных средств вооруженной борьбы. При этом рассчитывают не только сохранить личный состав, сделать решение всех боевых задач более безопасным, но и в перспективе разработать инновационные и эффективные средства для обеспечения национальной безопасности, борьбы с терроризмом и иррегулярными угрозами, а также эффективного проведения современных и будущих операций [90].

Планами роботизации ВС США предусмотрены следующие направления работ по параметрам робототехники:

- энергоснабжение;
- возможность функционирования в сложных условиях;
- способы излучения сигнала;
- структуры протоколов связи;
- системы описания объектов;
- распознавание человека;
- взаимосвязь человека с роботом;
- навигация;
- преодоление препятствий;
- приводы устройств и механизмов;
- повышение эффективности манипуляторов.

Самой сложной и неоднозначной проблемой на пути создания полностью автономных робототехнических комплексов военного назначения является легитимность и моральная возможность передачи машине права на убийство человека. Однако это моральная проблема, человека, но никак не робота, не технологии. Одним из вариантов решения этой проблемы может стать несмертельное оружие в арсенале обладающего искусственным интеллектом боевого робота, способного действовать полностью автономно, независимо от человека [326].

Кроме того, развитие робототехники делает актуальным ряд новых задач человекомашинного взаимодействия. Так, в вооруженных силах США в настоящее время разрабатываются концепции применения автономных роботизированных систем военного назначения, направленные на «создание партнерства между людьми и роботами,

позволяющего им работать в рамках синергетических команд». В рамках этих концепций прорабатываются варианты формирования боевых подразделений, в состав которых предположительно будут входить 150 солдат и офицеров и около 2000 роботов [326].

Роботизация принципиально меняет не только организационную структуру и тактику действий подразделений войск, но и социальную структуру ВС. В частности, к порожденным роботизацией вызовам следует отнести значительное перераспределение социальных ролей в воинских подразделениях. Уже сейчас проявляются проблемы, связанные с новым видом социальных отношений: «человек» – «автономный боевой робот с искусственным интеллектом». Роботизация переводит «живых» военнослужащих из психологически понятного состояния войны как борьбы человека против человека в плоскость борьбы человека против «разумной машины», нацеленной на убийство людей. В новых условиях отдельного решения потребует не только организация совместных действий роботов и людей на поле боя, но и проблема совместного размещения и совместной боевой подготовки людей и роботов вне этого времени [111].

Еще одной сложной задачей является проблема коммуникации, прежде всего, между людьми-исполнителями и роботами-командирами, которая может усугубляться недостаточной степенью адаптированности роботов к совместным действиям с людьми. Несомненно, на этой почве могут возникать не только трения, но и открытая конфронтация [111].

Не менее сложной может стать и социально-психологическая адаптация военнослужащих-людей, длительное время взаимодействовавших на поле боя с боевыми роботами как союзниками и как противниками. Так, в ходе активного внедрения роботов в состав группировок американских войск в Афганистане и Ираке известно немало случаев привязанности военнослужащих к своим «подшефным» роботам, а также к восприятию их как своих боевых товарищей или талисманов. Будущее активное взаимодействие военнослужащих с автономными роботами, обладающими развитым искусственным интеллектом, может только усугубить проблему[111].

Одним из главных приоритетов в развитии вооруженных сил развитых стран является создание боевых роботов и робототехнических комплексов воздушного, наземного и морского базирования. За последние 20 лет такие страны как США, Великобритания, Франция, Германия, Китай и Израиль в 20-30 раз увеличили объемы финансирования военных НИОКР по созданию боевых роботов и робототехниче-

ских комплексов. Бесспорным мировым лидером и инициатором крупных военных программ в этой области являются США (их доля работ составляет 65-75% общего мирового объема). К настоящему времени именно США добились наиболее ощутимых результатов в создании робототехнических комплексов военного назначения. Развитию военной робототехники в США способствует долгосрочное планирование и интенсивность проводимых в этой области работ. Еще в 1988 г. министерство обороны США в рамках специальной программы инициировало крупномасштабные исследования, результатом которых должно было стать создание боевых роботов. За 20 последующих лет на свет появилось более 200 прототипов боевых машин, способных вести военные действия самостоятельно или по командам оператора, управляющего ими дистанционно. Большинство роботов предназначено для патрулирования, ведения разведки, разминирования, доставки грузов и ряда других военных целей. Некоторые образцы способны самостоятельно принимать решения об открытии огня по противнику [29, 89, 164].

В планах и программах развития военной робототехники Unmanned Vehicles (UV) министерство обороны США выделяет следующие категории технических средств и робототехнических комплексов на их основе [164]:

- беспилотные летательные аппараты (БПЛА) – Unmanned Air Vehicles (UAV);
- мобильные наземные роботы (МНР) – Unmanned Ground Vehicles (UGV);
- безэкипажные наводные платформы (безэкипажные надводные корабли и маломерные суда – БНК) – Unmanned Surface Vehicles (USV);
- необитаемые подводные аппараты (НПА) – Unmanned Underwater Vehicles (UUV), которые делятся на:
    - дистанционно управляемые НПА (Remotely Operated Vehicles – ROV);
    - автономные НПА (Autonomous Underwater Vehicles – AUV).

В декабре 2007 г. были утверждены основные направления развития безэкипажных и беспилотных систем (Unmanned Systems Roadmap) на 2007-2032 гг., определяющие цели и направления создания робототехнических средств наземного, морского и воздушного базирования [13].

В США роботизация вооруженных сил возведена в ранг государственной политики. Американцы намерены постепенно отказаться от практики, когда одна система оружия заменяется на новую, более совершенную, и перейти к разработке целых комплексов роботизированных систем, заменяющих или дополняющих десятки традиционных систем оружия [89].

В настоящее время вооруженные силы США широко применяют военных роботов при ведении боевых действий в военных конфликтах новейшего периода. Так, в Ираке использовалось 365 единиц роботов различного назначения 32 типов. В частности, применение дистанционно управляемых инженерных машин при разминировании минных полей позволило в 2-3 раза увеличить темп наступление войск и значительно сократить потери личного состава. Кроме того, использование БПЛА для ведения тактической разведки в ходе боевых действий в Афганистане и Ираке позволило резко сократить сроки проведения боевой стадии операции [13].

До недавнего времени основные роботизированные средства разрабатывались в рамках программы FCS (Future Combat System), которая являлась составной частью полномасштабной программы модернизации техники и вооружения сухопутных войск США. В рамках программы осуществлялась разработка [90]:

- разведывательных сигнализационных приборов;
- автономной ракетной и разведывательно-ударной систем;
- беспилотных летательных аппаратов;
- разведывательно-дозорных, ударно-штурмовых, портативных дистанционно управляемых, а также легких дистанционно управляемых машин инженерного и тылового обеспечения.

Все эти устройства предполагалось объединить единой системой боевого управления, контроля, связи, разведки и наблюдения, в результате отдельные элементы смогли бы обмениваться информацией в реальном масштабе времени [89].

Однако роботизация вооруженных сил имеет ряд серьезных ограничений, с которыми вынуждены считаться даже самые богатые и развитые страны. Так, в 2009 г. США приостановили плановую реализацию программы FCS, начатую в 2003 г., по причине финансовых ограничений и технологических проблем. С мая 2003 г. по декабрь 2006 г. стоимость программы закупок для FCS выросла с 91,4 до 160,9 млрд долл. За тот же срок удалось реализовать лишь 2 технологии из 44 запланированных. Общая стоимость программы в 2006 г.

оценивалась в 203,3-233,9 млрд долл., затем она возросла до 340 млрд долл., из которых 125 млрд долл. планировалось потратить на НИОКР. В конечном итоге после израсходования более 18 млрд долл. программа FCS была остановлена, хотя по планам к 2015 г. треть боевой мощи армии США должны были составлять роботизированные системы [105, 106].

Кроме финансовых сложностей роботизации, неясным остается эффективность робототехнических или совместных человеко-робототехнических подразделений в бою с противником, располагающим большим арсеналом средств РЭБ и информационного оружия [29, 35].

Тем не менее процесс роботизации вооруженных сил США продолжается. Несмотря на то, что программа FCS была закрыта, разработка инновационных средств вооруженной борьбы, включая системы управления и связи, а также большую часть роботизированных и беспилотных средств, была сохранена в рамках новой программы модернизации боевых бригадных групп (Brigade Combat Team Modernization) [90].

В конце 2010 г. министерство обороны США обнародовало План развития и интеграции автономных систем на 2011-2035 гг. Согласно этому документу, количество воздушных, наземных и подводных автономных систем будет увеличено, причем перед разработчиками ставятся задачи сначала наделить эти аппараты «поднадзорной самостоятельностью» (то есть их действия контролирует человек), а в конечном итоге – и «полной самостоятельностью». При этом специалисты ВВС США полагают, что перспективный искусственный интеллект в ходе боя будет способен самостоятельно принимать решения, не нарушающие законодательство [105, 106].

К 2016 г. уже разработано около 20 дистанционно управляемых наземных машин для ВС США. При этом ВВС и ВМС работают над примерно таким же количеством воздушных, надводных и подводных систем [105, 106].

Обсуждается идея совместного комплектования пехотных и специальных подразделений людьми и роботами. Другая идея – комплексировать отработанные и новые технологии. Например, использовать транспортные самолеты и корабли в качестве «платформ-маток» для групп воздушных и морских беспилотных аппаратов, что изменит тактику их использования и увеличит их возможности [105, 106].

Таким образом, опыт роботизации вооруженных сил на примере США показал, что разработка военных робототехнических ком-

плексов – сложнейшая научно-техническая задача, требующая системного подхода и объемного финансирования. Так и не сумев создать систему FCS, американцы отдали предпочтение смешанным системам «человек+робот» либо «робот, управляемый человеком». Роботам отводятся задачи, которые они решают эффективнее человека, либо те, где риск жизни человека превышает допустимые ограничения. Преследуется также цель удешевления вооружения и военной техники.

При вторжении в Ирак в 2003 г. США имели всего несколько десятков БПЛА и ни одного наземного робота, в 2009 г. – 5300 БПЛА, а в 2013 г. – более 7000. Массированное применение повстанцами в Ираке самодельных взрывных устройств стало причиной резкого ускорения развития американцами наземных роботов. В 2009 г. вооруженные силы США уже имели более 12 тыс. роботизированных наземных устройств [109].

Опыт США показывает, что при разработке роботов военного и гражданского назначения используются общие подсистемы и элементы, основанные на передовых достижениях в области сенсорных устройств, машинного зрения, распознавания речевых команд, механических манипуляторов, математического обеспечения и т. д. Это позволяет на одной и той же научно-технической и промышленной базе создавать и автоматизированные средства вооруженной борьбы, и автоматизированные производственные системы, рассчитанные на массовый спрос или коммерческие товары. При такой схеме с одной стороны, обеспечивается внедрение результатов новых военных разработок в области робототехники в гражданские области, а с другой – выпуск военной продукции не требует наличия специальной военной промышленности. Анализ робототехнических комплексов, представляемых на международных салонах и выставках оборонных систем и вооружений, наглядно демонстрируют слияние гражданского и военного секторов в этой области [89].

Интересны следующие факты. Мировым лидером в гражданской робототехнике является Япония. По общему количеству промышленных роботов (около 350 тыс. шт.) Япония значительно опережает идущих за ней Германию и США. Она также лидер по количеству промышленных роботов на 10 тыс. человек, занятых в автомобильной промышленности, на которую приходится более 40% от всего объема продаж роботов в мире. В 2012 г. этот показатель у лидеров составлял: Япония – 1562 единиц; Франция – 1137; Германия – 1133; США – 1091. Китай имел 213 роботов на 10 тыс. работающих в авто-

проме. Однако по количеству промышленных роботов на 10 тыс. человек, занятых во всех отраслях промышленности, лидировала Южная Корея– 396 единиц; далее Япония – 332 и Германия – 273. Средняя мировая плотность промышленных роботов к концу 2012 г. составляла 58 единиц. При этом в Европе этот показатель составил 80, в Америке – 68, в Азии – 47 единиц. У России было 2 промышленных робота на 10 тыс. работающих. В 2012 г. в США было продано 22411 промышленных роботов, в России – 307 единиц [326].

По сообщениям иностранных СМИ, около 40 стран, в том числе США, Россия, Великобритания, Франция, Китай, Израиль, Южная Корея, разрабатывают роботов, способных воевать без человеческого участия. Ряд программ реализуется на базе совместных проектов. Считается, что рынок подобных вооружений может достигать 20 млрд долл. США. С 2005 г. по 2012 г. Израиль продал БПЛА на сумму в 4,6 млрд долл. США. Всего разработками военных роботов занимаются специалисты более чем 80 стран [109].

Основной тенденцией реализации этих проектов является дооснащение состоящих на вооружении средств системами технического зрения, средствами автоматизации управления, каналами связи (радио и оптоволоконными) и средствами управления движением, построенными на модульном принципе. Такой подход позволяет осуществлять быстрое внедрение робототехнических систем в специализированные подразделения.

Ниже более подробно представлены технологии и тенденции развития робототехнических комплексов военного назначения на основе анализа открытых источников в области развития: БПЛА [13, 89, 90, 92, 95, 97, 109, 116, 114, 115, 116, 117, 118, 144-147, 150, 156, 158, 300], наземных робототехнических средств [29, 95, 89, 90, 91 105, 106, 110,191], а также автономных необитаемых надводных и подводных аппаратов [44, 89, 90, 164, 166, 191, 197].

4.5.2. Робототехнические комплексы на основе БПЛА

4.5.2.1. Общая характеристика тенденций развития БПЛА

Сегодня в мире наблюдается устойчивый интерес к развитию и совершенствованию беспилотной техники. В развитых странах беспилотная техника уже несколько десятков лет используется для выпол-

нения боевых задач. В настоящее время в интересах вооруженных сил комплексы с БПЛА предполагается использовать для решения разнохарактерных задач в условиях, когда применение пилотируемой авиации невозможно или нецелесообразно (сильное противодействие средств ПВО противника, радиационное, химическое или бактериологическое заражение воздуха и местности в районе боевых действий, осуществление длительного наблюдения за противником и т.д.).

При этом современные комплексы с БПЛА должны решать [13]:

1. разведывательные задачи:
- ведение воздушной разведки;
- корректировка огня артиллерии;
- целеуказание высокоточному оружию (подсветка целей);
- оценка результатов нанесения ударов;
- длительное воздушное патрулирование заданных районов;
- определение местоположения и масштабов загрязнения (радиационного, химического, бактериологического и др.) территорий (акваторий);

2. ударные задачи:
- поражение наземных, надводных и воздушных объектов;

3. специальные задачи:
- радиоэлектронное противодействие огневым и обеспечивающим средствам противника;
- усложнение воздушной обстановки путем использования БПЛА в качестве авиационных ложных целей;
- ретрансляция информации и команд боевого управления.

К основным недостаткам существующих комплексов с БПЛА относятся [13]:
- меньшая гибкость применения, по сравнению с пилотируемой авиацией;
- нерешенность ряда проблем связи, передачи данных, вопросов посадки и спасения;
- более низкий, по сравнению с самолетами пилотируемой авиации, уровень надежности;
- большие расходы на создание целевых нагрузок;
- ограничения на полеты в населенных районах в мирное время.

Анализ опыта применения БПЛА в современных военных конфликтах позволяет сделать вывод, что наличие полной оперативной и достоверной информации о противнике является необходимым усло-

вием успешного ведения боевых действий. Таким образом, приоритетным направлением развития БПЛА является создание разведывательных и разведывательно-ударных комплексов на их основе [13].

Разрабатываемые и планируемые к созданию комплексы с БПЛА различных классов и назначений должны образовывать единую систему беспилотных средств, характеризующуюся высокой степенью унификации на уровне общих принципов построения. Должна быть предусмотрена унификация процессов производства комплексов, их эксплуатации и обслуживания в войсках, а также обучения личного состава. Эта система должна быть открытой и предусматривать поэтапную разработку и внедрение комплексов и их вариантов в войска, а также длительный жизненный цикл при возможности совершенствования в ходе модернизации с наращиванием ТТХ и расширением функциональных возможностей [13].

Сегодня 30 государств разрабатывают и производят до 150 типов БПЛА, из них 80 приняты на вооружение 55 армий мира. Лидируют в данной области США, Израиль и Китай. Следует заметить, что БПЛА не относятся к классическим роботам, так как не воспроизводят человеческую деятельность, хотя и считаются роботизированными системами. По прогнозам, ло 2025 г. доля американцев в мировых расходах на БПЛА составит: по НИОКР – 62%, по закупкам – 55% [109].

4.5.2.2. Применение комплексов различного назначения на основе БПЛА (на примере средств ВС США)

К числу перспективных летательных аппаратов относятся специализированные ударные и многоцелевые боевые беспилотные летательные аппараты, тактико-технические характеристики и боевая эффективность которых приближаются к современным образцам тактической авиации. Так, большое внимание уделяется созданию БПЛА, предназначенных для доставки средств ВТО к рубежам выполнения задач нанесения ударов по расположенным на большом удалении наземным целям [95, 300].

Для решения таких задач в ВВС США применяются многоцелевой БПЛА MQ-1 Predator, оснащенный противотанковыми управляемыми ракетами AGM-114 Hellfire, и его усовершенствованный вариант MQ-9 Reaper, успешно применявшиеся в Ираке и Афганистане.

Одно из ведущих мест в арсенале американских ВВС среди БПЛА до последнего времени занимал летательный аппарат Predator.

Он сравнительно дешевле (3,4 млн долларов), имеет высокий уровень надежности работы бортового оборудования, но относительно небольшую скорость полета. Именно этот БПЛА был применен США для обнаружения и нанесения ударов по Аль-Каиде в Йемене и Афганистане [300].

Однако сейчас на вооружение принимается новый вид БПЛА, способный проводить штурмовые операции. В июле 2007 г. США приступили к развертыванию в Афганистане и Ираке первых ударных эскадрилий новейших БПЛА Reaper для ведения боевых действий против Аль-Каиды и талибов [89].

БПЛА MQ-9 Reaper (Рипер) несет на борту до 1,5 т вооружений. Это 4 ракеты AGM-114 Hellfire и две бомбы Mark 82 по 250 кг. По сообщениям зарубежной печати, этот БПЛА обладает следующими характеристиками: максимальная взлетная масса – около 5 т, максимальная скорость полета – 480 км/ч, дальность полета – около 5800 км, практический потолок – до 15 км, время выполнения задач в воздухе – около суток (с полной нагрузкой – около 14 ч). Бортовая аппаратура Reaper позволяет на малых скоростях полета (до 70 узлов, около 130 км/ч) сканировать поверхность с разрешением 1 м, просматривая 25 кв.км поверхности в минуту, а на больших скоростях (около 250 узлов, более 460 км/ч) – до 60 кв.км. В режиме поиска бортовая РЛС обеспечивает получение с расстояния 40 км мгновенных снимков локальных участков земной поверхности размером 300×170 м с разрешением до 10 см [89, 95].

Стоимость образца БПЛА Reaper составляет приблизительно 30 млн долларов США в зависимости от конфигурации.

Таким образом, Reaper – это уже не аппарат воздушной разведки с опциями для нанесения ударов, а серьезный БПЛА-штурмовик с богатыми возможностями авиаразведки. Он может парить над заданной территорией до 14 ч, находясь в полном боевом вооружении и ожидая, когда на земле появится нужная цель. Управление производится на расстоянии почти 10 тыс. км из специального компьютерного центра, находящегося в американском штате Невада. Оператор, использующий систему виртуального присутствия, имеет возможность через спутник связи руководить полетом БПЛА и наносить удары [89].

До 2015 г. БПЛА Reaper прошел две модификации:

- Block-1 – в апреле 2012 г. была представлена модификация БПЛА с увеличенной продолжительностью полета. Модернизированный БПЛА находится в воздухе на 10-15 ч дольше, чем предыдущая версия. Этот результат был достигнут

благодаря дополнительным топливным бакам и обновленным шасси, благодаря чему продолжительность полета увеличилась до 37 ч без дозаправки. По сообщениям компании-производителя, если на БПЛА MQ-9 Reaper установить более длинные крылья – 26,8 м (вместо штатных 20 м), то БПЛА сможет находиться в воздухе до 42 ч;

- Block-5 – увеличена мощность двигателя, установлена вторая радиостанция для передачи данных нескольким воздушным или наземным объектам, увеличена грузоподъемность.

Анализ боевого применения БПЛА Reaper показал, что значительная высота ведения разведки и высокая дальность обнаружения целей, а также сниженные демаскирующие признаки БПЛА в акустическом и оптическом диапазонах позволяют ему скрытно вести разведку в заданном районе для выявления активности противника. Наблюдение за потенциальным объектом атаки с задействованием одного аппарата может при необходимости продолжаться более 12 ч. Для выполнения аналогичной (по боевой производительности) задачи по вскрытию обстановки в районе такой же площади силами тактической авиации требуется не менее 6 самолето-вылетов [146].

БПЛА RQ-4 Global Hawk – высотный стратегический разведывательный БПЛА. Первый аппарат Global Hawk был передан ВМС США в 2004 г. и приступил к выполнению боевых задач в марте 2006 г. Global Hawk выполнен по классической аэродинамической схеме. Крыло полностью изготовлено из композиционного материала на основе углеволокна. V-образное хвостовое оперение также сделано из композиционных материалов. Фюзеляж изготавливается из алюминиевых сплавов. Размах крыльев составляет примерно 35 м, длина – 13,3 м, а взлетная масса приближается к 15 т. БПЛА может осуществлять патрулирование в течение 30 ч на высоте до 18 км [89].

Global Hawk оснащен интегрированной системой наблюдения и разведки HISAR (Hughes Integrated Surveillance & Reconnaissance). Это упрощенная и более дешевая версия комплекса ASARS-2, разработанного фирмой Hughes для разведывательного самолета Lockheed U-2. Комплекс HISAR включает в себя радиолокационную, оптическую и инфракрасную разведывательные подсистемы. Все эти подсистемы могут работать одновременно, а их данные обрабатываются единым вычислительным комплексом БПЛА. Радиолокатор с синтезированной апертурой изготовлен фирмой Raytheon (Hughes) и предназначен для работы в любых погодных условиях. В нормальном режиме

работы он обеспечивает получение радиолокационного изображения местности с разрешением в 1 м. За сутки может быть получено изображение с площади 138 кв. км на расстоянии 200 км. В точечном режиме проводится съемка области размером 2×2 км, за 24 ч может быть получено более 1900 изображений с разрешением 0,3 м. Global Hawk имеет широкополосный спутниковый канал связи и канал связи в пределах зоны прямой видимости. Подсистема радиолокационной разведки работает в X-диапазоне и обеспечивает:

- сканирование и обнаружение движущихся целей в радиусе 100 км;
- комбинированный SAR/MTI – режим, который предоставляет возможность наблюдения с разрешением 6 м за полосой шириной 37 км и длиной от 20 до 110 км;
- в режиме детальной съемки обеспечивает наблюдение с разрешением 1,8 м на территории до 10 кв. км.

РЛС обладает возможностью обнаружения наземных подвижных объектов и передачи сведений о подобных объектах (координаты и скорость) в текстовых сообщениях. Дневная электронно-оптическая цифровая камера изготовлена компанией Hughes и обеспечивает получение изображений с высоким разрешением. Оптический датчик (1024×1024 пикселей) сопряжен с телеобъективом с фокусным расстоянием 1750 мм. В зависимости от программы есть два режима работы. Первый – сканирование полосы шириной 10 км, а второй – детальное изображение области 2×2 км. Изображения, получаемые с РЛС, оптического и ИК-сенсора, обрабатываются на борту БПЛА и передаются на наземную станцию в виде отдельных кадров. Обработанные данные могут передаваться на землю в режиме реального времени со скоростью до 50 Мбит/с через УКВ-канал прямой видимости или через спутниковый канал Ku-диапазона. Наземная станция собирает из кадров изображения и подготавливает их для дальнейшего использования. Для навигации Global Hawk используется инерциальная система с поправками от GPS.

Стоимость комплекса на основе БПЛА оценивается в 140 млн долл. США. Расходы на час полета БПЛА оцениваются в 31 тыс. долл.

До 2015 г. время БПЛА Global Hawk прошел несколько модификаций:

- RQ-4B Global Hawk Block 30 – модификация, официально принятая на вооружение ВВС США с августа 2011 г.

- RQ-4B Global Hawk Block 40 – отличается от предыдущей модификации Block 30 наличием мультиплатформенной РЛС MP-RTIP.
- RQ-4E Euro Hawk – немецкая модификация RQ-4, представленная в октябре 2009 г. На европейской версии БПЛА установлено оборудование радиотехнической разведки SIGINT, разработанное EADS.
- MQ-4C Triton – морской патрульный БПЛА, оснащен РЛС X-диапазона для обнаружения различных надводных кораблей вошел в систему расширенной морской разведки ВМС США – BAMS. Управляют этими БПЛА экипажи патрульных самолетов P-8 Poseidon. По состоянию на июнь 2012 г., Northrop Grumman построила 2 испытательных образца MQ-4C Triton. На вооружение MQ-4C Triton планируется принять в декабре 2016 г.

Данный аппарат широко и успешно используется в военных конфликтах. Например, в ходе активной фазы военных действий в Ираке в течение марта 2003 г. один аппарат RQ-4A Global Hawk совершил 16 боевых вылетов с общим налетом около 360 ч. Это составило всего 3% от общего количества разведывательных полетов авиационной группировки. При этом аппарат передал более 55% всей информации о критичных по времени целях противника. Отмечается также, что к концу 2007 г. только 3 такими БПЛА, задействованными в Афганистане и Ираке, было выполнено около 400 вылетов с суммарным налетом около 8 тыс. ч. Напряженность боевого применения машин составила 8-12 вылетов в месяц продолжительностью более 24 ч каждый [146].

БПЛА-бомбардировщик UCAV на основе Steth-технологий активно разрабатывается в США. Уже создан прототип UCAV – экспериментальный многоцелевой БПЛА X-45. Первый полет продолжительностью 14 мин этот БПЛА выполнил в 2002 г., в ходе полета были достигнуты высота 2,5 км и скорость 360 км/ч. Пентагон планирует использовать системы, созданные на базе X-45, для решения двух задач:

- подавление системы противовоздушной обороны в момент начала активных боевых действий;
- нанесение ударов по целям, прикрытым сильной ПВО.

В обоих случаях планировалось использовать эти БПЛА для немедленных действий на удаленных ТВД (заданное время развертыва-

вания системы на любом аэродроме планеты – 32 ч, готовность к взлету после переброски – 75 мин).

Программа X-45 получила 767 млн долл. от DARPA в октябре 2004 г. на строительство и испытания трех БПЛА. Предполагалось, что X-45 понесет 680 кг ракетобомбовой нагрузки, а также то, что он сможет автоматически выбирать важные цели, определять трассу полета к ним и сам возвращаться на базу. Скорость БПЛА – 0,8 М. Эти БПЛА должны были быть встроены в единую сеть разведки и управления боевыми действиями и стать основой для проведения сетецентрических беспилотных операций.

Однако по состоянию на 2 марта 2006 г. ВВС США приняли решение прекратить финансирование проекта X-45. Несмотря на прекращение финансирования, Boeing продолжил программу X-45 в инициативном порядке, в рамках которого планирует создать и предложить ВМС США демонстрационный вариант X-45N.

Интерес в плане перспективного использования БПЛА вызывает проект БПЛА RAQ-25 CBARS (Carrier-Based Aerial-Refueling System – «Палубная система дозаправки»). Целью нового проекта CBARS является создание БПЛА, предназначенного для осуществления дозаправки в полете других летательных аппаратов. Разработка такой техники позволит ВМС США избавиться от давней проблемы, связанной с увеличением боевого радиуса имеющихся самолетов. Дело в том, что с конца девяностых годов палубная авиация не имеет полноценного самолета-заправщика, что мешает ей с большей эффективностью выполнять поставленные задачи. В 1997 г. с вооружения был снят специализированный заправщик Grumman KA-6D Intruder, и с тех пор дозаправка выполняется только истребителями F/A-18 с подвесными заправочными агрегатами. Предполагается, что перспективный БПЛА-танкер RAQ-25 сможет полноценно решать поставленные задачи и тем самым высвободить истребители F/A-18, позволив им заниматься только боевой работой. При этом можно ожидать, что использование беспилотных заправщиков приведет к некоторому повышению эффективности подобной работы. БПЛА с характеристиками на уровне X-47 или выше смогут в течение длительного времени находиться в указанном районе за пределами зоны действия ПВО противника и производить там дозаправку боевых самолетов, отвечающих за завоевание господства в воздухе или нанесение ударов по объектам противника [116].

С 1996 г. ВВС США ведут большую программу создания самых разнообразных ударных и разведывательных комплексов, беспи-

лотных систем ретрансляции и связи, а также ложных целей на основе БПЛА. Дешевые мини-БПЛА, объединившись в сети, превратятся в массовое оружие на новых принципах «роевого» интеллекта.

К таким мини-БПЛА можно отнести Wasp. Свой первый полет он совершил в 2007 г. Аппарат предназначен для наблюдения, целеуказания, корректировки огня и оценки ущерба при нахождении над вражеской территорией. Wasp оснащен двумя миниатюрными видеокамерами, которые собирают информацию и передают ее оператору в режиме реального времени. Масса Wasp 200 г, размах крыла – 33 см, оснащен электромотором, получающим энергию от аккумуляторов и подзаряжающимся во время полета от солнечных батарей. Модификация Wasp III имеет размах крыльев 73,5 см, массы 454 г и несет электрооптические цветные камеры, направленные вперед и в стороны, плюс дополнительную модульную нагрузку оптических или инфракрасных сенсоров. Имеет дальность действия до 5 км от оператора и максимальное время нахождения в воздухе до 45 мин [89].

От США стараются не отставать и другие страны. В настоящее время уже более 80 типов БПЛА состоят на вооружении 41 страны. 32 государства сами производят и предлагают к продаже более 250 моделей БПЛА различных типов. По мнению американских специалистов, производство БПЛА на экспорт не только позволяет поддерживать собственный военно-промышленный комплекс, снижать стоимость БПЛА, закупаемых для своих вооруженных сил, но и обеспечивать совместимость аппаратуры и оборудования в интересах проведения многонациональных операций [90].

Одним из лидеров в создании и применении БПЛА считается Израиль. В Израиле БПЛА производятся сразу несколькими оборонными предприятиями такими как концерн Rafael и концерн ТАА. Ливанская война 2006 г. стала первой в истории по масштабам применения БПЛА. Так, израильские боевые БПЛА Hermes совершили более 2500 боевых вылетов. Они использовались для разведки, а также поиска и уничтожения живой силы противника.

В настоящее время прорабатывается применение БПЛА не только для решения боевых задач. Используя БПЛА, можно доставлять за линию фронта оружие и амуницию, а также эвакуировать раненых. Так, в настоящее время отдел логистики и снабжения ЦАХАЛа вместе с ВВС и командованием сухопутных войск Израиля проверяют ряд разработок, предложенных израильскими компаниями для этих целей. Израильская компания ТАА уже начала проводить эксперименты по превращению обычного грузового вертолета в беспилотный.

Компания Urban Aeronautics разрабатывает новый беспилотный вертолет Mule, работающий не при помощи внешнего винтового ротора, а при помощи внутренних роторов на основе турбореактивного двигателя. Этот небольшой вертолет (длиной всего 5 м) будет способен перевозить груз массой 230 кг – еду, воду, медикаменты, боеприпасы и т.д. Параллельно съезде специалистов оборонных предприятий Израиля было принято решение сделать максимальное усилие для создания беспилотного медицинского вертолета для эвакуации раненых с поля боя. Согласно заданным параметрам, вертолет будет длиной около 8 м и высотой около 1,5 м. Он будет способен перевезти 4 человек и медицинское оборудование, предназначенное для оказания экстренной помощи, и передвигаться со скоростью 150 км/ч на высоте 3 км [89].

Эксперты считают, что боевые БПЛА во многом превзойдут обычные боевые самолеты. Дело не только в их дешевизне по сравнению с пилотируемыми истребителями или бомбардировщиками. БПЛА по маневренности превзойдут обычные самолеты хотя бы потому, что являются более маневренными, так как могут позволить себе самые высокие перегрузки, недоступные для человека. Кроме того, на БПЛА можно возложить ряд дополнительных задач обеспечения боевых действий и тылового обеспечения.

4.5.2.3. Проблемные аспекты применения БПЛА

Несмотря на то, что доля использования БПЛА в вооруженных конфликтах и локальных войнах постоянно увеличивается, для их массового применения есть существенные ограничивающие факторы и различного рода проблемные аспекты. Как показал анализ работ [89, 92, 97, 114, 115, 116, 117, 147, 150, 156, 158], к числу основных из них относятся:

- низкая автономность существующих комплексов на основе БПЛА;
- недостаточная пропускная способность подсистемы связи для одновременного дистанционного управления множеством БПЛА или получения от них больших объемов разведывательной информации;
- необходимость создания принципиальной новой наземной обслуживающей и эксплуатационной инфраструктуры;
- необходимость специальной подготовки операторов БПЛА;
- сложности, связанные с эффективным применением БПЛА против объектов, прикрываемых системами ПВО и РЭП;

- необходимость разработки новых правил и технических средств обеспечения безопасности полетов с учетом БПЛА как равноправного участника воздушного движения.

Одним из основных ограничений на применение БПЛА является его низкая автономность и необходимость постоянного взаимодействия с оператором на Земле. Таким образом, несмотря на десятки разрабатываемых систем автоматического управления, БПЛА продолжают быть «ручными». Они нуждаются в человеческом контроле, иначе применять их будет попросту невозможно. Даже управление такими высокотехнологичными БПЛА, как Reaper или Global Hawk, все равно ведется вручную во всех сложных режимах, включая взлет, посадку, барражирование над целью и применение оружия [147].

Анализ [97] показал, что успешному применению БПЛА препятствуют недостаточное количество каналов связи (ширина полосы частот) на всех потенциальных ТВД и ограничения пространственного (географического) характера на некоторых из них. Отмечается, что системы связи при дистанционном управлении БПЛА настолько перегружены, что некоторые планировавшиеся действия приходилосьоткладывать или отменять. Таким образом, оказалось, что недостаточные возможности систем связи ограничивают количество одновременно применяемых БПЛА. Соответственно начало каждой новой операции требует окончания предыдущей. В конечном итоге опыт применения БПЛА RQ-4 Global Hawk и MQ-1 Predator в операции в Афганистане показал продолжающейся рост потребности в используемой полосе частот, которая, как показывает практика, удваивается ежегодно.

Еще одним ограничением на использование БПЛА является то, что эффективно они могут применяться в относительно свободном воздушном пространстве, днем, при минимальном противодействии средств ПВО и РЭП противника. Ночное применение БПЛА не получило широкого распространения по следующим причинам [115]:

- сложность ночного пилотирования;
- высокая стоимость оборудования – тепловизора или чувствительной ИК-камеры;
- сложность дешифрирования полученной информации, так как при ночной съемке трудно распознавать гражданские или военные цели.

При этом большие БПЛА, применяемые днем, нередко становятся легкими целями для средств ПВО, в том числе и ПЗРК. Так, при проведении 78-дневной операции союзных сил в Югославии в 1999 г. было потеряно около 47 БПЛА, из которых 35 были сбиты сербской

ПВО. Три грузинских БПЛА (включая, по меньшей мере, один Elbit Hermes 450) были сбиты над Абхазией российскими истребителями в российско-грузинском конфликте 2008 г. [117].

Как отмечается в работе [115], основным способом борьбы ВС технологически развитого государства с БПЛА становится применение средств РЭП, так как расход дорогостоящих ракет ЗРК против малых БПЛА ведет к быстрому исчерпанию ресурсов системы ПВО и фактически является неэффективным. Средства РЭП представляют серьезную угрозу для малых БПЛА, которые, как правило, не имеют полноценной альтернативной инерциальной системы навигации, используют каналы управления и передачи информации с низкой помехозащищенностью, а их алгоритмы управления не предусматривают высокой степени автономности. Опыт воздействия РЭП на БПЛА в локальных конфликтах [115] показывает, что средства РЭП работают следующим образом: средства радиомониторинга сканируют радиодиапазон в поисках источника радиосигнала БПЛА, после чего проводится анализ сигнала и принимается решение о постановке помехи:

- в канале видеотракта;
- в канале радиокомандной линии управления;
- для блокирования навигационных сигналов;
- в виде информационного воздействия на БПЛА с целью перехвата управления аппаратом.

Так как противодействовать помехам в каналах видеотракта или каналах радиоуправления в большинстве случаев невозможно, то БПЛА должен быть запрограммирован таким образом, чтобы при выявлении помех и прерывании управления с земли или попытке вмешаться в управление он переходил бы в полностью автономный полет в режиме радиомолчания и продолжал его до выхода из зоны действия РЭП. При этом БПЛА, который летит в автономном режиме (в режиме радиомолчания) и имеет слишком малую эффективную отражающую поверхность для РЛС, может быть обнаружен только визуально, поэтому становится практически неуязвимым для РЭП. В случае постановки помех в каналах GPS (подмена координат) аппарат должен переходить на управление с помощью инерциальной системы или по магнитному компасу [115].

Еще одним проблемным фактором, сдерживающим широкое внедрение БПЛА, являются экономические затраты. Так, даже относительно низкотехнологичные БПЛА стоят немало, требуют принципиально новых подходов к эксплуатации и обслуживанию, но при этом обеспечивают незначительный уровень эксплуатационной гибкости по

сравнению с пилотируемыми воздушными аппаратами. Как указанно в [117], «необитаемые» БПЛА в реальности требуют значительных людских ресурсов. Например, по имеющимся данным, ВВС США планируют выделять по десять пилотов на каждый БПЛА во время обычных операций. К этому необходимо добавить операторов различного оборудования, обслуживающих техников, аналитиков разведывательных данных, и получится, что каждый «беспилотный» летный час требует сотен человеко-часов. Кроме этого, применение БПЛА требует развертывания соответствующих учебно-тренировочных комплексов и элементов наземной и радиотехнической инфраструктуры. При этом все эти ресурсы необходимо обеспечить, даже если используется только один БПЛА [117, 151].

Применение военных БПЛА показало необходимость принятия мер, гарантирующих, что они не будут сталкиваться с другими летающими объектами, использующими воздушное пространство. До настоящего времени это реализовывалось за счет использования пилотируемого самолета сопровождения или наземного наблюдателя, что ограничивало операции с использование БПЛА дневным временем. Однако ряд происшествий, связанных со столкновением пилотируемых и непилотируемых аппаратов, вынудил приступить к разработке соответствующих систем. Так, американская армия в настоящее время начала установку системы обнаружения и предотвращения столкновений в воздухе GBSAA (Ground-Based Sense-And-Avoid) производства компании SRC на своих ключевых авиабазах в континентальной части, начав с Fort Hood в декабре 2014 г. Система GBSAA получает данные по оптоволоконным кабелям или каналам коротковолновой связи от нескольких датчиков и рассчитывает риск столкновения БПЛА, сопоставленный с маршрутами других воздушных судов. Оператор GBSAA передает эту информацию оператору БПЛА для принятия соответствующих действий по исключению столкновения [117].

Для решения аналогичных задач компания General Atomics разработала РЛС воздушного трафика DRR (Due Regard Radar), которая устанавливается на БПЛА в качестве компонента системы предотвращения столкновений для беспилотной авиации ACAS-Xu (Airborne Collision-Avoidance System for Unmanned Aircraft). РЛС DRR тестировалась в составе системы SAA, предназначенной для предотвращения столкновений в воздухе, разработки компанией General Atomics, которая реализует функцию автоматического ухода от столкновений и функцию слияния данных сенсоров с целью предоставления оператору БПЛА картины воздушного трафика вокруг его аппарата. Указанная

компания работает с NASA с целью установки своей системы SAA на опытный БПЛА Predator-B, получивший обозначение Ikhana [117].

Кроме того, широкое внедрение БПЛА выявило ряд психологических аспектов применения дистанционно управляемых робототехнических устройств как со стороны операторов, так и среди противника, против которого применяются подобные аппараты.

Анализ опыта применения БПЛА в Ираке и Афганистане [147] показал, что зачастую операторы управляют БПЛА и применяют его оружие в условиях действия противоречивых разведывательных данных и без учета специфики конкретной ситуации. Отмечается отсутствие «вживления» оператора, находящегося за тысячи километров, в реальную боевую обстановку. Ввиду того, что информация о наземной цели, как правило, добывалась разведкой непосредственно в районе операции, оператор часто получал множество противоречивых сообщений и команд. Кроме того, большая длительность прохождения сигналов и команд на линии «оператор-БПЛА» накладывает на управляемость БПЛА определенную инертность. При этом за ту пару секунд, за которые сигнал доходит до БПЛА, ситуация в районе проведения операции может кардинально измениться. Вследствие этих факторов из 10 случаев применения ракетного вооружения БПЛА в Афганистане 5 попаданий приходилось на мирных жителей. Таким образом, каждый второй выстрел – это поражение мирного жителя. При этом, по данным фонда New America Foundation [150, 158], с 2004 по январь 2012 г. американские БПЛА, применяемые в боевых операций Аль-Каидой, Талибаном и другими террористическими группировками, нанесли 285 ракетных ударов, уничтожив от 1727 до 2690 человек, среди которых 385 – мирные жители. Все это ведет к низкой психологической устойчивости операторов БПЛА. Так, только за 2013 г. было отмечено 25 случаев, когда операторы БПЛА сводили счеты с жизнью без явных на то причин [147].

Для противника и мирного населения боевое применение БПЛА имеет эффект теракта за счет своей внезапности. Анализ использования БПЛА в Пакистане показал, что их применение наносит существенные психологические травмы мирному населению противоборствующей стороны. В докладе [156] указывается, что БПЛА летают над населенными пунктами на северо-востоке Пакистана круглосуточно и без предупреждения наносят удары по домам, транспортным средствам, общественным местам. Их присутствие вызывает у мужчин, женщин и детей постоянное чувство беспокойства и наносит психологические травмы. Нередко пакистанцы, которые становятся сви-

детелями авиаудара, боятся прийти на помощь пострадавшим, так как могут быть атакованными БПЛА, – пишут авторы доклада. Кроме того, родственники людей, погибших в результате операций БПЛА, часто боятся присутствовать на похоронах своих близких из-за угрозы нанесения удара по участникам похорон. Отмечается также, что, исходя из сообщений СМИ и отчетов американских спецслужб, судить о реальных результатах беспилотной войны нельзя. Так, американское правительство редко признает факт убийства мирных жителей и регулярно занижает число убитых среди гражданского населения. Созданию иллюзии борьбы с террористами способствует ряд уловок: в частности, в официальных отчетах все убитые мужчины, достигшие совершеннолетия, фигурируют как «боевики» независимо от того, являлись они ими или нет [158].

Таким образом, практика применения БПЛА является довольно неоднозначной, однако с учетом перспектив, которые открывает сам принцип «беспилотности» авиационных средств, можно ожидать, что развитие БПЛА и комплексов на их основе продолжится. При этом большинство современных проблемных аспектов применения БПЛА относится к «детским болезням» этого вида авиации, и они будут успешно разрешены по мере развития соответствующих технологий.

4.5.2.4. Перспективы развития комплексов на основе БПЛА

В настоящее время продолжаются процессы совершенствования комплексов на основе БПЛА. При этом, как показано в работе [144], бурное развитие беспилотной авиации в военных целях обусловлено, прежде всего, фактическим исчерпанием возможностей экстенсивного развития пилотируемой авиации. А реализация же интенсивного пути развития пилотируемой авиации за счет перехода к 5-му поколению авиационных комплексов требует очень существенных финансовых затрат. К числу основных тенденций в направлении создания новых и совершенствования существующих БПЛА можно отнести следующие [116, 117, 118]:

- создание гиперзвуковых БПЛА;
- использование при проектировании БПЛА технологий снижения радиолокационной и оптической заметности;
- увеличение автономности и длительности полета;
- повышение пропускной способности каналов связи;

- оснащение БПЛА интеллектуальными системами автономного управления, маневрирования в полете, целеопределения и применения оружия;
- оснащение БПЛА средствами активного противодействия системам ПВО, а также комплексами защиты борта на основе средств РЭБ и лазерного оружия;
- оснащение БПЛА системами определения и противодействия средствам РЭП или информационно-техническим воздействиям с целью нарушения или перехвата управления;
- проработка вопросов создания смешанных авиационных групп, состоящих из пилотируемых и непилотируемых аппаратов;
- разработка новых тактических приемов действия множества БПЛА на основе поведения «стаи» или «роя».

Далее более подробно представлены некоторые из основных тенденций развития БПЛА.

Анализ, проведенный в работе [97], показал, что успешному применению БПЛА препятствует недостаточная пропускная способность подсистемы связи. Для преодоления ограничений систем связи для БПЛА в настоящее время ведется ряд прорывных работ.

Во-первых – это технологии создания конформных антенн, которые размещаются на поверхности аппарата, что позволяет использовать всю поверхность БПЛА в качестве антенны [97].

Во-вторых – рациональное использование имеющегося радио ресурса. Так, в США в качестве платформы для информационного обмена с перспективными БПЛА предлагается единый тактический канал связи TCDL (Tactical Common Data Link), охватывающий каналы связи, которые могут быть установлены как на самолетах разведки, так и на БПЛА. TCDL предназначен для передачи радиолокационных данных, изображений, видео и другой информации, получаемой датчиками БПЛА, со скоростью от 10,7 Мбит/с, а в перспективе – до 274 Мбит/с на расстоянии до 200 км [97].

В-третьих – отказ от использования радиоспектра для передачи данных и переход на оптические каналы. Так, французское оборонное агентство предоставило компании EADS контракт на разработку оптического канала связи между перспективным БПЛА и КА на геостационарной орбите. Канал будет задействован для защищенной передачи информации между БПЛА и удаленным центром управления. Предполагается на начальном этапе обеспечить связь через КА со скоростью

порядка 50 Мбит/с, в последующем – порядка несколько сотен мегабит в секунду [97].

Специалисты управления воздушной разведки США, занимающиеся исследованием путей решения проблемы ограниченной пропускной способности систем связи, предусматривают использование [97]:

- общего воздушного радиоканала связи с большой шириной полосы частот для бортовых платформ на основе БПЛА;
- лазерных каналов связи со скоростью передачи данных до 1 Гбит/с, в том числе и в направлениях БПЛА-ПУ, БПЛА-БПЛА и БПЛА-КА;
- бортового индикатора движущейся цели, который мог бы применяться в качестве «индикаторного протокола» для других бортовых датчиков, благодаря чему сократится время непрерывного наблюдения и, как следствие, потребность в широкой полосе частот;
- инструментальных средств автоматизации, облегчающих планирование и распределение доступной ширины полосы частот для достижения лучшего возможного результата.

Зарубежные аналитики также указывают разработчикам БПЛА на тот факт, что использование частотного ресурса является критичным ограничением, поэтому они должны проектировать технику и разрабатывать тактические приемы с таким расчетом, чтобы минимизировать запросы этого ресурса и повысить автономность БПЛА. В настоящий момент БПЛА могут оснащаться полезной нагрузкой самого различного назначения, однако их использование ограничено недостаточной шириной полосы частот для передачи данных заинтересованным потребителям. При этом управление ресурсом связи для БПЛА сопоставимо по значимости с управлением летательным аппаратом или повышением его боевых возможностей [97].

Другим путем преодоления ограничения недостаточной пропускной способности систем связи БПЛА является повышение его автономности за счет использования новейших интеллектуальных технологий. Ведутся исследования [114, 115, 234] применения групп БПЛА и новых тактических приемов на основе «роевого» интеллекта. Открываются программы, направленные на повышение автономности отдельных БПЛА с одновременным улучшением их маневренности. Так, компанией BAE Systems (Великобритания) ведется разработка тяжелого ударного БПЛА Taranis. В октябре 2007 г. компания объявила о завершении работ по созданию для него полностью автономной

системы управления, которая позволит аппарату полностью автономно совершать все операции – как в воздухе, так и на земле. Скоростной ударный Taranis станет одним из крупнейших боевых БПЛА в мире. Предполагается, что он сможет наносить удары в стратегической глубине обороны противника, самостоятельно разведывать цели и уничтожать их после подтверждения оператором, будет способен самостоятельно защищаться от действий авиации противника – как пилотируемой, так и беспилотной.

Для повышения живучести, помимо увеличения автономности, возможно кардинально нарастить скоростные возможности БПЛА. Так, в настоящее время ведется разработка прототипов гиперзвуковых БПЛА. Косвенным показателем сложности проблем разработки в этой области служит тот факт, что несмотря на то, что Lockheed Martin обсуждала свой проект SR-72 Mach 6.0 с экспертами по двигателям из фирмы Aerojet Rocketdyne в течение нескольких лет, конечный продукт в виде разведывательного БПЛА для прорыва ПВО, по данным компании, будет готов не ранее 2030 г. Известно только, что коммерческие турбинные двигатели сначала смогут придать ускорение аппарату SR-72 примерно до 3 М (скорость, достигнутая предыдущим проектом SR-71 Blackbird), а последующее использование на БПЛА гиперзвуковых воздушно-реактивных двигателей увеличит затем эту скорость вдвое [117].

Для работы в пределах атмосферы гиперзвуковые БПЛА могут появиться как побочный продукт проекта по экспериментальному космическому самолету XS-1, над которым работают DARPA, а также компании Boeing и Northrop Grumman [117].

Относительно использования технологий снижения признаков заметности (технология Stealth) нужно отметить, что БПЛА RQ-170 Sentinel компании Lockheed Martin, проектировался с учетом двух аспектов: наличие достаточного уровеня живучести, чтобы летать над такими странами, как, например, Иран, но при этом его потеря не должна иметь больших последствий. Это делает его первым недорогим БПЛА, на котором используется технология снижения заметности. Предполагается, что он поступил на вооружение ВВС США в 2007 г. и был развернут на базах в Афганистане и Южной Корее, возможно, для мониторинга ядерных разработок в соседних странах. Кроме того, в настоящее время на вооружение ВВС США принят разведывательный БПЛА RQ-180 с управляемыми сигнатурами, который создан компанией Northrop Grumman (БПЛА представляет собой дозвуковое летающее крыло в стиле B-2). Предполагается, что контракт на разработку

RQ-180 был получен в 2008 г., первые поставки прошли в 2013 г., а аппарат мог быть поставлен на вооружение в 2015 г. [117].

Остро стоит вопрос с повышением живучести БПЛА при преодолении зоны ПВО. С целью защиты БПЛА от ракет с инфракрасным наведением систем ПВО и переносных зенитно-ракетных комплексов компания Elbit Systems разработала лазерную систему управляемого противодействия ИК-средствам mini-Music. Атакующая ракета вначале определяется системой предупреждения о ракетной атаке, затем захватывается тепловизионным автоматом сопровождения, что позволяет направить лазерный луч точно на атакующую ракету и тем нарушить функционирование ее системы наведения. Вполне возможно, что крупные БПЛА могут в будущем иметь некую систему оборонительных микроракет или перехватчиков, аналогичных комплексу активной обороны для вертолетов HAPS (Helicopter Active Protective System), разработанному компанией Orbital ATK для защиты от РПГ [117].

Важным направлением развития тактики применения БПЛА считаются совместные (групповые) действия пилотируемых аппаратов и беспилотных систем различных типов. По оценкам американских специалистов, обеспечение возможности получения экипажами пилотируемых аппаратов информации о целях или потенциальных угрозах от бортовых разведывательных систем БПЛА считается одним из перспективных путей снижения потерь армейской авиации. Кроме того, реализация такого взаимодействия позволит увеличить глубину ведения разведки и обеспечит своевременное принятие решения на атаку цели или выполнение маневров обхода зон поражения огневых средств ПВО противника. Операторы вооружения пилотируемых объектов, оснащенных унифицированной аппаратурой управления армейскими беспилотными аппаратами, смогут задавать маршрут полета БПЛА, режим работы разведывательных систем, а в перспективе – выдавать целеуказание и команды на применение их бортового вооружения [146].

В данном направлении в ВС США разрабатывается концепция комбинации пилотируемых и беспилотных средств Manned-Unmanned Teaming (Mum-T или просто Mut), в которой пилоты вертолетов (таких как Boeing AH-64 Apache и Bell OH-58D) могут контролировать БПЛА (такие как MQ-1C Gray Eagle General Atomics, MQ-5B Hunter Northrop Grumman, RQ-7B Shadow Textron Systems, RQ-11B Raven и Puma AE от AeroVironment), определять их маршруты, управлять их сенсорами и получать информацию от них. Это достигается за счет постепенно повышающихся уровней функциональности оборудования пилотиру-

емой авиации. Например, вертолет AH-64D Block II имеет оборудование, позволяющее принимать видео с БПЛА в полете и управлять его сенсорами. Вертолет AH-64E Guardian (бывший AH-64D Block III) получил уже более совершенное оборудование, позволяющее пилоту, кроме других функций, еще и контролировать траекторию полета БПЛА. По сути, концепция совместных действий пилотируемых и беспилотных летательных аппаратов Mut позволяет приближаться к вражеским целям без риска для контролирующего БПЛА вертолета, при этом обеспечивая экипаж вертолета высококачественной картинкой цели, которая будет атакована, получаемой в реальном времени. Планируется, что в долгосрочной перспективе за счет применения БПЛА вертолет AH-64E возьмет на себя задачи вооруженного разведывательного вертолета OH-58D [118].

Своего рода уникальной концепцией является программа Gremlin, разработанная DARPA министерства обороны США. Данной программой транспортным самолетам и бомбардировщикам отводится роль «воздушных авианосцев», запускающих с безопасного расстояния множество небольших универсальных БПЛА, которые будут выполнять боевые задачи в воздушном пространстве, а затем возвращаться на «самолет-матку». В конце 2014 г. DARPA обнародовало техническое задание на ОКР по разработке таких полноценных систем в течение 4 лет. В 2016 г. DARPA выделило на программу Gremlin первые 8 млн долл. [118].

Программа Team-US (Technology for Enriching and Augmenting Manned-Unmanned Systems – технология расширения и дополнения пилотируемых беспилотных систем) – это еще один радикальный подход DARPA к будущим сценариям воздушного боя. Программа Team-US предусматривает, что пилотируемые самолеты четвертого и пятого поколений смогут управлять «стаями» недорогих «ведомых БПЛА», которые будут вести наблюдение, проводить атаки с помощью средств РЭБ, а также осуществлять доставку боеприпасов к наиболее опасным целям, таким как средства ПВО. На программу Team-US управление DARPA запросило 12 млн долл. на 2016 г. [118].

Исследовательская лаборатория ВВС США также работает над концепцией «доступного функционального БПЛА, но которого не жаль потерять» (англ. термин «attritable»), запускаемого с воздушного судна. При этом стоимость БПЛА не должна превысить 3 млн долл. [118].

Одной из основ применения «стаи» БПЛА является программа DARPA под обозначением CODE (Collaborative Operation in Denied

Environments – Совместная работа в запретных пространствах). В соответствии с ней один человек сможет контролировать шесть и более БПЛА, оборудованных системой «общей автономности» для поиска и уничтожения целей [118].

Еще одна прорывная программа, разрабатываемая DARPA, получила обозначение Tern. В ней использованы решения, которые позволят БПЛА класса Male (medium-altitude, long-endurance – средневысотный, большой продолжительности полета) с разведывательными и ударными возможностями действовать (даже при сильном волнении моря) с американских боевых кораблей передового базирования, которые не имеют взлетной палубы, а имеют палубу таких же размеров, как у эсминца класса Arleigh Burke. При этом ВМС США заинтересованы в работе БПЛА Tern также с боевых кораблей прибрежной зоны, десантно-вертолетных транспортных доков, десантных кораблей-доков и грузовых кораблей командования военно-морских перевозок. В конечном виде БПЛА Tern будет способен вести патрулирование в зоне радиусом до 925 км в течение более чем 10 ч и доставлять полезный груз на расстояние до 1700 км. Предполагается, что БПЛА Tern будет использоваться для разведки, наблюдения и ударных задач в глубине суши без задействования передовых баз или помощи страны-оператора. Поскольку заметность здесь не упоминается, то, по-видимому, эта концепция предусматривает неожиданные атаки и действия в регионах со слабо развитыми системами ПВО и РЭП противника. Основные решения системы Tern относятся к системе запуска и возвращения БПЛА, но DARPA также заинтересовано в разработке компактной схемы размещения аппаратов, роботизации палубных манипуляций с БПЛА, автоматизации их обслуживания и предполетной проверки. Целью программы является демонстрационный полет прототипа БПЛА Tern в 2017 г. [118].

Обсуждение возглавляемых DARPA работ по перспективным БПЛА было бы неполным без упоминания о программе по созданию аппарата вертикального взлета и посадки X-Plane (стоимость 130 млн долларов, срок 52 месяца), хотя она нацелена на технологию, которая в равной мере может быть применена и к пилотируемому аппарату. DARPA планирует разработать демонстрационный образец, который сможет достичь скорости 550-750 км/ч, эффективности зависания более 60%, коэффициента аэродинамического качества в крейсерском полете как минимум 10 и полезной грузоподъемности, равной, по меньшей мере, 40% от его общей массы 4500-5500 кг. Соответствующие 22-месячные контракты на этап 1 программы X-Plane были выда-

ны в октябре 2013 г. компаниям Aurora Flight Sciences, Boeing, Karem Aircraft и Sikorsky Aircraft (объединилась с Lockheed Martin Skunk Works). Проект Phantom Swift компании Boeing имеет два подъемных винта, спрятанных в фюзеляже, и два поворотных винта на концах крыльев в направляющих насадках. Концепция Sikorsky Rotor Blown Wing представляет собой самолет с вертикальным взлетом и посадкой, садящийся на хвост. Проект компании Karem имеет поворотные несущие винты в середине крыльев, а внешние крылья поворачиваются вместе с несущими винтами. Эти четыре претендента должны были подать предварительные проекты в конце 2015 г., после чего DARPA планировало выбрать одного подрядчика на создание технологического демонстратора X-Plane, который должен осуществить первый полет в 2018 г. [118].

Проблемы ВС США, связанные с безопасностью в Афганистане и Ираке, привели к пониманию актуальности систем круглосуточной воздушной разведки с высоким разрешением. Это сделало актуальным разработку БПЛА с высокой продолжительностью полета в несколько дней.

В 2007 г. компания Aurora Flight Sciences была выбрана исследовательской лабораторией ВВС США для проведения исследования сверхдолгого полета и определения возможности для БПЛА с неподвижным крылом предложить альтернативу концепциям аппаратов легче воздуха (дирижаблям). В результате появился одномоторный БПЛА Orion массой 3175 кг, работающий на водороде и предназначенный для совершения крейсерских полетов на высоте 20 км длительностью более суток с грузом 180 кг. В результате дальнейшего развития проекта Orion был разработан БПЛА категории Male массой 5080 кг со сдвоенным дизельным двигателем Austro и размахом крыльев 40,2 м. БПЛА Orion в настоящее время способен совершать полеты с крейсерской скоростью в течение 120 ч с грузом 450 кг, но на высоте до 6 км, что, естественно, сокращает площадь обзора. В декабре 2014 г. прототип БПЛА Orion с балластным грузом 450 кг выполнил полет на высоте до 3000 м продолжительностью 80 ч. Полет был прекращен досрочно в связи с достижением запланированной дальности полета. По оценкам экспертов, БПЛА Orion способен барражировать в воздухе 114 ч (4,75 дня) в радиусе 800 км. При расширении радиуса барражирования до 4800 км продолжительность полета сокращается до 51 ч. Для увеличения продолжительности полета на высоте до 20 км БПЛА используют двигатели на водородном топливе. Этот БПЛА может быть сконфигурирован таким образом, что будет нести

под каждым крылом груз массой до 450 кг, что позволит получить определенные ударные возможности. Дальность перегоночного полета составляет 24 тыс. км. Скорость крейсерского полета составляет 125-160 км/ч, а максимальная скорость 220 км/ч. БПЛА Orion может стать экономически целесообразной заменой невооруженному БПЛА Predator [118].

Уменьшенный демонстрационный образец Phantom Eye от компании Boeing массой 4450 кг имеет размах крыльев 45,7 м и два 3-литровых двигателя Ford с турбонаддувом мощностью 112 кВт, которые работают на жидком водороде, закаченном в два сферических бака диаметром 2,44 м. Аппарат может оставаться в воздухе 4 дня на высоте до 20000 м с грузом массой 240 кг. Прототип Phantom Eye совершил свой первый полет в июне 2012 г. Следующий полет проходил на высоте 8500 м и длился 5 ч. Компания Boeing продолжает испытания, стремясь увеличить продолжительность полета и достигнуть высоты как минимум 20 км. В случае успеха эта программа может продолжиться в виде заказа на постройку полноразмерного аппарата Phantom Eye с размахом крыльев 64 м, который сможет оставаться в воздухе до 10 дней с грузом 450 кг. Заявлено, что четыре таких аппарата смогут обеспечить непрерывную зону радиосвязи на локальном ТВД [118].

В этом же классе, что и маломасштабный демонстрационный образец Phantom Eye, находится аппарат Global Observer GO-1 от AeroVironment, имеющий размах крыльев 40 м и один двигатель, работающий на водороде. Впрочем, в этом БПЛА двигатель питает электрогенератор, подающий энергию на 4 электродвигателя, которые, в свою очередь, вращают винты, установленные на кромке крыла. По задумке разработчика, GO-1 должен оставаться в воздухе до 5 дней на высоте до 20 км с полезным грузом 170 кг. Прототип GO-1 совершил первый полет в январе 2011 г., но 3 месяца спустя на 19-м часу своего девятого полета потерпел крушение. В декабре 2012 г. Пентагон прекратил финансирование проекта. Однако компания AeroVironment достроила второй прототип и в феврале 2014 г. вместе с Lockheed Martin вышла на международный рынок с БПЛА Global Observer, дав ему определение «атмосферная спутниковая система» [118].

БПЛА с неподвижным крылом и водородными поршневыми двигателями в конечном счете имеют хорошие перспективы достижения высокой продолжительности полета на больших высотах, но рекорды по продолжительность полета и установившейся высоте среди БПЛА удерживают аппараты на солнечных батареях [118].

Так, БПЛА Zephyr Seven, разработанный британской компанией Qinetiq, в июле 2010 г. установил официальный рекорд по продолжительности полета для пилотируемой/беспилотной авиации – 336 ч и 22 мин. Он также установил рекорд среди БПЛА по высоте полета – 21575 м. БПЛА Zephyr Seven имеет размах крыла 22,5 м, взлетную массу 53 кг, грузоподъемность 10 кг. Он способен лететь с крейсерской скоростью 55 км/ч и максимальной скоростью 100 км/ч [118].

В конце 2013 г. южнокорейская организация по оборонным закупкам DAPA (Defense Acquisition Program Administration) объявила о планах разработки к 2019 г. сверхлегкого БПЛА на солнечных батареях, который будет выполнять такие задачи, как, например, ретранслятор связи. БПЛА должен оставаться на боевом дежурстве в воздухе в течение 3 дней на высоте 10-50 км. Бюджет этой программы составит 42,5 млн долл. [118].

Тем временем американское DARPA проявило интерес к разработке БПЛА на солнечных батареях, который мог бы вести мониторинг военной и коммерческой активности к северу от Полярного круга в течение более 30 дней, отслеживая воздушные, наземные и подводные цели. Следует при этом отметить, что круглогодичная работа БПЛА на солнечных батареях, на таких высоких широтах очень затруднена.

4.5.2.5. Средства ПВО, основанные на новых принципах и ориентированные на применение против БПЛА

Активное развитие БПЛА актуализирует разработку принципиально новых систем ПВО, приоритетом которых будет являться борьба именно с массированным применением беспилотных средств. Существующие сейчас системы ПВО ориентированы на поражение пилотируемой авиации и средних/крупных БПЛА, но неэффективны для борьбы с малоразмерными БПЛА, которые могут применяться одновременно в больших количествах («стаями»). Радиолокационное обнаружение БПЛА эффективно, но сложно осуществимо на уровне небольшого подразделения в силу больших массогабаритных размеров РЛС, поэтому широко изучается возможность использования пассивных инфракрасных и других диапазонов волн. Касаемо механизмов поражения БПЛА следует отметить, что мини-ракеты, даже производясь серийно, имеют стоимость в десятки тысяч долларов за штуку, делающую их слишком дорогими для борьбы со «стаями» БПЛА [117].

В связи с вышеуказанными факторами, активно прорабатываются вопросы использования для поражения БПЛА оружия направленной энергии наземного и корабельного базирования. Использование лазеров или СВЧ волн предлагает овладение преимуществом низкой стоимости одного поражения, а также меньших косвенных потерь и ущерба по сравнению, например, с осколочными боеприпасами. Подвергшийся воздействию БПЛА не обязательно должен быть разрушен. Повреждения его антенны, подсистемы связи или управления, вывод из строя БЦВМ вполне возможно сделают его аэродинамически нестабильным, что негативно скажется на выполнении задачи. Лазерное оружие обеспечивает не только небольшую стоимость одного уничтожения, быстрый захват цели и способность справляться с маневрирующими целями, но также имеет фактически неограниченную емкость применения. С другой стороны, оно подвержено влиянию атмосферных явлений (особенно водяного пара и дыма) и может поражать только одну цель единовременно. Кроме того, это оружие может применяться только против целей, находящихся в зоне прямой видимости [117].

В настоящее время в США и в ряде других технологически развитых государств именно в этом направлении развиваются средства ПВО ориентированные на поражение именно мини- и микро-БПЛА.

Американская корпорация Boeing в 2009 г. объявила об успешном проведении опыта по применению боевого лазера против малогабаритного БПЛА. Лазер был установлен на платформе бронемашины Avenger (модифицированной HMMWV), которая обычно используется армией и морской пехотой США в качестве транспортной базы при выполнении задач ПВО. Laser Avenger способен применять против БПЛА свое вооружение, не раскрывая при этом позиции войск, т.е. можно уничтожать БПЛА противника, не подвергая при этом опасности другие подразделения, находящиеся вблизи бронемашины [300].

В 2012 г. компания Lockheed Martin официально представила прототип компактной наземной системы лазерной ПВО-ПРО ADAM (Area Defense Anti-Munitions) [135]. Система испытывалась в 2012 и 2013 гг. для борьбы с небольшими БПЛА и ракетами на расстоянии в 1,5-2 км и в 2014 г. у – против моторных лодок [136].

Корпорация Boeing в кооперации с британским подразделением европейского консорциума BAE System создали гибрид лазера и малокалиберной автоматической пушки Mk-38. Автоматом Mk-38 на

турели вооружаются десантные и вспомогательные суда ВМС США. Эффективный огонь может вестись на дальность 2,5 км. Исполнители в июле 2011 г. объявили о создании прототипа тактической лазерной системы TLS (Tactical Laser System) для поражения БПЛА и малых судов [316].

Годом раньше подобную систему ПВО-ПРО на авиакосмическом салоне Farnborogh-2010 в Великобритании показала американская компания Raytheon. Шесть волоконных лазеров LaWS (Laser Weapon System) общей мощностью 50 кВт были объединены с корабельной 20-мм шестиствольной автоматической артиллерийской установкой Mark 15 Phalanx CIWS (Close-In Weapon System –орудийная система ближнего боя). Подразумевается, что комбинированная установка сможет поражать цель 6 лазерами, чьи лучи сведены в одну точку. Если же это не удастся, то на более близком расстоянии в дело вступит шестиствольная пушка. На испытаниях в мае 2010 г. система обнаружила, захватила, взяла на сопровождение и поразила четыре БПЛА, летевших на разных высотах и дальностях. Представители Raytheon дали понять, что условия испытаний были близки к реальным боевым. При этом в британских СМИ появилось неподтвержденное сообщение, что один из БПЛА был поражен на дальности 3,2 км при скорости 480 км/ч [316].

В декабре 2013 г. в США прошли испытания боевого мобильного лазера HEL MD (High Energy Laser Mobile Demonstrator) мощностью 10 кВт, который во время испытаний уничтожил более 90 минометных снарядов и несколько БПЛА на дальностях до 5 км [117, 317].

В настоящее время в США ведутся программы SSL-QRC (Solid State Laser Quick Reaction Capability) и SSL-TM (Solid State Laser Technology Maturation), целью которых является создание экспериментальной модели лазера мощностью 100-150 кВт и в конечном счете установка высокоэнергетического лазера на такие корабли, как, например, эсминцы класса Arleigh Burke (DDG-51) и фрегаты LCS. ВМС США планируют выполнять программу по корабельной лазерной установке до 2019 г. с первоначальной готовностью в 2020-2021 гг. Ожидается, что эти более мощные лазеры будут эффективны против различных надводных и воздушных целей на дальностях до 15-20 км [117].

В 2014 г. научно-исследовательское управление ВМС выдало компании Raytheon контракт стоимостью 11 млн долл. на установку лазерной системы ближнего действия на бронеавтомобиль Hummer. Как ожидается, эта разработка приведет к созданию лазерного оружия

мощностью 30 кВт и компактной РЛС с фазированной антенной решеткой, которые будут устанавливаться на перспективный легкий тактический бронеавтомобиль JLTV (Joint Light Tactical Vehicle) в интересах защиты сухопутного подразделения от средств разведки противника на БПЛА [117].

Немецкая компания Rheinmetall в 2013 г. успешно продемонстрировала лазер мощностью 50 кВт, а также вариант мощностью 30 кВт с оптической системой слежения, установленный на зенитную установку Oerlikon Revolver Gun и соединенный с РЛС управления огнем Oerlikon Skyguard. На проведенных испытаниях лазер мощностью 30 кВт сбил на дистанции около 2 км 3 реактивных БПЛА, летевших со скоростью 20 м/с [117].

Более подробно сведения о разработках перспективных средств ПВО, основанных на лазерном оружии, представлены в разделе 4.9 «Оружие на новых физических и других принципах» – 4.9.1 «Лазерное оружие».

Таким образом, США и ряд других технологически развитых стран уже сейчас добились ощутимых результатов в области роботизации своих вооруженных сил. На вооружении уже сегодня состоят как тактические, так и стратегические комплексы БПЛА разведывательного и ударного назначения. Вместе с тем абсолютно неправильно сводить всю деятельность по оснащению вооруженных сил робототехническими комплексами исключительно к БПЛА. Как свидетельствует мировой опыт, это только первый и не самый сложный шаг [326].

4.5.3. Наземные робототехнические комплексы (на примере средств ВС США)

4.5.3.1. Общая характеристика задач наземных робототехнических комплексов

Планы DARPA Минобороны США состоят в том, чтобы в ближайшее время одна треть транспортных средств была построена на основе робототехнических систем. Кроме того, к 2025 г. планируется переход к полноценной робототехнической армии.

Наземные роботизированные комплексы сухопутных войск, по мнению специалистов, способны решать широкий спектр задач, основными из которых являются [95]:

- обнаружение, обследование и обезвреживание мин, фугасов и самодельных взрывных устройств;
- ведение разведки и наблюдения;
- вскрытие позиций снайперов, огневых средств, засад и систем наблюдения противника;
- обследование зданий, сооружений и отдельных объектов;
- доставка материально-технических средств к месту назначения.

До недавнего времени основные робототехнические комплексы для ВС США разрабатывались в рамках программы FCB. Однако, несмотря на то, что она закрыта, разработка инновационных средств вооруженной борьбы, включая системы управления и связи, а также большую часть робототехнических комплексов и БПЛА, была сохранена в рамках новой программы модернизации боевых бригадных групп. В рамках этой программы осуществляется разработка [29]:

- разведывательных сигнальных приборов;
- автономной ракетной и разведывательно-ударной систем;
- БПЛА;
- разведывательно-дозорных, ударно-штурмовых, портативных, а также легких дистанционноуправляемых машин для инженерного и тылового обеспечения.

При этом к наиболее массово-выпускаемым видам наземных робототехнических систем относят дистанционноуправляемые машины.

4.5.3.2. Дистанционноуправляемые машины

В настоящее время большинство наземных роботизированных комплексов состоят из дистанционноуправляемой машины (ДУМ) и пульта управления. Дистанционноуправляемые машины применяются для решения задач разведки местности, обнаружения взрывных устройств, разминирования и других задач [95].

Из состоящих на вооружении США ДУМ самой легкой и малоразмерной считается Recon Scout (масса – 1,3 кг, длина – 200 мм, оборудована видео- и ИК-камерой).

Одним из представителей гусеничных роботизированных мини-машин является First Look 110 (размеры – 250×230×100 мм; масса – 2,2 кг; оборудована 4 видеокамерами с подсветкой) [29].

ДУМ SpyRobot выпускается в двух вариантах – с шасси 4×4 и 6×6 (масса – 5 кг, разведывательная аппаратура включает тепловые и

оптические датчики, а также радиолокационную станцию с синтезированной апертурой). Основными задачами этого робота являются разведка в городских условиях, использование датчиков различного назначения в заданном районе, участие в поисковых операциях, разведка возможных засад и обнаружение слабых мест в обороне противника [29].

В результате модернизации машины SpyRobot была создана ДУМ Dragon Runner для разведки местности в радиусе эффективной дальности стрельбы стрелкового оружия (масса – 9 кг, размеры – 230×200×75 мм, оборудована ИК-датчиками и видеокамерой) [29].

Другим классом роботов является ДУМ Warrior 710 (масса – 157,4 кг). Она предназначена для обнаружения, транспортирования и обезвреживания взрывоопасных предметов, расчистки завалов, проделывания проходов и подъема тяжестей [29].

Робот PackBot выполнен на гусеничной платформе. Он успешно применялся в Ираке и Афганистане для обнаружения с помощью видеокамер взрывных устройств и неразорвавшихся боеприпасов. Именно самоходные гусеничные роботы проводили замеры уровня радиации внутри энергоблоков АЭС «Фукусима» на территории Японии в апреле 2011 г. Совершенствуя PackBot, компания-разработчик оснастила этот образец комплектом обнаружения снайпера, усилив тем самым его разведывательные возможности. Новая модификация робота (масса – 2,5 кг) получила название REDOWL (Robotic Enhanced Detection Outpost With Lasers), в переводе с английского «red owl» – «красная сова». Он оборудован лазерным дальномером, звукоулавливающим оборудованием, тепловизорами, GPS-приемником и 4 автономными видеокамерами. По сообщениям западных открытых источников, характеристики образца позволяют прочесть надпись на именном жетоне военнослужащего с расстояния 100 м, а также вести наблюдение ночью, в неосвещаемых помещениях и обеспечивать лазерную подсветку цели на дальность около 1,6 км, определять местоположение снайпера до и после выстрела с вероятностью 0,9 на удалении до 900 м. При этом оператор имеет возможность осуществлять целеуказание не только пехотным подразделениям, но и сообщать координаты позиции снайпера артиллерийскому или авиационному подразделению для нанесения точечного удара [95].

Машина разминирования MV-4 (или M160) массой 5,32 т предназначена для нейтрализации (обезвреживания) противопехотных мин и неразорвавшихся боеприпасов. Дистанционное управление этим средством предусмотрено на расстоянии до 2 км. Другим примером

ДУМ разминирования некоторых типов противопехотных и противотанковых мин является модель ABV (Assault Breacher Vehicle). По своим габаритам эта машина сравнима с танком Abrams. Появление полностью автономного варианта ДУМ ABV ожидается после 2025 г. [29].

Самым крупным боевым роботом в настоящее время можно считать ДУМ Black Knight (масса – 9,5 т, размеры – 5×2,4×2 м). Для автономного движения робота используется видеокамера, стерео- и ИК-камеры, лазерные локаторы, а также приемник сигналов космической радионавигационной системы NAVSTAR. Вооружение этой ДУМ включает 25- или 30-мм автоматическую пушку со спаренным 7,62-мм пулеметом [29].

Также необходимо упомянуть еще о двух роботах, которые разрабатывались в рамках программы FCB – MULE и SUGV.

Многоцелевая ДУМ MULE разрабатывается компанией Lockheed Martin на базе легкой платформы 6×6 м в трех вариантах [29].

1. Транспортный MULE-T.
2. Штурмовой MULE/ARV-A(L) планируется использовать для атак на укрепления противника и для обеспечения огневой поддержки наземных войск. Его предполагается оснастить противотанковыми управляемыми ракетами (ПТУР), 7,62-мм пулеметом (либо 30-мм пушкой, либо 40-мм гранатометом) и оптоэлектронными сенсорами. Аппарат будет в состоянии идентифицировать цели. Машина обладает самостоятельной навигацией и может перемещаться автономно.
3. Противоминный MULE-C, который создается для проделывания проходов в заминированных зонах.

Наземный малогабаритный переносной дистанционно управляемый аппарат SUGV предназначен для обезвреживания взрывных устройств, разведки и обнаружения противника в труднодоступных местах. Это первый робот, который полностью соответствует требованиям пехотных подразделений [29].

На вооружение 3-й пехотной дивизии уже поступают первые боевые роботы SWORDS. Данный робот предназначен для действий в городе, способен преодолевать песок, воду и снег до 0,3 м глубины, а также осуществлять подъем по лестнице. Он рассчитан на 8,5 ч работы от батарей в нормальном эксплуатационном режиме, в режиме ожидания до 7 суток. Контролируется оператором на расстоянии до 1 км.

Масса около 45 кг. Есть целый ряд различных видов оружия, которые могут быть размещены на SWORDS: винтовки M16, 5,56-мм SAW M249, 7,62 мм пулемет M240, шестиствольный 40-мм гранатомет или четырехствольный 66-мм M202A1 FLASH. Успешно применялся в Афганистане и Ираке.

К 2020 г. в США планируют разработать робота, который будет сопровождать военнослужащего, при этом управление будет голосовым и жестами [105, 106].

Разработку дистанционных робототехнических систем ведут не только в США. В данном направлении работают и другие технологически развитые страны, такие как Израиль и Южная Корея.

В Израиле автоматизация боевых действий уже стала основной тенденцией. Вдоль 60-километровой полосы Газа в настоящее время устанавливаются роботы-снайперы. Разработанные израильским военным концерном Rafael стационарные системы See-Shoot оснащены автоматическими пулеметами с камерами. Дальность их боя достигает 1500 м [89].

Сразу две израильские компании заняты разработкой автономных патрульных автомобилей, способных совершать регулярные объезды по периметру заданной местности, фиксируя любые изменения и самостоятельно преодолевая преграды, одновременно передавая информацию на контрольный пункт. Первым объектом охраны, на котором будут использованы автономные патрульные автомобили, судя по всему, станет аэропорт имени Бен-Гуриона. На данный момент эти автомобили безоружны, однако согласно оценкам специалистов уже в ближайшем будущем на них можно будет ставить системы вооружений. Авторы проектов считают, что за подобными автомобилями – будущее патрульной службы: они не устают, не теряют бдительности, не засыпают за рулем, и их уничтожение не влечет за собой потерь в человеческих жизнях [89].

На авиасалоне в Ле-Бурже в 2008 г. компания Elbit Systems Ltd представила первого в мире действующего боевого робота VIPeR, предназначенного для ведения боевых действий в городских условиях. Робот способен самостоятельно вести огонь и метать различные виды гранат. Его масса – 12 кг, длина – 36 см, ширина — 36 см, а высота – 22 см. Управление роботом – дистанционное. Он способен подниматься по лестницам и преодолевать препятствия, параллельно отслеживая все, что происходит вокруг. VIPeR вооружен специально сделанным для него мини-вариантом пистолета-пулемета Uzi калибром 9 мм, на котором установлен лазерный прицел. Согласно идее создателей, ро-

бот, имеющий небольшую массу, переносится одним из солдат боевой группы и включается, когда есть необходимость в проникновении в здание [89].

На выставке TADTE (Taipei Aerospace & Defense Technology Exhibition) в 2015 г. министерство обороны Тайваня представило новую ДУМ, предназначенную для повышения живучести и огневой мощи подразделений тайваньской армии [91]. Прототип легкой дистанционноуправляемой боевой машины RCLCV (Remote-Controlled Light Combat Vehicle), разработанный 209-м военным заводом в сотрудничестве с университетом Ченг Шу, предназначен для обеспечения поддержки подразделений в боевых операциях и может развертываться в составе мотопехотного отделения с бронетранспортера CM-32 Cloud Leopard. Разработчики представили два разных варианта, базирующихся на шасси гусеничного вездехода массой 200 кг [91]:

- платформа вооружения для поддержки ближним огнем;
- робот, предназначенный для выполнения опасных боевых задач, например, обезвреживания взрывоопасных предметов, обнаружения мин и эвакуации пострадавших.

Вариант огневой поддержки имеет стабилизированную опору, которая может принять различное вооружение, включая 5,56-мм легкий пулемет M249, 7,62-мм пулемет T74 местного производства, а также 12,7-мм крупнокалиберный пулемет QCB. Для борьбы с транспортными средствами на ДУМ можно установить легкий противотанковый гранатомет M72 или французский легкий гранатомет APILAS. Кроме основного вооружения, машина огневой поддержки также оборудована встроенной системой дневных/ночных камер и лазерным дальномером, которые передают на консоль оператора видео и тактические данные в реальном времени [91].

4.5.3.3. Робототехнические комплексы сопровождения и тылового обеспечения

Помимо роботов для непосредственного участия в боевых действиях, инженерами США и других технологически развитых стран активно прорабатываются вопросы использования робототехнических средств для решения небоевых задач, таких как тыловое и медицинское обеспечение, сопровождение грузов и др. Вскоре на каждого американского солдата может приходиться до 10 роботов обеспечения, способных на патрулирование местности и транспортировку снаряжения до прикрытия солдат на поле боя.

Так, между агентством передовых оборонных технологий Пентагона и Boston Dynamics в 2010 г. был подписан контракт на разработку для морской пехоты системы поддержки отряда LS3 (Legged Squad Support System), больше известной как AlphaDog или BigDog. Планировалось, что данная система позволит перемещать по пересеченной местности грузы, предназначенные для снабжения участвующих в боевых действиях подразделений спецназа и морской пехоты [110].

Робот-мул BigDog должен переносить на себе грузы массой до 180 кг на дальность до 32 км. Кроме того, его можно использовать в качестве источника энергии для портативных устройств. Однако затраченные на создание робота 42 млн долл. не окупились. Испытания летом 2014 г. в ходе учений RIMPAC-2014 выявили у него ряд проблем. «Проведенные учения с использованием роботов BigDog показали, что их применение затрудняет действия подразделений при выполнении боевых заданий. Связано это, в первую очередь, с ограниченными возможностями этих роботов, – заявил представитель корпуса морской пехоты К. Олсон. – Кроме этого, это слишком шумный робот, который полностью демаскирует позиции и перемещения морских пехотинцев».

Командование морской пехоты не устроила и облегченная версия робота BigDog – Spot. Его нагрузка не более 18 килограммов, и поэтому он не подошел морским пехотинцам в качестве транспортного средства, хотя и обладает рядом достоинств. На испытаниях Spot карабкался по каменистым холмам, продирался через лесную чащу и ориентировался в условиях городских улиц. Дистанционно управляемый робот примерил на себя и роль разведчика, изучая обстановку, до того как в здание войдут солдаты. Управление осуществляется с помощью обычного игрового контроллера от приставки Xbox, подключенного к ноутбуку [110].

Несмотря на успешное создание прототипов BigDog и Spot, агенство DARPA отказалось от проекта робота LS3. Однако технологии, отработанные при их создании компанией Boston Dynamics, заинтересовали корпорацию Google. Созданные новые технологии дают ей хорошую возможность работать по другим направлениям. Опять-таки по заказу DARPA она совершенствует уже созданные ею человекоподобные роботы Atlas (Agile Anthropomorphic Robot) и PETMAN (Protection Ensemble Test Mannequin) [110].

Робот Atlas предназначен для передвижения по пересеченной местности. Робот передвигается на двух ногах, может использовать

руки для переноса груза или при карабканьи на вертикальные препятствия. Рост робота составляет 188 см, ширина плеч – 76 см, масса – около 150 кг. Робот PETMAN используется для тестирования защитных костюмов. Он симулирует дыхание, потоотделение и изменения температуры тела в зависимости от количества и типа физических нагрузок. Очевидно, что его дальнейшее усовершенствование может открыть путь к разработке нового поколения человекоподобных роботов [110].

Недавно компания Boston Dynamics получила официальный контракт от американского оборонного института Sandia на создание военного робота PUH (Precision Urban Hopper – высокоточный городской кузнечик). По замыслу заказчиков, полнофункциональный PUH будет представлять собой небольшой четырехколесный робот, способный автономно перемещаться и даже перепрыгивать через препятствия. Мощная толчковая «нога» позволит ему преодолевать преграды высотой до 7,5 м. Легкая колесная платформа PUH идеально подходит для передвижения в городских условиях и позволяет доставлять необходимый груз в нужную точку [110].

Следует подчеркнуть, что Boston Dynamics далеко не единственная американская компания, с которой Пентагон сотрудничает в сфере военной робототехники. Об этом свидетельствует хотя бы тот факт, что среднегодовой объем финансирования НИОКР и закупок только наземных роботов будет составлять в ближайшие годы порядка 1,3-1,5 млрд долл. Таким образом, несмотря на нынешнюю экономическую непривлекательность многих проектов, а иногда и их бесперспективность, как это произошло с роботом BigDog, Пентагон продолжает проводить долгосрочную политику в области роботизированных и беспилотных средств вооруженной борьбы. Расчет делается на то, что это позволит не только снизить численность армии, но и значительно повысить ее боевые возможности [110].

4.5.4. Морские робототехнические комплексы (на примере средств ВС США)

4.5.4.1. Общая характеристика надводных и подводных робототехнических комплексов

В настоящее время ведущими технически развитыми странами и, прежде всего, США в интересах ВМС активно ведутся работы в области создания безэкипажных надводных платформ и необитаемых

подводных аппаратов. При этом, если в области создания полноценных необитаемых надводных платформ успехи пока достаточно скромны, то в области создания необитаемых подводных аппаратов (НПА) наметился ряд прорывных разработок. По всей видимости, в ближайшем будущем стоит ожидать резкого развития НПА, сходного с революционным развитием и внедрением БПЛА.

За последние два-три десятилетия в различных странах, занимающих ведущее положение в области морских технологий, было создано значительное количество НПА военного назначения. За этот период НПА не только продемонстрировали свою эффективность при выполнении разведывательных, противоминных и обзорно-поисковых работ, но и открыли ряд новых важных применений. Достижения в науке и появление новых технологий непрерывно расширяют сферу применения НПА, за последние 5-10 лет количество разработок автономных НПА выросло более чем 2 раза. На начало 2007 г. в мире насчитывалось более 155 проектов автономных НПА различного назначения. Однако их общее количество еще невелико и оценивается специалистами в пределах 550-650 единиц. Анализ содержания планов и бюджетных проектов НИОКР министерства обороны США показал, что в настоящее время существует не менее 10 крупных целевых программ, ориентированных на создание робототехнических комплексов на основе НПА. В рамках этих программ изучаются, разрабатываются и совершенствуются примерно 65-70 проектов НПА различных типов и размеров, а также формируются военно-технические концепции их применения [164].

Помимо разработки НПА ведутся работы в области создания надводных необитаемых аппаратов, однако не столь активно. Так, в настоящее время в Израиле ведутся испытания сразу двух видов безэкипажных плавательных аппаратов. Один из них – боевой катер Protector разработки компании Rafael, на который инженеры установили всю необходимую аппаратуру для обнаружения морских целей. Катер создан на базе фиберглассового десантного катера, способного нести более 1 т груза и которым пользуются израильские морские коммандос. В настоящее время на нем установлен пулемет калибром 7,62 мм, однако в будущем предполагается, что катер сможет нести значительно более тяжелое вооружение [89].

В 2003 г. во время операции «Свобода Ираку» для решения различных задач ВМС США уже применялись необитаемые морские аппараты, а позднее, в рамках программы МО США по демонстрации технических возможностей перспективных образцов вооружения и

техники в том же Персидском заливе проводились эксперименты по совместному применению аппарата SPARTAN и крейсера УРО Gettysburg в интересах ведения разведки [90].

В настоящее время к основным задачам необитаемых морских аппаратов относят [90]:

- противоминную борьбу в районах действия авианосных ударных групп, портов, военно-морских баз и др. Площадь такого района может варьироваться от 180 до 1800 кв. км;
- противолодочную оборону, включающую задачи контроля за выходами из портов и баз, обеспечение защиты авианосных и ударных групп в районах развертывания, а также при переходах в другие районы;
- обеспечение безопасности на море, предусматривающее защиту военно-морских баз и соответствующей инфраструктуры от всех возможных угроз, включая угрозу террористической атаки;
- обеспечение действий сил специальных операций;
- радиоэлектронную войну и др.

Для решения всех вышеуказанных задач могут применяться разнообразные типы дистанционноуправляемых, полуавтономных или автономных морских надводных аппаратов. Так, при решении задач противолодочной обороны 6 надводных автономных морских аппаратов способны обеспечить безопасное развертывание авианосных ударных групп, действующих в районе 36×54 км. При этом вооружением гидроакустических станций с дальностью действия 9 км обеспечивается 18-километровая буферная зона вокруг развернутой авианосной группы.

Помимо степени автономности, в ВМС США используется классификация по размерам и особенностям применения, позволяющая систематизировать все разрабатываемые необитаемые морские аппараты по четырем классам [90]:

- X-Class представляет собой небольшой (до 3 м) необитаемый морской аппарат для обеспечения действий ССО и изоляции района. Такой аппарат способен вести разведку для обеспечения действий корабельной группировки и запускаться даже с 11-метровых надувных лодок с жестким каркасом;
- Harbor Class – аппараты такого класса разрабатываются на базе стандартной 7-метровой лодки с жестким каркасом и предназначены для выполнения задач обеспечения морской

безопасности и ведения разведки, кроме того, аппарат может оснащаться различными средствами летального и нелетального воздействия. Скорость превышает 35 уз, а автономность – 12 ч;

- Snorkeler Class представляет собой 7-м полупогружной аппарат, предназначенный для противоминной борьбы, противолодочных операций, а также обеспечения действий ССО ВМС. Скорость аппарата достигает 15 уз, автономность – 24 ч;
- Fleet Class – это 11-м с жестким корпусом аппарат, разработанный для противоминной борьбы, противолодочной обороны, а также участия в морских операциях. Скорость аппарата варьируется от 32 до 35 уз, автономность – 48 ч.

Аналогичная классификация существует и у НПА.

Сама необходимость разработки и принятия на вооружение морских необитаемых аппаратов для ВМС США определена рядом официальных документов как собственно ВМС, так и вооруженных сил в целом. Это «Морская мощь 21» (Sea Power 21, 2002), «Всесторонний обзор состояния и перспектив развития ВС США» (Quadrennial Defense Review, 2006), «Национальная стратегия морской безопасности» (National Strategy for Maritime Security, 2005), «Национальная военная стратегия» (National Defense Strategy of the United States, 2005) и др. [90].

Широкое внедрение в ВМС США робототехнических комплексов базируется на сетецентрических технологиях, которые позволяют повысить оперативность и эффективность боевого управления и взаимодействия мобильных соединений флота с силами и средствами морского базирования, как в наступательных, так и в оборонительных операциях. Пример включения средств ВМС в общую сеть в соответствии с концепцией «Единая сеть ВМС (FORCEnet)» представлен на рис. 4.26 [166].

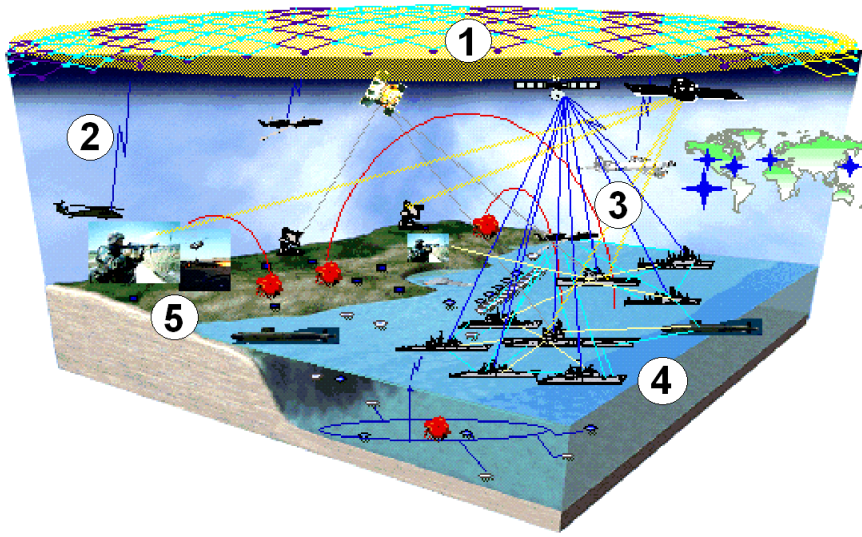


Рис. 4.26. Реализация концепции «Единая сеть сил ВМС» [166]: 1 – единая коммуникационная сеть; 2 – ведение непрерывного наблюдения средствами разведки, объединенными в сеть; 3 – каналы связи и передачи информации; 4 –сеть обмена информацией и система идентификации своих сил; 5 –взаимодействие с другими родами войск и военными структурами.

Отдельная существенная роль в сетецентрической системе ВМС отводится необитаемым аппаратам, поставляющим информацию о вражеских территориях и акваториях, а также выступающим в качестве боевых платформам. Информация, полученная роботами, поступает на бортовые компьютеры автоматизированной системы боевого управления сил, участвующих в операции, которые находятся в «едином информационном боевом пространстве». При этом наблюдается характерная тенденция к расширению взаимодействия между необитаемыми подводными и надводными аппаратами и развертываемыми наземными, подводными (находящимися в толще воды), донными, а также воздушными системами необслуживаемых датчиков рис. 4.27 [166, 167].

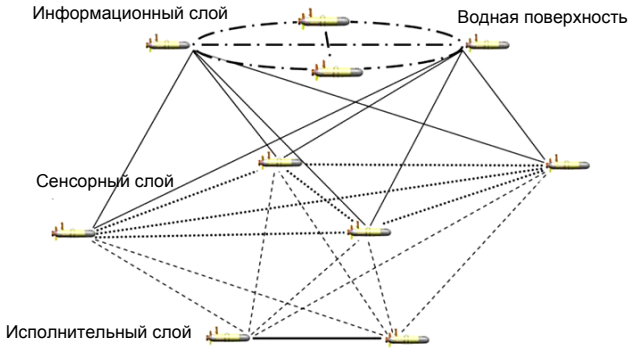


Рис. 4.27. Организация обмена информацией между надводными и подводными датчиками, аппаратами и носителями на основе сетецентрического подхода [166, 167]

При сетецентрическом принципе управления морскими робототехническими комплексами информационный слой может состоять из всплывающих на поверхность НПА, надводных роботизированных аппаратов, БПЛА, буев или надводных кораблей обеспечения в различных сочетаниях. Сенсорный слой формируется группой НПА, оснащенных аппаратурой освещения и анализа обстановки, а также многоканальными средствами связи и навигации. В свою очередь аппараты, составляющие исполнительный слой, выполняют конкретные поставленные перед группой НПА задачи (например, физическое уничтожение обнаруженных мин).

Таким образом, в рамках внедрения концепции сетецентрической войны круг задач, возлагаемых на надводные и подводные робототехнические комплексы, существенно расширяется. Во многом это определяется возрастающим значением таких присущих им качеств, как скрытность действий, автономность и способность нести разнообразную полезную нагрузку. В этой связи возможны следующие направления применения надводных и подводных необитаемых аппаратов [164]:

1. Скрытное оборудование за акваториями ТВД, в том числе и в территориальных водах вероятного противника, за элементами радиоэлектронных систем различного назначения, а именно:

- системами гидроакустической навигации и связи для обеспечения боевой деятельности подводных лодок, НПА и подводных средств движения подразделений боевых пловцов;

- системами освещения подводной обстановки;
- системами ведения радиотехнической разведки.

2. Применение НПА в качестве элемента системы освещения обстановки:

- размещение на борту НПА гидроакустических станций дальнего обнаружения с гибкой протяженной буксируемой антенной и гидроакустической системой связи для совместных действий с маневренными и стационарными гидроакустическими средствами;
- размещение на борту НПА излучающей антенны для гидроакустической «подсветки» целей;
- размещение на борту НПА гидроакустических станций ближнего радиуса действия в интересах обеспечения собственной безопасности.

3. Сбор, обобщение и доставка геофизической информации, в том числе информации о гидрометеорологическом режиме, гидрофизических и гидролого-акустических полях, геоморфологии морского дна, характере береговой черты и др., в интересах достоверной оценки и прогноза эффективности применения высокоточного оружия. Элементами этой системы могут являться распределенные в пространстве датчики, размещаемые на борту НПА либо стационарно на грунте, а также дрейфующие в толще воды и на поверхности.

4. Поддержание технического состояния различных систем долговременного действия (например, универсальных подводных автономных модулей и станций):

- диагностика их технического состояния;
- коррекция программного обеспечения;
- зарядка источников питания.

5. Защита от несанкционированного доступа к развернутым системам и средствам их информационным потокам.

6. Обеспечение стыковки информационных потоков, поступающих от различных систем освещения обстановки (радиоэлектронной, гидроакустической, оптоэлектронной и др.), а также глобальных информационных центров и центров управления, с каждой «боевой единицей» (подводной лодкой, надводным кораблем, самолетом, вертолетом, БПЛА, НПА, разведывательно-диверсионной группой).

Ряд возможных применений необитаемых надводных и подводных аппаратов в военных целях проиллюстрирован на рис. 4.28-4.31 [166, 168]. На них введены следующие дополнительные обозначения: НК – надводный корабль; ННА – необитаемый надвод-

ный аппарат; КА – космический аппарат; ГАС – гидроакустическая станция; ВОЛС – волоконно-оптическая линия связи; СРНС – спутниковая радионавигационная система.

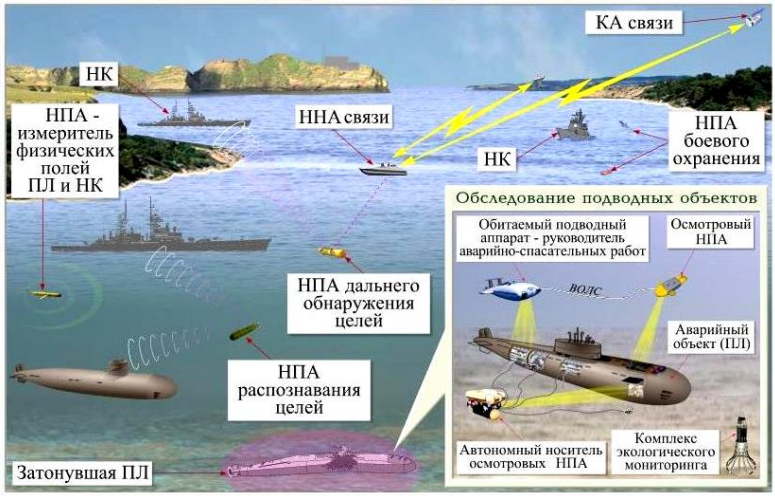


Рис. 4.28. Применение НПА и ННА для освещения оперативной обстановки [166, 168]

Рис. 4.29. Применение НПА в целях противолодочной обороны [166, 168]

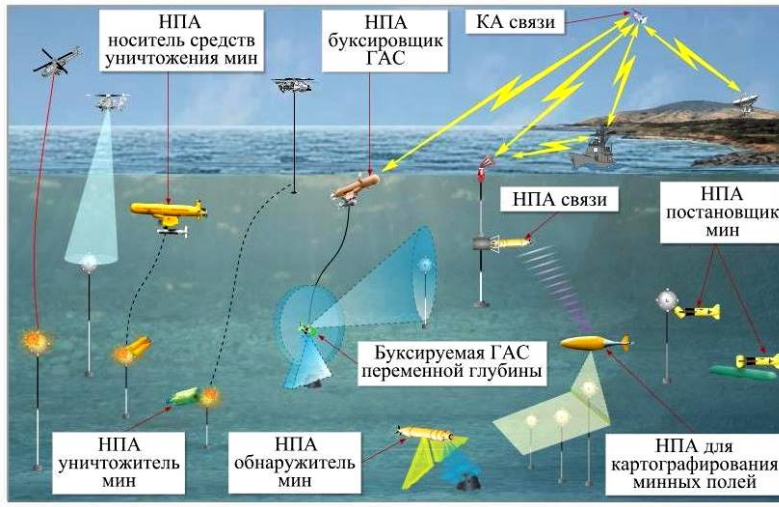


Рис. 4.30. Применение НПА для поиска
и уничтожения мин [166, 168]

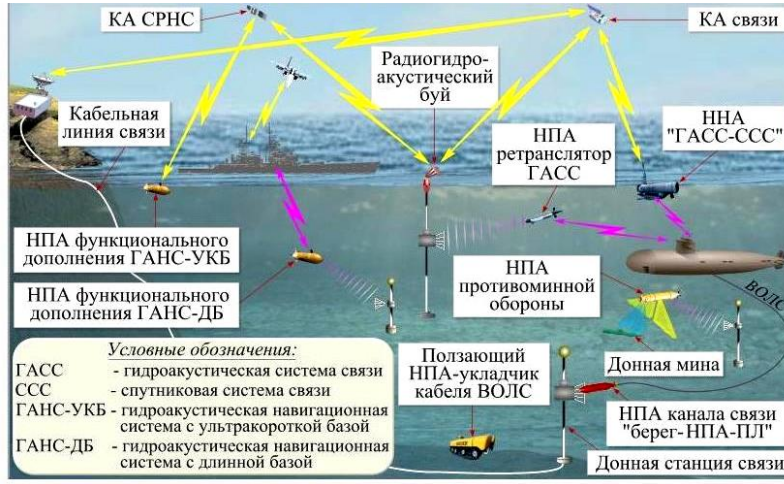


Рис. 4.31. Применение НПА при развертывании
подводной связи [166, 168]

В ВМС США в рамках внедрения концепции сетецентрической войны за последние 5-10 лет значительная часть программ исследований и разработок была ориентирована на отработку элементов распределенной системы освещения подводной обстановки в прибрежных

мелководных районах. По замыслу американских военных, создание такой системы позволит вести продолжительное наблюдение за подводной обстановкой, своевременно обнаруживать и распознавать подводные цели на акватории общей площадью до 100-200 тыс. кв. км, а ее оперативное развертывание – обеспечивать эффективное решение следующих задач [164]:

- формирование противолодочных барьеров на маршрутах развертывания подводных сил противника;
- повышение живучести ракетных подводных лодок;
- охрана авианосно-ударных групп, корабельных поисково-ударных групп, десантных соединений и конвоев от многоцелевых подводных лодок противника;
- защита морских коммуникаций от подводных лодок противника;
- подготовка скрытого проведения специальных операций (например, таких как: минирование, разведка, наблюдение, высадка диверсионно-разведывательных групп).

Официально объявленной американским военным руководством целью создания распределенной системы освещения подводной обстановки является защита от угроз действия дизельных подводных лодок потенциального противника в своих прибрежных водах. Высокая оперативность ее развертывания в заданных районах будет обеспечиваться подводной лодкой, выступающей в качестве носителя автономных стационарных и мобильных измерительных средств системы [164, 166].

Существующие в США планы развития необитаемых подводных аппаратов предполагают их стремительную интеллектуализацию, которая приведет к возникновению принципиально нового класса устройств, которые смогут самостоятельно производить поиск подводных и надводных объектов противника, идентифицировать их и уничтожать, при этом оставаясь практически незаметными для самого противника (рис. 4.32).

В генеральном плане развития НПА, выпущенном в 2004 г. [176], было обозначено девять высокоприоритетных задач, которые обеспечивают действия в четырех направлениях, определенных планом «Морская мощь 21» (Sea Power 21). В порядке приоритетности данные девять задач представлены ниже [166]:

- разведка;
- противоминная борьба;
- противолодочная оборона (ПЛО);

- осмотр и идентификация подводных объектов;
- океанография;
- обеспечение связи и поддержка навигационных сетей;
- подводная доставка грузов;
- информационные операции;
- обеспечение внезапности удара.

Рис. 4.32. План развития морских роботизированных систем США до 2034 г. [166, 175]

Таким образом, можно констатировать, что текущий этап развития необитаемых морских аппаратов характеризуется созданием базовой основы для долговременного развития этого направления подводной техники. Основные разработки по всем направлениям развития надводных и подводных аппаратов активно проводятся в США, однако целый ряд других стран, в том числе входящих в блок НАТО, также имеет существенные наработки в данной области. При этом реализация планов развития НПА военного назначения может привести к революционным изменениям в конструктивном облике подводных лодок, а также существенному изменению тактики их действий.

Дополнительные сведения о тенденциях развития и ТТХ необитаемых надводных и подводных аппаратов изложены в работах [44, 89, 90, 164, 166, 197].

4.5.4.2. Перспективные разработки разведывательно-ударных необитаемых подводных и гибридных аппаратов

Рассмотрим основные тенденции и перспективные разработки в области создания и применения НПА на основе соответствующих проектов в ВМС США.

Автономный НПА типа Manta. С 1996 г. НИЦ подводной войны ВМС США – NUWC (Naval Undersea Warfare Center) реализует программу UUVI (Unmanned Undersea Vehicle Initiative), направленную на разработку перспективных автономных НПА нового поколе-

ния. Согласно концепции, получившей наименование Manta, НПА будет способен решать следующие задачи [164]:

- обнаружение и уничтожение подводных лодок, мин и других подводных целей с применением тяжелых и легких торпед, неуправляемых ракет, а в перспективе и высокоскоростных (суперкавитирующих) боеприпасов;
- ведение гидроакустической, радиотехнической и оптоэлектронной разведки;
- установка быстроразвертываемых позиционных, мобильных и дрейфующих линейных антенн, низкочастотных гидроакустических излучателей, необслуживаемых подводных датчиков длительного действия и др., а также прибрежных систем обнаружения подводных лодок;
- осуществление широкополосной цифровой звукоподводной связи, управление распределенной сетью датчиков, ретрансляция данных от выдвинутых к побережью систем разведки и обнаружения подводных лодок на корабельные и береговые командные центры и центры тактической поддержки;
- развертывание малогабаритных автономных НПА для решения обеспечивающих и специальных задач;
- сбор гидрологических и океанографических данных, картографирование морского дна в интересах боевого обеспечения действий подводных лодок и надводных кораблей.

Аппаратами типа Manta планируется вооружить атомные подводные лодки типа Virginia, а также многоцелевые атомные подводные лодки перспективных проектов. Эти лодки будут нести 4 разведывательно-ударных НПА, размещенных в носовой части в нишах легкого корпуса. В печати отмечается, что большинство концептуальных и технологических решений, необходимых для реализации с помощью НПА вышеуказанных задач, уже разработано или находится на заключительном этапе разработки. Кроме того, определены две концепции создания НПА Manta [164].

Первая концепция, получившая наименование Proud conformal, предусматривает постройку НПА длиной 15 м, оснащенного 2 маршевыми движителями, 4 подруливающими устройствами, а также бортовым оборудованием управления и энергообеспечения. Аппарат данного типа будет способен нести полезную нагрузку (разведывательно-ударный модуль) массой до 8 т. В состав модуля войдут средства гидроакустической, радиотехнической и оптоэлектронной разведки, 6-8

малогабаритных, 2 легкие и 2 тяжелые торпеды, а также их пусковые установки [164].

Вторая концепция, названная Integrated conformal (получила обозначение Super Manta), рассматривает возможность создания аппарата длиной 25 м, водоизмещением 90 т, способного нести полезную нагрузку массой до 14 т [164].

Испытания экспериментального образца НПА Manta ведутся с 1999 г. Исследовались варианты комплектации модуля полезной нагрузки и тактики применения НПА (вплоть до его перезарядки торпедами на плавбазе снабжения атомных подводных лодок). На морских испытаниях двухсторонняя подводная связь аппарата с обеспечивающим судном осуществлялась с помощью универсального акустического модема, разработанного специалистами института в Woods Hall (скорость передачи данных составила 1,75 кбит/с), затем обеспечивающее судно через спутниковый канал связи ретранслировало полученные данные на береговой узел связи. В 2001 г. исследовались возможности ведения аппаратом радиотехнической и оптоэлектронной разведки. В частности, проводились испытания выдвижного подъемно-мачтового устройства с антенной обнаружения радиолокационных сигналов, разработанного фирмой Sean Sea Tea. Проводились испытания трех видеокамер гражданского образца: одной – переднего обзора и двух – бокового. Испытывалась инфракрасная аппаратура фирмы Sensor Unlimited, установленная в верхней части вертикального стабилизатора (ниже ее была вмонтирована обычная видеокамера для сравнения результатов). Изображение подводной обстановки от цифровых видеокамер передавалось по каналу гидроакустической связи на обеспечивающее судно и далее по спутниковому каналу связи ретранслировалось на атомную подводную лодку Prowidens, находящуюся в доке (на данной подводной лодке развернут пост управления НПА). Известно, что оператор наблюдал изображение подводной обстановки на мониторе, мог управлять маневрированием аппарата и активизировать командами необходимые программы [164].

В одном из вариантов полезной нагрузки разведывательно-ударного НПА Manta предусматривается оснащение его пусковой установкой для сверхскоростных (суперкавитирующих) боеприпасов. На испытаниях в 2002 г. продолжалась отработка вариантов компоновки торпедного оружия, в том числе изучалась способность НПА нести сверхскоростные боеприпасы (программа Supercav). Также исследовались и оценивались с учетом технического риска варианты стыковки аппарата с подводной лодкой, проблемные вопросы пуска,

управления и обратного приема аппарата на ходу, а также взаимное влияние этих операций на гидроакустические средства подводной лодки и аппарата [164].

В качестве примера гибридного необитаемого аппарата, который можно отнести как к подводному, так и надводному классу, можно привести аппарат, получивший наименование ACTUV (Anti-submarinewarfare Continuous Trail Unmanned Vessel). Общая масса аппарата составляет около 157 т длина корпуса примерно 19 м, при этом корпус судна в рабочем состоянии практически полностью погружается под воду, а над поверхностью воды остается только небольшая часть (арка), внутри которой будут расположены системы связи с оператором. Судно развивает максимальную скорость до 35 узлов при автономности функционирования на срок до 30 суток [166, 178].

4.5.4.3. Перспективные разработки многоцелевых реконфигурируемых автономных необитаемых подводных аппаратов

В ВМС США ведется программа разработки многоцелевых автономных НПА – MRUUV (Multi Mission Reconfigurable Unmanned Undersea Vehicle). Они предназначены для применения с подводных лодок и будут способны обеспечивать решение широкого круга задач в интересах корабля-носителя, оперативных формирований флота и высшего командования. Автономный НПА типа MRUUV имеет следующие тактико-технические характеристики: длина 6,06 м, диаметр 0,533 м; масса 1360 кг; предельная глубина погружения 300 м; минимальная рабочая глубина 12 м; скорость хода 8 уз; мощность гребного электродвигателя 1,5 кВт (один винт в насадке с изменяемым вектором тяги). Автономность аппарата зависит от типа применяемых источников электрической энергии (16 ч с литиево-ионной аккумуляторной батареей и более 60 ч с батареей одноразовых литиевых источников тока). В состав бортового навигационного комплекса входят: ИНС, приемники GPS или NAVSTAR, доплеровский лаг и гидроакустическая навигационная система. Состав бортовой аппаратуры: гидроакустическая система высокоточного картографирования дна и обнаружения препятствий L-PUMA, средства радиотехнической и оптоэлектронной разведки, пассивные и активные ГАС поиска целей и выдачи целеуказания оружию, а также аппаратура радио- и гидроакустической связи [164].

Аппарат типа MRUUV состоит из 7 отсеков:

- носовая (первая) секция включает сонар и гидроакустическую систему связи;
- вторая секция включает системы управления, навигации, связи и распределения энергии;
- третья секция включает оборудование GPS, SATCOM, антенны радиосвязи с подъемно-мачтовым устройством, якорное устройство и носовую балластную цистерну;
- четвертая секция имеет объем для размещения полезной нагрузки объемом до 36 л со стандартными интерфейсами;
- пятая секция включает балластный насос, клапанный блок и кормовую балластную цистерну;
- шестая секция включает источник электрической энергии с обеспечивающими системами;
- седьмая (кормовая секция) включает электродвигатель и ряд вспомогательных систем.

Сами аппараты MRUUV и их корабельное оборудование на период выполнения боевой задачи размещаются на стеллажах торпедного отсека подводных лодок типов Los Angeles и Virginia, что уменьшает боекомплект последних на 8-10 ед. оружия. Запланирована поставка 11 комплексов НПА MRUUV (в состав одного комплекса входит один НПА со сменными отсеками) и дополнительно к ним еще 31 НПА.

Еще большими возможностями и гибкостью применения будет обладать крупный НПА типа MRUUV-L. Этот аппарат, имеющий, по предварительным оценкам, длину до 11 м, ширину до 2 м и массу около 70 т, будет способен развивать скорость хода 18-25 уз. В рамках программы создания многоцелевых реконфигурируемых автономных НПА типа MRUUV-L прорабатываются следующие 7 вариантов их технического оснащения применительно к различным носителям [164]:

- ISR Mission Reconfigurable Modules – модули полезной нагрузки и навесного оборудования для решения задач разведки, освещения надводной и подводной обстановки;
- Detect/Engage Mission Reconfigurable Modules – модули полезной нагрузки для обнаружения целей, целеуказания и наведения оружия, а также комплекс боевого оснащения (минное и торпедное вооружение);
- COMMs Relay Mission Reconfigurable Modules – модули полезной нагрузки для организации надводной и подводной связи (радио и гидроакустические модемы). Преду-

сматривается возможность функционирования оборудования в режимах ретранслятора (т.е. точки доступа) и беспроводного телекоммуникационного концентратора (шлюза) радио- и гидроакустического каналов связи;

- MIW Mission Reconfigurable Modules – полезная нагрузка для решения задач минной войны: выполнение противоминных действий (разведывательный поиск мин и картографирование минных заграждений, уничтожение мин) или постановки минных заграждений;
- ASW Mission Reconfigurable Modules – модули полезной нагрузки для решения задач противолодочной обороны, включающие аппаратуру и буксируемые средства для обнаружения, классификации и идентификации подводных лодок, средства постановки активных помех и пусковые устройства для легких противолодочных торпед;
- ASUW Mission Reconfigurable Modules – модули полезной нагрузки для борьбы с подводными лодками противника;
- Search & Survey Mission Reconfigurable Modules – модули полезной нагрузки для проведения поисковых и осмотровых работ.

Наряду с выполнением перечисленных выше задач, НПА MRUUV-L сможет выступать в качестве носителя малогабаритных БПЛА и мини-НПА, выставлять многочисленные подводные системы, а также эффективно вести сбор и передачу разведывательных данных [164].

4.5.4.4. Перспективная система освещения подводной обстановки на основе необитаемых подводных аппаратов

Один из вариантов построения автономной информационно-измерительной сети подводного наблюдения рассматривается в рамках комплексной программы ВМС США – PLUSNet (Persistent Littoral Undersea Surveillance Network). К числу основных задач, решаемых в рамках программы PLUSNet, относится освещение подводной обстановки [164]:

- отработка способов и технических средств, необходимых для развертывания мобильных и стационарных узлов сети с борта подводной лодки в заданном районе;
- экспериментальная оценка возможностей измерительных средств мобильных и стационарных измерительных

средств сети по достоверному и своевременному обнаружению подводных целей в охраняемом районе. Большой объем исследований по данному направлению выполняется по программе UPS (Undersea Persistent Surveillance);

- демонстрация возможностей автоматического формирования беспроводной сети стационарных и мобильных абонентов, точек доступа, средств сбора и передачи информации с использованием гидроакустических и радиочастотных каналов связи (большая часть технических вопросов в данном направлении отрабатывалась в ходе реализации программы SeaWeb).

В состав стационарных средств, отрабатываемых в рамках проекта PLUSNet, входят следующие компоненты [164]:

- заякоренные подповерхностные буи. Каждый буй оснащен вертикальной многоэлементной протяженной гидроакустической антенной длиной 75 м (пассивная ГАС с вертикальной многоэлементной антенной Kelp) и малогабаритным гидроакустическим модемом;
- донные станции, каждая из которых имеет две протяженные горизонтальные антенны с гидроакустическими и электромагнитными датчиками (для измерения вектора гидроакустического и параметров электромагнитного полей) и малогабаритный модем гидроакустической связи.

В состав мобильных средств, отрабатываемых в рамках проекта PLUSNet, входит группировка, состоящая из 5 проектов автономных НПА [164]:

- автономные НПА торпедообразной формы на основе гребных электродвигателей (проекты Bluefin 21, BPAUV, Odyssey III и Seahorse);
- автономные НПА планерной формы с системой движения, основанной на изменении собственной (остаточной) плавучести аппаратов (проекты Seaglider, Slocum Glider, XRay).

Автономный НПА Bluefin-21 является носителем низкочастотной гидроакустической буксируемой антенной решетки, состоящей из 21 низкочастотного гидрофона. Большой автономный НПА Sea Horse является носителем низкочастотной пассивной ГАС LUPA (с антенными решетками, размещенными по бортам аппарата). Большой автономный НПА – планер XRay является носителем среднечастотной ГАС, антенные решетки которой вмонтированы в переднюю кромку крыльев аппарата. Автономный НПА – планер Sea Glider является но-

сителем ГАС с направленными гидрофонами, а также датчиков измерения параметров водной среды (температуры, давления и солености) [164].

При боевом применении системы PLUSNet предполагается, что сетевое оборудование должно скрытно доставляться и разворачиваться в непосредственной близости от побережья атакуемой страны. Например, ПЛАРБ типа Ohio, переоборудованные как носители крылатых ракет Tomahawk (далее ПЛАРК), могут быть адаптированы как носители группировки НПА и другого оборудования сети PLUSnet [164].

Проект PLUSnet предусматривает размещение материальной части в 5 модулях полезной нагрузки, которые загружаются в переоборудованные ракетные пусковые шахты. В модулях находятся [164]:

- 1 большой автономный НПА типа Sea Horse;
- 1 большой автономный НПА-планер типа XRay;
- 6 автономных НПА типа Bluefin 21;
- 18 автономных НПА-планеров типа Sea Glider;
- 9 контейнеров с разворачиваемыми протяженными гидроакустическими антеннами.

Последовательное извлечение всех НПА из ракетной шахты, старт аппаратов и их возвращение в шахту обеспечиваются при помощи универсального модуля URLM (Universal Launch and Recovery Module).

В качестве иллюстрации последних разработок американских специалистов в направлении PLUSnet можно привести комплекс DADS (Deployable Autonomous Distributed System). Развертываемая автономная протяженная система DADS – это акустический комплекс быстрого реагирования рубежного типа, оперативно разворачиваемый для защиты гаваней, заливов или бухт дислокации подводных лодок в любой прибрежной акватории (рис. 4.33) [166]. При этом количество НПА в комплексе определяется протяженностью рубежа наблюдений [166].

В качестве иллюстрации взаимодействия между элементами подобной информационно-измерительной сети подводного наблюдения можно привести схему (рис. 4.34) организации испытаний сети «Морская паутина» (Seaweb network). Данные испытания проводились в рамках учений в Мексиканском заливе 1-8 февраля 2003 г. [166, 169].

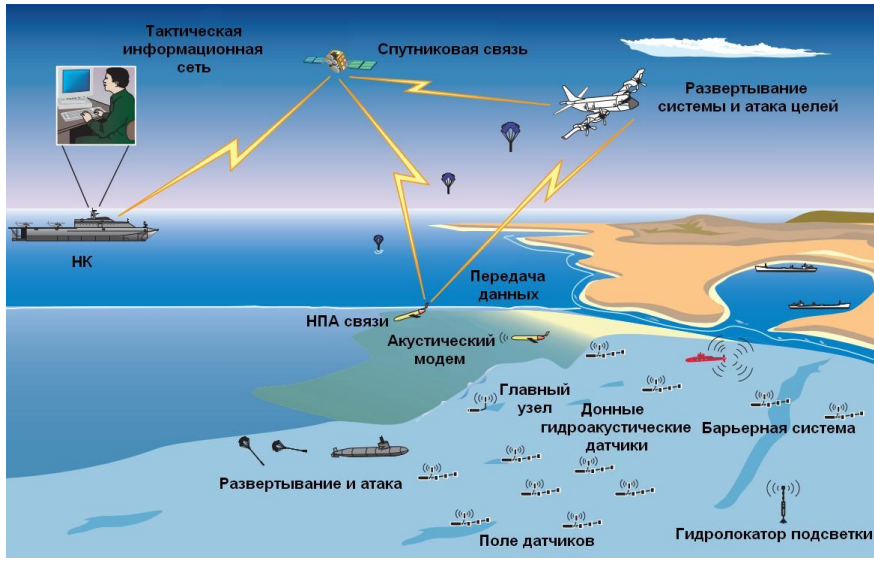


Рис. 4.33. Построение комплекса DADS [166, 172]

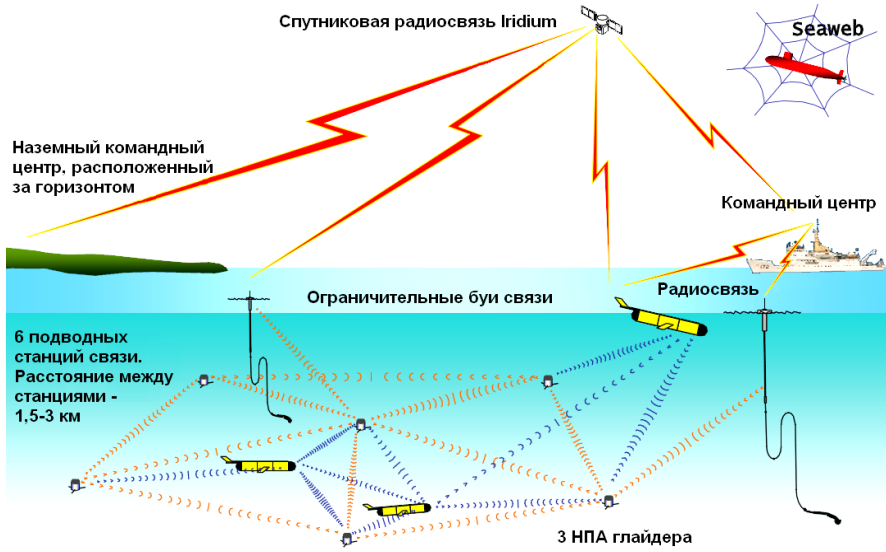


Рис. 4.34. Схема взаимодействия элементов сети Морская паутина [166, 169]

Таким образом, особое внимание активному применению развертываемых необслуживаемых датчиков, взаимодействующих с необитаемыми морскими аппаратами, предполагается уделить в сфере борьбы с подводными лодками противника в прибрежных водах США и их стран-союзников. Это связано с тем, что такие системы позволяют обеспечить ударные противолодочные силы гораздо более точным целеуказанием, чем это было раньше [166].

По мнению американских специалистов, создание подобных систем позволит вести продолжительное наблюдение за подводной обстановкой, своевременно обнаруживать и распознавать подводные цели на обширной акватории, а ее оперативное развертывание будет обеспечивать эффективное решение целого ряда важных стратегических задач [166].

4.6. Информационное оружие

4.6.1. Актуальность развития информационных средств и способов воздействия в современных сетецентрических конфликтах

Военно-политическое руководство США первым начало рассматривать информационное пространство как новую сферу ведения боевых действий наряду с наземной, морской и воздушно-космической сферами. Для данной сферы характерна своя специфическая форма ведения боевых действий – информационное противоборство.

Информационное противоборство – борьба в информационной сфере, которая предполагает комплексное деструктивное воздействие на информацию, информационные системы и информационную инфраструктуру противоборствующей стороны с одновременной защитой собственной информации, информационных систем и информационной инфраструктуры от подобного воздействия. Целью информационного противоборства является завоевание и удержание информационного превосходства над противоборствующей стороной [216, 349].

Объектом информационного противоборства является любой объект, в отношении которого возможно осуществление информационного воздействия (в том числе применение информационного оружия) либо иного воздействия (силового, политического, экономического, технического и т. д.), результатом которого будет модификация

его свойств как информационной системы. Объектом информационного противоборства может стать любой компонент или сегмент информационного пространства, в том числе массовое и индивидуальное сознание граждан; социально-политические системы и процессы; информационная инфраструктура; информационные и психологические ресурсы; технические системы передачи и обработки информации а также системы управления [216, 349].

К субъектам информационного противоборства относят: государства, их союзы и коалиции; международные организации; негосударственные незаконные (в том числе незаконные международные) вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности; транснациональные корпорации; виртуальные социальные сообщества; медиакорпорации и СМИ; виртуальные коалиции [349].

Анализ результатов операции «Буря в пустыне», в которой применялись первые элементы информационных операций, провел генерал-майор Г. Отис. В опубликованных им работах указывалось: «Из операции «Буря в пустыне» можно извлечь много уроков. Один урок тем не менее является поистине фундаментальным. Природа войны коренным образом изменилась. Та сторона, которая выиграет информационную кампанию, победит. В этой войне мы продемонстрировали этот урок всему миру: информация является ключом к современной войне в стратегическом, оперативном, тактическом и техническом отношении» [95].

По заключению специальной объединенной комиссии Пентагона и ЦРУ, исследовавшей проблематику информационного противоборства и ее составляющей – информационной безопасности: «...информационные технологии позволят обеспечить разрешение геополитических кризисов, не производя ни одного выстрела. Наша политика обеспечения национальной безопасности и процедуры ее реализации должны быть направлены на защиту наших возможностей по ведению информационных войн и на создание всех необходимых условий для воспрещения противоборствующим США государствам вести такие войны» [95].

Военные аналитики США сравнивают ущерб от нарушения функционирования информационных систем страны с последствиями применения стратегического ядерного оружия. Таким образом, поражение в информационной войне надолго отбрасывает «проигравшую» страну на обочину мировой истории. И, наоборот, страны, добившиеся

подавляющего преимущества в информационной области, смогут с достаточно высокой степенью вероятности моделировать поведение остальных стран, «заставляя» их делать определенные ходы. Одним словом они получат неограниченные возможности управления побежденными странами, которым будет очень трудно «догонять» своего соперника [131].

В настоящее время диапазон возможностей информационного оружия настолько велик, что имеются прецеденты достижения победы в операциях и конфликтах только за счет его применения, без использования традиционных средств вооруженной борьбы. При этом информационное противоборство ведется постоянно как в мирное, так и в военное время. Оно может вестись не только между государствами-противниками, но и между государствами-союзниками во имя достижения своих целей [13].

Технологическое опережение в области информатизации США принимают как одну из главных предпосылок реализации своего информационного преимущества. В то же время военные аналитики США констатируют, что современные информационные технологии доступны любому, кто имеет финансовые возможности получить их. Постоянно увеличивающиеся распространение и доступность информации создают для потенциального противника (при растущей зависимости США от информации и информационных систем) предпосылки достижения временного или локализованного паритета в боевом пространстве или асимметричного преимущества [16].

В настоящее время, по мнению ряда экспертов Пентагона, информационная сфера остается единственной областью боевых действий, где у США имеются равные противники. По мнению экспертов, в этом отношении наибольшую опасность для США представляет Китай, власти которого к середине XXI века намерены добиться такого уровня развития информационных технологий, который позволит им обеспечить полную победу в информационной войне [95].

Пентагон уже давно занимается реализацией программ обеспечения безопасности своего информационного пространства. В их основе лежит подход, названный разработчиками «глубокая оборона» (Defense-in-Depth). В информационных системах, создаваемых в соответствии со сформулированными в его рамках принципами, предусматривается многоступенчатая защита. Она функционирует, используя активные и пассивные мероприятия, позволяющие предотвратить неправомочный доступ к информации. Глубокая оборона защищает наиболее важные критические структуры военного ведомства. Специ-

алисты полагают, что такое построение защиты важных информационных ресурсов Пентагона заставит потенциальных противников США расходовать значительные средства, чтобы получить возможности для ее преодоления [95].

Далее в кратком виде рассмотрим особенности реализации информационное оружие в технической и психологической сфере. В более полном виде данные об информационном оружии в технической и психологической сфере представлены в работе [462].

4.6.2. Общие понятия об информационном оружии

4.6.2.1. Определение информационного оружия

К информационному оружию сейчас нередко относят широкий класс приемов и способов информационного воздействия на противника – от дезинформации и пропаганды до средств радиоэлектронной борьбы. При этом на сегодняшний день нет единого толкования понятия «информационное оружие». В различных источниках приводятся различные определения этого понятия. При этом наиболее общим является следующее.

Информационное оружие – совокупность средств информационного воздействия на технику и людей [2, 360].

В соответствии со сферами, в которых ведется информационное противоборство, информационное оружие подразделяется на два основных вида [2, 360]:

- информационно-техническое оружие;
- информационно-психологическое оружие.

Главными объектами информационного оружия первого вида является техника, второго – люди.

При этом надо подчеркнуть, что информационно-техническое оружие включает в себя средства РЭБ, а информационно-психологическое оружие является элементом более широкого типа оружия – психологического оружия (рис. 4.35).

Полковник ВВС США Р. Сафрански, один из идеологов концепции сетецентрической войны дает достаточно широкое определение информационному оружию.

Информационное оружие – использование специально подобранных средств, под воздействием которых происходит изменение процессов не только в информационных, но также и в социальных системах в соответствии с поставленными целями [13].

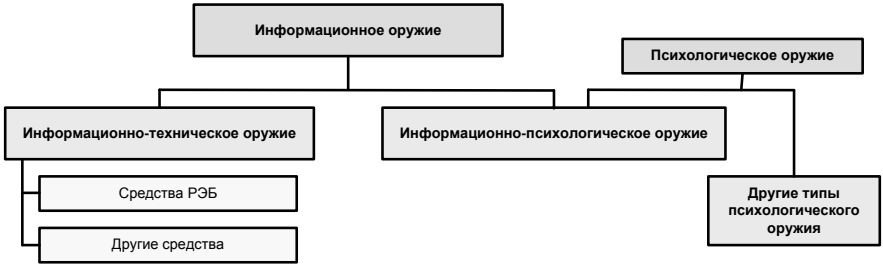


Рис. 4.35. Основные виды информационного оружия [462]

Применять информационное оружие предполагается на стратегическом, оперативном и тактическом уровнях. При этом основными объектами его воздействия являются информационно-технические системы (от финансово-экономических до систем управления войсками), социальные системы, отдельные личности или группы лиц (то есть групповое и индивидуальное сознание) [13].

Оригинальный подход к определению понятия «информационное оружие» сделан в работе [368]. В соответствии с этой работой дано следующее определение информационному оружию.

Информационное оружие – различные средства поражения: высокоточное оружие для поражения органов управления или отдельных радиоэлектронных средств, средства радиоэлектронной борьбы, источники мощного электромагнитного импульса, программные вирусы и др., эффективно решающие задачи информационной войны [368].

Спорным в данном подходе является отнесение к классу информационного оружия большинства средств поражения и физического оружия по той лишь причине, что оно обеспечивает физическое уничтожение органов управления и радиоэлектронных систем (РЭС) противника.

В работах [368] и [368] приводятся близкие по смыслу определения информационного оружия.

Информационное оружие – совокупность информационных технологий, способов и средств информационного воздействия, предназначенных для ведения информационной войны [368].

Информационное оружие – оружие, наиболее эффективно решающее задачи информационной войны, основной задачей которой является достижение информационного превосходства [368].

Указывая на недостаток двух приведенных выше определений информационного оружия, заключающийся в привязке данного поня-

тия к неоднозначно трактуемому в различных источниках понятию «информационная война», автор монографии [369] приводит следующее определение этого вида оружия.

Информационное оружие – это средства информационного воздействия на технику и людей с целью решения задач воздействующей стороны и специфичные способы их применения [369].

Это определение, а также определение, представленное в работах [2, 360], по мнению авторов, являются наиболее общими и полными и включают в себя всю совокупность средств для организации воздействий, которые могут быть использованы для деструктивного влияния как в технической, так и в психологической сфере.

Современная стратегия применения информационного оружия основана на модели «пяти колец» Вардена. Под пятью «центрами тяжести» в данном случае понимается руководство страны и система государственного управления, производство, транспортная сеть, население и вооруженные силы. Применять информационное оружие возможно против всех элементов этой модели. При этом максимальная эффективность его использования достигается против индустриально развитого и географически сконцентрированного противника [13].

Информационному оружию присущи следующие качественные характеристики, которыми оно отличается от других видов оружия [370]:

- универсальность – его применение не зависит от климатических и географических условий, времени суток, сезонов года и т.п.;
- скрытость – для его применения не требуется проводить мобилизацию, создавать большие группировки войск, в то же время его действие незаметно, а по воздействию сопоставимо с оружием массового поражения;
- внезапность применения – не требуется его длительная подготовка;
- экономическая эффективность – разработка информационного оружия и его применение требует существенно меньших затрат по сравнению с другими видами оружия;
- масштабность применения как для решения задач стратегического, так и тактического уровня;
- эффект «цепной реакции» – воздействие информационного оружия на отдельный элемент информационной системы информационного ресурса может привести к выводу из

строя других элементов системы, а затем и системы в целом;

- сложность осуществления контроля за созданием и испытанием информационного оружия – его разработку, а в ряде случаев и сам факт применения можно надежно скрыть от разведки противника.

При этом темпы совершенствования информационного оружия (как, впрочем, и любого вида атакующего вооружения) превышают темпы развития технологий защиты и противодействия ему [131].

4.6.2.2. Общая классификация информационного оружия

В соответствии со сферой своего применения информационное оружие подразделяется на [13]:

- информационно-техническое оружие;
- информационно-психологическое оружие.

В соответствии со своим целевым назначением информационное оружие подразделяется на два типа [13]:

- оборонительное информационное оружие;
- наступательное информационное оружие.

Оборонительное информационное оружие решает задачи обороны в информационной войне и включает системы многоуровневой компьютерной безопасности и различные системы активного противодействия информационно-психологическому оружию противника. Таким образом, в состав оборонительной составляющей информационного оружия входят средства противодействия и нейтрализации наступательного информационного оружия противника [13].

Наступательное информационное оружие решает задачи воздействия на систему принятия решения противником путем поражения наиболее критичных из входящих в нее компонентов (как в технической, так и психологической сферах) [13].

Рассмотрим наступательное информационное оружие более подробно.

Исходя из имеющихся определений информационного оружия, анализа опыта его применения в войнах и вооруженных конфликтах новейшего исторического периода, информации о направлениях зарубежных исследований и разработок в данной предметной области, опубликованной в открытых источниках, можно выделить следующие

наиболее распространенные средства наступательного информационного оружия [13]:

- средства воздействия на компоненты радиоэлектронного оборудования и системы их энергообеспечения для временного или необратимого вывода из строя РЭС или их отдельных компонентов;
- средства воздействия на информационные ресурсы и аппаратно-программные средства АСУ или другие технические средства с целью вывода их из строя либо изменения алгоритма их функционирования;
- средства воздействия на процесс передачи информации, предназначенные для полного прекращения либо дезорганизации функционирования подсистем обмена информацией за счет воздействия на среду распространения сигналов и алгоритмы функционирования;
- средства дезинформации и пропаганды для внесения изменений в информацию, циркулирующую в системах управления, создания виртуальной картины обстановки, отличной от действительности, деформации системы ценностей человека, нанесения ущерба духовно-нравственной жизни гражданского населения противоборствующей стороны;
- средства специальных психологических воздействий, предназначенные для воздействия на психику и подсознание человека в целях снижения и подавления его воли, временного вывода из строя, зомбирования.

Перечисленные средства наступательного информационного оружия, включающие различные виды воздействий, основаны на различных энергетических, химических и информационных технологиях (табл. 4.5) [13, 369]. При этом надо отметить, что представленные в таблице средства специальных психологических воздействий ряд специалистов относит не к информационно-психологическому, а к психологическому оружию. Это связанно с тем, что данные средства не манипулируют с информацией, а осуществляют прямое вмешательство в психику человека.

Таблица 4.5. Примеры некоторых видов информационного оружия, основанных на различных технологиях [13]

Вид информационного оружия	**Используемые средства**	**Тип технологии**
Средства воздействия на компоненты радиоэлектронного оборудования и системы их энергообеспечения	- Средства силового радиоэлектронного подавления; - сверхмощные генераторы СВЧ-излучения (гиротроны, рефлектные триоды, релятивистские магнетроны и др.); - взрывомагнитные генераторы (ВМГ), взрывные МГД-генераторы; - средства силового воздействия через электросеть; - средства вывода из строя электросетей	На основе энергетического воздействия
	- Программные средства вывода из строя оборудования (резонанс головок жестких дисков, выжигание мониторов и др.); - программные средства стирания перезаписываемой памяти; - программные средства воздействия на системы бесперебойного питания и др.	На основе информационных технологий
Средства воздействия на информационные ресурсы и аппаратно-программные средства АСУ	- Средства преодоления систем защиты информации; - средства проникновения в информационные системы (ИС) противника; - средства маскировки источников получения информации; - средства вывода из строя программного обеспечения (ПО) информационной системы;	На основе информационных технологий

Продолжение табл. 4.5

Вид информационного оружия	Используемые средства	Тип технологии
	- средства скрытого частичного изменения алгоритма функционировапия ПО; - средства сбора данпых, циркулирующих в ИС противника; - средства доставки и внедрения определенных алгоритмов в конкретное место информационной системы; - средства воздействия на системы охраны объектов	
Средства воздействия на процесс передачи информации	- Средства РЭБ; - станции помех радиосвязи (в том числе, с элементами искусственного интеллекта); - забрасываемые передатчики помех одноразового использования;	На основе энергетического воздействия
	- средства воздействия на протоколы передачи данных систем связи и передачи данных; - средства воздействия на алгоритмы адресации и маршрутизации; - средства перехвата и нарушения прохождения информации в технических каналах ее передачи; - средства вызова перегрузки системы ложными запросами на установление связи.	На основе информационных технологий
Средства психологического. воздействия, дезинформации и пропаганды	- Воздействие посредством СМИ; средства пропаганды; средства создания или модификации виртуальной реальности; - средства имитации голосов операторов систем управления (например, систем УВД) и видеоизображения конкретных людей с их голосом (руководителей государств, лидеров партий и др.);	На основе информационных технологий

Продолжение табл. 4.5

Вид информационного оружия	Используемые средства	Тип технологии
	- средства модификации информации, хранимой в базах данных ИС противника; - средства ввода в ИС противника ложной информации и данных (целеуказания, мест доставки грузов и др.); - средства дезинформации охранных систем; - средства модификации данных навигационных систем, систем точного времени и др.	
Средства специальных психологических воздействий	Специальные генераторы излучения, воздействующего на психику человека.	На основе энергетического воздействия
	- Антидепрессанты; галлюциногены, наркотические вещества; - специально структурированные лекарственные средства	На основе химического воздействия
	- Специальная видеографическая и телевизионная информация; - средства создания виртуальной реальности, подавляющей волю человека и вызывающей страх; - зомбирование и нейролингвистическое программирование (НЛП).	На основе информационных технологий

Подробности о различиях видов психологического и информационно-психологического оружия представлены в разделе 4.6.4 «Психологическое и информационно-психологическое оружие».

4.6.3. Информационно-техническое оружие

4.6.3.1. Определение и классификация информационно-технического оружия

Особенностью информационно-технического оружия является его ориентированность на поражение аппаратно-программных средств систем передачи, хранения и обработки информации, функционирую-

щих в технической сфере информационного пространства (в киберпространстве).

Взяв за основу определения информационного оружия, ориентированного на применение в технической сфере, представленные в работах [2, 220, 269, 292], можно дать следующее определение.

Информационно-техническое оружие – совокупность специально организованной информации, информационных технологий, способов и средств, позволяющих целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование систем обработки информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, а также другой инфраструктуры высокотехнологического обеспечения жизни общества и функционирования системы управления государством, применяемая в ходе информационной операции для достижения поставленных целей.

В соответствии с этим определением информационно-техническое оружие включает технические и программные средства, обеспечивающие несанкционированный доступ к базам данных, нарушение штатного режима функционирования аппаратно-программных средств, а также вывод из строя ключевых элементов информационной инфраструктуры отдельного государства или группы государств.

В соответствии с различными классификационными признаками и основаниями информационно-техническое оружие можно классифицировать следующим образом (рис. 4.36).

Информационно-техническое воздействие (ИТВ) – основной поражающий фактор информационно-технического оружия, представляющий собой воздействие либо на информационный ресурс, либо на информационную систему или на средства получения, передачи, обработки, хранения и воспроизведения информации в ее составе с целью вызвать заданные структурные и/или функциональные изменения.

Объекты информационно-технического воздействия – информация, ее свойства, связанные с информационной безопасностью, информационно-технические системы (системы связи и управления, телекоммуникационные системы, радиоэлектронные средства, компьютерные сети и т.д.), технические средства, компьютерные системы и информационно-вычислительные сети, а также другая инфраструктура

высокотехнологического обеспечения жизни общества и функционирования системы управления государством.

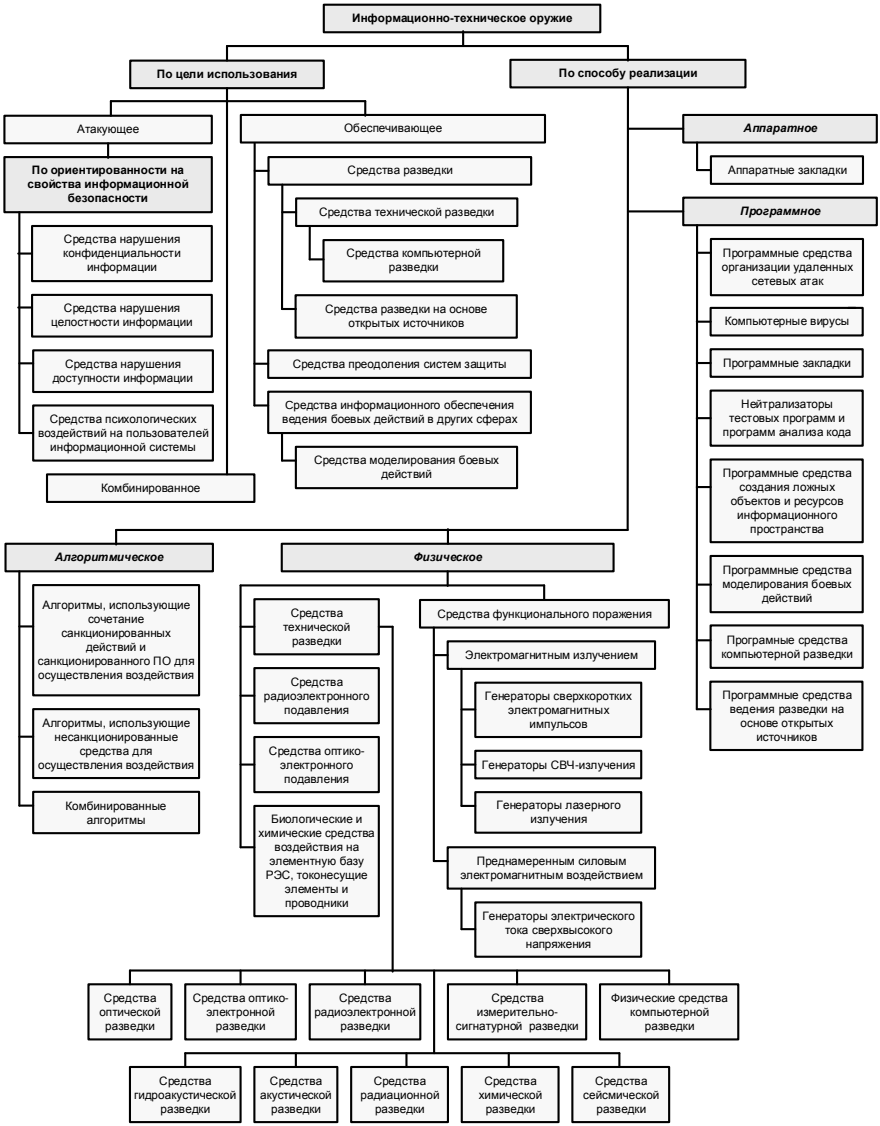


Рис. 4.36. Классификация информационно-технического оружия [220, 462]

Классификация информационно-технических воздействий (рис. 4.37) в общем случае по смыслу совпадает с классификацией информационно-технического оружия, за исключением оборонительных воздействий. Традиционно средства оборонительных информационно-технических воздействий не рассматриваются в качестве оборонительного информационно-технического оружия, вместе с тем они существуют и играют одну из ведущих ролей в информационном противоборстве при организации защиты собственной стороны.

Оборонительные информационно-технические воздействия ориентированы на противодействие информационно-техническому оружию противника. Их можно классифицировать следующим образом:

- *выявляющие* – воздействия, ориентированные на выявление как самого факта, так и последовательности атакующих воздействий противника;
- *блокирующие* – воздействия, ориентированные на блокировку атакующих воздействий противника;
- *контратакующие* – воздействия на информацию, информационные ресурсы и информационную инфраструктуру противника с целью срыва его атакующих воздействий;
- *отвлекающие* – воздействия, ориентированные на дезинформацию противника, отвлечение его атакующих или обеспечивающих воздействий на незначащие или ложные объекты;
- *противодействие обеспечивающим воздействиям противника* – способы маскировки, обеспечения безопасности, повышения скрытности реальных режимов функционирования, а также мониторинга каналов утечки в отношении собственных информационных систем.

Средства информационно-технического воздействия – средства, используемые в качестве информационно-технического оружия или для защиты от него [2].

Необходимо отметить, что классификация атакующих и обеспечивающих информационно-технических воздействии в общем виде совпадает с классификацией соответствующих видов информационно-технического оружия. Однако необходимость защиты от атакующих и обеспечивающих информационно-технических воздействий противника позволяет дополнительно выделить, оборонительные средства информационно-технического воздействия.

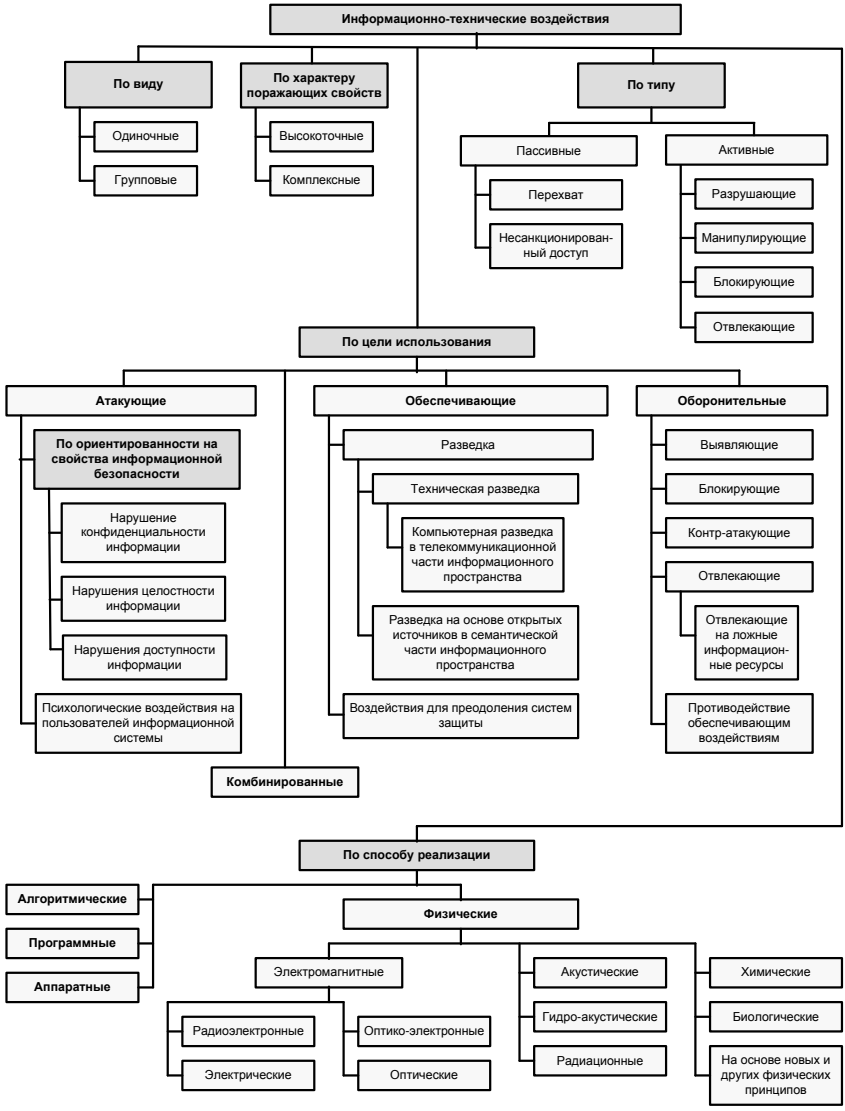


Рис. 4.37. Классификация информационно-технических воздействий [462]

К оборонительным средствам информационно-технического воздействия можно отнести:

- средства антивирусной защиты;
- системы обнаружения и предотвращения вторжений;

- средства криптографической защиты;
- стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
- средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей;
- средства тестирования программного обеспечения и анализа кода для выявления программных закладок и недекларируемых возможностей;
- средства создания ложных объектов и ресурсов в информационном пространстве.

Применительно к новейшим разработкам атакующего информационно-технического оружия наибольшее развитие получили средства специального программно-математического (алгоритмического) воздействия, которые объединяют возможности алгоритмического и программного информационно-технического оружия.

Средства специального программно-математического воздействия – некоторая программа (набор инструкций) или комплекс программ, способных выполнить любое подмножество перечисленных ниже функций [2, 372]:

- скрывать признаки своего присутствия в программно-аппаратной среде информационной системы;
- обладать способностью к самокопированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать) код программ в памяти информационной системы;
- сохранять фрагменты информации из памяти информационной системы в некоторой области внешней памяти прямого доступа (локальной и удаленной);
- искажать, блокировать и/или подменять выводимый во внешнюю память или канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных;
- подавлять информационный обмен в телекоммуникационных сетях, фальсифицировать информацию, передаваемую по каналам управления;

- противодействовать работе тестовых программ и систем защиты информационных ресурсов.

Отдельно необходимо отметить следующее. К средствам технической разведки, представленным в данной классификации, относятся те средства, которые добывают информацию об атакующих средствах информационно-технического оружия противника и способах его применения, т.е. являются средствами обеспечивающего информационного оружия. Средства технической разведки могут оказывать воздействие на объекты противника как путем пассивных действий, направленных на добывание информации, что, как правило, связано с нарушением ее конфиденциальности, так и путем активных действий (атак), направленных на создание условий, благоприятствующих добыванию информации.

Классификация средств информационно-технических воздействий представлены на рис. 4.38.

Рассмотрим более подробно наиболее распространенные средства информационно-технического воздействия из представленных на рис. 4.38. Основное внимание уделим следующим средствам информационно-технического воздействия:

- удаленные сетевые атаки;
- компьютерные вирусы;
- программные закладки;
- аппаратные закладки;
- нейтрализаторы тестовых программ и программ анализа кода;
- средства создания ложных объектов информационного пространства;
- средства моделирования боевых действий;
- средства технической разведки (средства компьютерной разведки рассмотрены отдельно);
- средства разведки по отрытым источникам в глобальном информационном пространстве.

4.6.3.2. Удаленные сетевые атаки

С учетом определения и классификации удаленных воздействий на распределенные вычислительные системы, представленные в работе [373], можно дать следующее определение.

Удаленная сетевая атака – это разрушающее или дестабилизирующее информационно-техническое воздействие, осуществляемое

по каналам связи удаленным относительно атакуемой системы субъектом и характерное для структурно- и пространственно-распределенных информационных систем.

Рис 4.38. Классификация средств информационно-технического воздействия [462]

Удаленные сетевые атаки становятся возможными благодаря уязвимостям в существующих протоколах обмена данными и в подсистемах защиты распределенных информационных систем. При этом к основным уязвимостям информационных систем, которые позволяют проводить против них успешные удаленные сетевые атаки, относятся [374, 373]:

- открытость информационной системы, свободный доступ к информации об организации сетевого взаимодействия, способах защиты, применяемых в системе;
- наличие ошибок в операционных системах, прикладном программном обеспечении, протоколах сетевого обмена;
- разнородность используемых версий программного обеспечения и операционных систем;
- сложность организации защиты межсетевого взаимодействия;
- ошибки конфигурирования систем и средств защиты;
- неправильное или ошибочное администрирование систем;
- несвоевременное отслеживание и выполнение рекомендаций специалистов по защите и анализу случаев вторжения для ликвидации эксплойтов и ошибок в программном обеспечении;
- «экономия» на средствах и системах обеспечения безопасности или игнорирование их.

В соответствии с различными основаниями удаленные сетевые атаки можно классифицировать следующим образом (рис. 4.39) [374, 373, 462].

В связи с тем, что удаленные сетевые атаки совместно с воздействием вирусных средств составляют подавляющее большинство всех информационно-технических воздействий, рассмотрим их более подробно. Основные способы и средства информационно-технического воздействия, которые можно отнести к удаленным сетевым атакам, представлены на рис. 4.40 по материалам [373, 374, 462]. Рассмотрим самые распространенные удаленные сетевые атаки.

Анализ сетевого трафика. Основной особенностью сетевой информационной системы является то, что ее объекты распределены в пространстве и связь между ними осуществляется по сетевым соединениям. Таким образом, сообщения и данные, пересылаемые между объектами информационной системы, передаются по каналам связи в виде пакетов. Эта особенность привела к появлению специфичного для сетевой информационной системы типового удаленного воздей-

ствия, заключающегося в прослушивании канала связи. Данное воздействие называется *анализом сетевого трафика*.

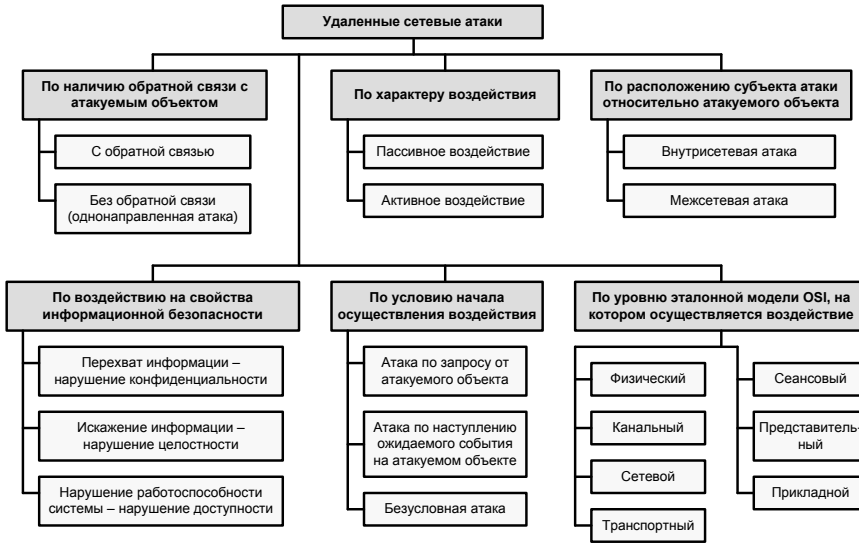


Рис. 4.39. Классификация удаленных сетевых атак [462]

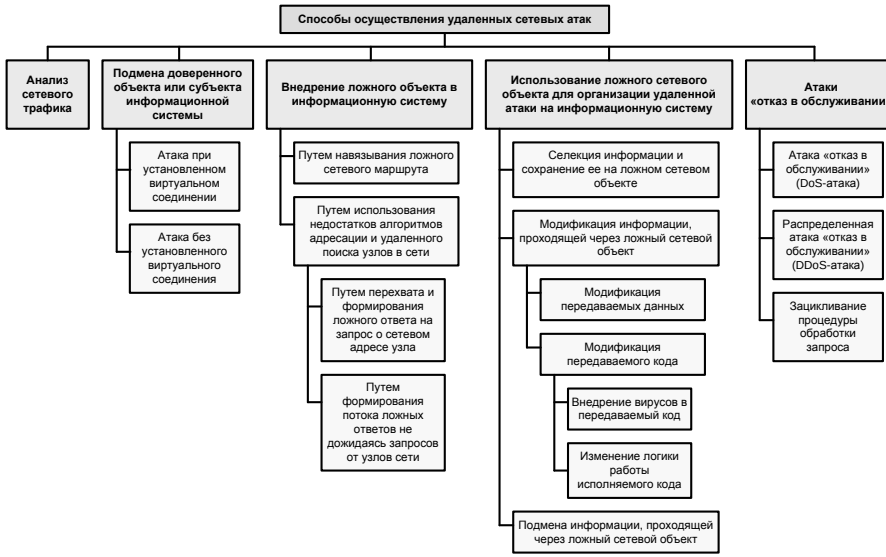


Рис. 4.40. Классификация способов осуществления удаленных сетевых атак [462]

Атака «отказ в обслуживании». В общем случае в сетевой информационной системе каждый ее субъект должен иметь возможность подключиться к любому объекту системы и получить в соответствии со своими правами удаленный доступ к его информационным ресурсам. Обычно в сетевых информационных системах возможность предоставления удаленного доступа реализуется следующим образом – на объекте системы запускается на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т.п.), предоставляющих удаленный доступ к ресурсам данного объекта. В случае получения запроса на соединение сервер должен по возможности передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет. Очевидно, что сервер способен отвечать лишь на ограниченное число запросов. Эти ограничения зависят от параметров информационной системы, пропускной способности ее сети и быстродействия ЭВМ на которых сервер функционирует. Атака «отказ в обслуживании» направлена на блокировку доступа к объекту путем исчерпания его ресурсов за счет отправки большого числа запросов к нему.

Различают три типа этих удаленных атак:

- *Отказ в обслуживании* (DoS-атака) – передача с одного адреса такого количества запросов на атакуемый объект, которое позволит передать пропускная способность канала связи. Если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) системы, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная блокировка объекта из-за невозможности системы заниматься ничем другим, кроме обработки запросов.
- *Распределенная атака «отказ в обслуживании»* (DDoS-атака) – передача с нескольких объектов системы на другой атакуемый объект бесконечного числа запросов на подключение от имени этих или других объектов. Результатом применения этой удаленной атаки является нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов сетевой информационной системы.
- *Зацикливание процедуры обработки запроса* – передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной

системе возможно переполнение буфера с последующим зависанием системы.

Наиболее распространенные способы осуществления атаки «отказ в обслуживании» представлены на рис. 4.41 [462].

Рис. 4.41. Способы осуществления атаки «отказ в обслуживании» [462]

В настоящее время атаки типа «отказ в обслуживании» являются не только наиболее распространенными, но и наиболее опасными воздействиями. Так, в ноябре 2002 г. была проведена глобальная DDoS-атака на корневые DNS-серверы с целью полного блокирования общедоступного сегмента сети Интернет. В результате этой атаки злоумышленники смогли вывести из строя 7 из 13 корневых DNS-серверов [375].

4.6.3.3. Компьютерные вирусы

Несмотря на долгую историю компьютерной вирусологии, использование вирусов в качестве боевых средств информационно-технического воздействия начато сравнительно недавно. К первому случаю относится использование в 2010 г. вируса Stuxnet с целью сры-

ва ядерной программы Ирана за счет инфицирования АСУ технологическим процессом обогащения урана [376].

Классификация компьютерных вирусов представлена на рис. 4.42 по материалам работ [374, 462].

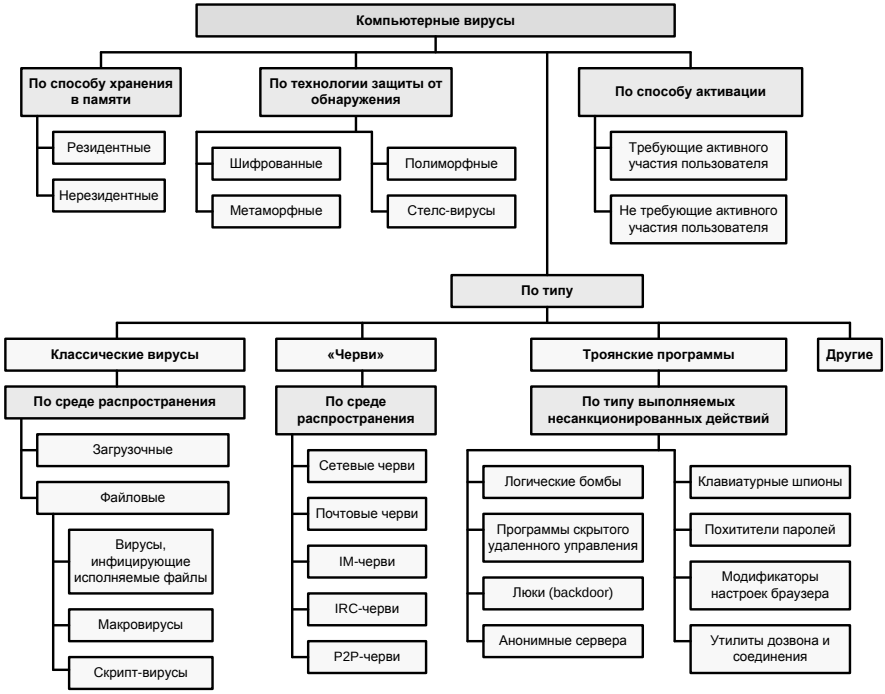


Рис. 4.42. Классификация компьютерных вирусов [374, 462]

В отличие от своих «непрофессиональных собратьев» средства информационно-технического воздействия на основе вирусов обладают следующими особенностями функционирования [376]:

- избирательность цели и действий;
- использование уязвимостей, в том числе уязвимостей нулевого дня, закладок и скрытых каналов;
- маскировка, скрытность, криптозащита, самоликвидация;
- широкая функциональность в плане решения целевых задач;
- гибкая система саморазмножения;
- инфраструктурная поддержка, обновление и управление;
- масштабируемость, наличие СУБД атак;

- высокое качество кода и возможности обработки некорректных ситуаций.

Особенностью современных боевых вирусов является то, что они, как правило, являются комплексными продуктами и состоят из различных модулей, которые относятся к различным типам и которые ориентированы на решение конкретной задачи (модули типа «классический вирус» – для саморазмножения в информационной системе, модули типа «червь» – для распространения по сети, модуль типа «троян» – для организации дестабилизирующего воздействия).

Наиболее известными к настоящему времени средствами информационно-технических воздействий на основе вирусов являются Stuxnet, Flame (известный также как Skywiper или Flamer), Duqu, Regin, Gauss, MiniFlame, MiniDuqu, Sputnik [376, 378, 379, 462].

Необходимо отметить, что использование вирусных средств не только позволяет решать целевые задачи вооруженным силам и органам безопасности, но и требует корректности в их конфигурировании и использовании.

Как показано в работе [380], использование вирусного программного обеспечения для целей государственной безопасности, которая не обладает широким спектром защиты собственных каналов управления, может привести к утрате контроля над этими программами и бот-сетями на их основе. Кроме того, при использовании таких средств необходимо тщательно продумывать тактику действий вируса и допустимый уровень вреда, который он может причинять инфицируемой системе.

Еще одним проблемным вопросом при использовании вирусных средств является контроль над профессиональными способами их создания и применения со стороны государственных служб.

Низкая стоимость разработки, наличие большого количества документации по принципам функционирования критической информационной инфраструктуры делает вероятным разработку и использование вирусных средств со стороны иррегулярных воинских формирований, и террористических групп и организованной преступности для проведения акций информационной войны.

Как отмечается в работе [381], в настоящее время уже имеются профессиональные платформы для создания вирусных средств, разработка которых финансируется международной организованной преступностью.

Таким образом, уже сейчас наблюдается процесс, в результате которого иррегулярные воинские формирования, террористические

группы и организованная преступность могут перейти от использования вирусов в качестве средств шпионажа и хищения финансовой информации к созданию этих вирусных средств на основе профессиональных технологий, а в дальнейшем – их применения, для организации высокоэффективных терактов, ориентированных на информационные системы государственного и военного управления, энергосети, транспортную инфраструктуру и особо опасные промышленные производства.

4.6.3.4. Программные закладки

Программная закладка – скрытно внедренная в защищенную информационную систему программа либо намеренно измененный фрагмент программы, которая позволяет осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты [382]. При этом в большинстве случаев закладка внедряется самим разработчиком программного обеспечения для реализации в информационной системе некоторых сервисных или недекларируемых функций.

Программные закладки, получая несанкционированный доступ к данным в памяти информационной системы, перехватывают их. После перехвата эти данные копируются и сохраняются в специально созданных разделах памяти или передаются по сети. Программные закладки, подобно вирусам, могут искажать или уничтожать данные, но в отличие от вирусов деструктивное действие таких программ, как правило, более выборочно и направлено на конкретные данные. Довольно часто программные закладки выполняют роль перехватчиков паролей, сетевого трафика, а также служат в качестве скрытых интерфейсов для входа в систему. Однако в отличие от вирусов программные закладки не обладают способностью к саморазмножению, они встраиваются в ассоциированное с ними программное обеспечение и латентно функционируют вместе с ним. При этом особенностью закладок, внедренных на стадии разработки программного обеспечения, является то, что они становятся фактически неотделимы от прикладных или системных программ информационной системы [377].

Классификация программных закладок приведена на рис. 4.43.

Часто для программных закладок используют синонимы из терминологии компьютерных вирусов: «логическая бомба», «логический люк», «троянский конь». Однако такая семантическая связь не совсем верна. Обычно понятие программной закладки связано с разра-

боткой программного обеспечения, а именно – с процессом написания исходных текстов программ, в которых создаются дополнительные недекларируемые или сервисные функции. Следовательно, под закладкой, как правило, понимается внутренний объект защищенной системы. Однако в редких случаях закладка может быть и внешним объектом по отношению к защищенной системе [377].

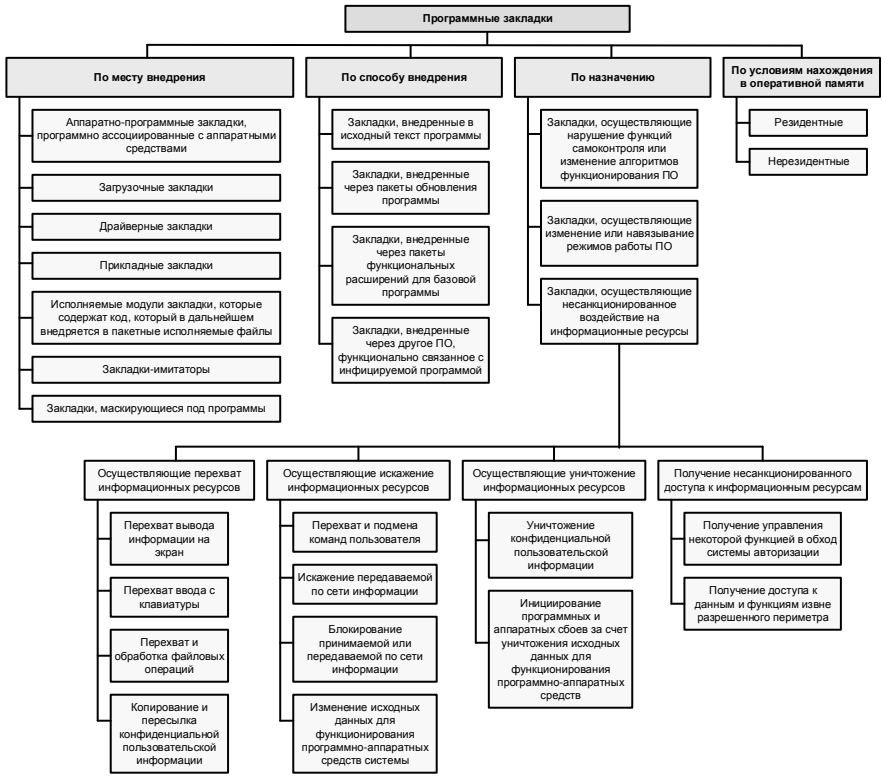


Рис. 4.43. Классификация программных закладок [462]

Как и вирус, программная закладка должна скрывать свое присутствие в программной среде информационной системы. Однако программные закладки невозможно обнаружить при помощи стандартных антивирусных средств, их выявление возможно только специальными тестовыми программами, выявляющими аномальное поведение и недекларируемые возможности программного обеспечения. В связи с этим средства маскировки программных закладок преимущественно ориентированы на противодействие отладчикам программ, анализато-

рам кода и дисассемблерам. В качестве одного из широко применяемых способов маскировки является обфускация («запутывание») программ, в которые внедрена закладка [377].

Подавляющая часть программных закладок устанавливается самими производителями программного обеспечения для несанкционированного сбора данных о действиях пользователей программ, обрабатываемых и хранящихся данных, блокировании определенных действий пользователя, а также по запросам органов государственной безопасности.

В связи с широким распространением в мире электронных устройств на основе закрытых операционных систем, произведенных в США, становится особенно актуальным выявление и блокирование программных закладок в ЭВМ, использующихся в службах государственного и военного управления, а также в различного рода персональных устройствах (телефонах, планшетах, смартфонах) должностных лиц.

Как показано в работе [384], по итогам сертификации иностранного программного обеспечения, в нем массово встречаются программные закладки, маскируемые под отладочные средства (встроенные учетные записи и мастер-пароли, а также средства удаленного управления). Около 70% от общего числа выявленных уязвимостей программного обеспечения являются именно такими.

Закладки в программном обеспечении широко используются в браузерах, операционных системах, программах смартфонов и планшетов. Отдельные программные закладки в указанных объектах рассмотрены в работах [385, 386, 387, 388, 389, 390]. Необходимо отметить, что в настоящее время подавляющее число закладок предназначено для шпионажа в пользу производителя программного обеспечения, а также сотрудничающих с ними служб государственной безопасности. Кроме того, подобные закладки смогут применяться и для активного воздействия на пользователя, а также управляемые программами технологические процессы. Например, за счет закладок можно реализовать средства психологического воздействия на пользователей информационной системы.

4.6.3.5. Аппаратные закладки

Аппаратная закладка – устройство в электронной схеме, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу аппаратных средств информационной системы. Ре-

зультатом работы аппаратной закладки может быть как полное выведение системы из строя, так и нарушение ее нормального функционирования, например несанкционированный доступ к информации, ее изменение или блокирование [391].

Аппаратной закладкой также может называться отдельная микросхема, несанкционированно подключаемая к атакуемой системе для достижения тех же целей [391].

Классификация аппаратных закладок приведена на рис. 4.44 по материалам работ [392, 462].

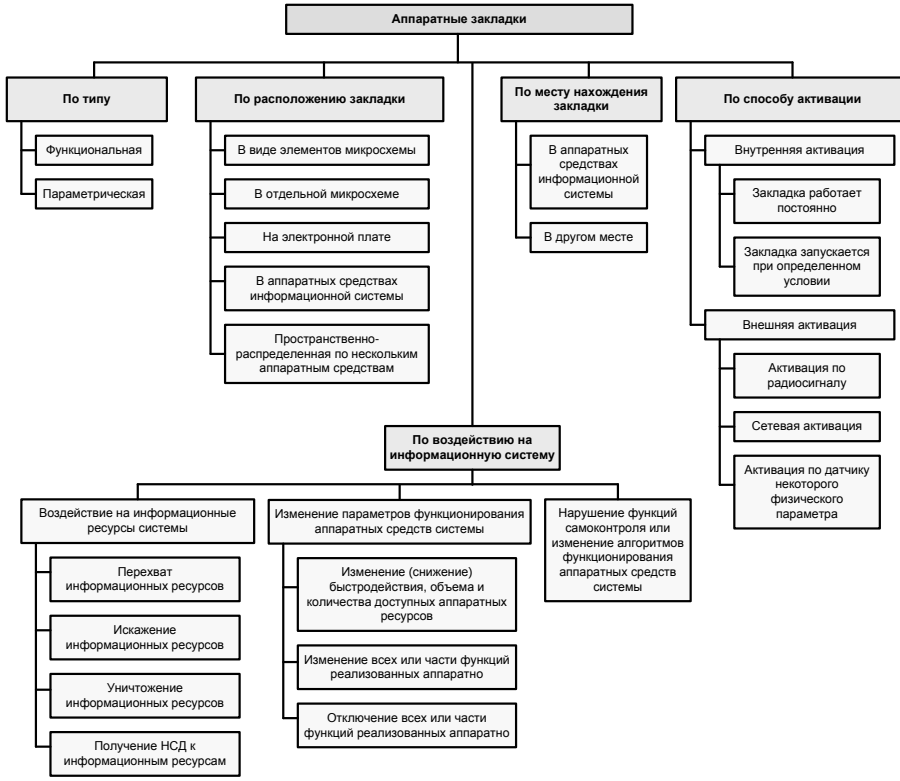


Рис. 4.44. Классификация аппаратных закладок [392, 462]

Схематическая сложность современного микроэлектронного оборудования, тенденции по миниатюризации его элементов ведут к тому, что производители оборудования могут бескомпроматно и практически неограниченно наращивать функциональные возможности аппаратных закладок, а при подключении устройств к глобальной сети

осуществлять обновление алгоритма их функционирования, а также условий срабатывания.

Достижения в области разработки и внедрения аппаратных закладок напрямую связаны с научным заделом в области микроэлектроники, а также с мощностями электронной промышленности. В настоящее время такие страны, как США, Китай, Япония, в которых функционируют развитые производственные комплексы в области микроэлектронной и микропроцессорной техники, имеют потенциальную возможность встраивания аппаратных закладок в производимые ими на экспорт микроэлектронные компоненты. В дальнейшем это позволит контролировать функционирование подавляющей части АСУ технологическими и критическими процессами, а также средств радиоэлектроники в других странах. При этом в отношении этих стран может быть реализован сценарий мгновенного вывода из строя их критической инфраструктуры за счет одновременного отключения входящих в ее состав микроэлектронных компонентов.

В связи с этим можно выделить следующие риски использования импортных микроэлектронных компонентов при производстве систем управления войсками и оружием [393]:

- встроенная технологическая и схемотехническая избыточность микроэлектронных компонентов, превышающая необходимый уровень для предоставления сервисов по прямому назначению, позволяет внедрять в них недекларированные функции, в том числе и враждебного характера;
- отсутствие технической документации на топологии микросхем и логику функционирования не позволяет в полной мере провести эффективный технический контроль наличия закладок;
- отсутствие гарантированно подтвержденной надежности микроэлектронных компонентов, а также их стойкости к воздействию электромагнитного оружия позволит противнику эффективно применять это оружие против систем управления войсками и оружием. При этом противник может создать электромагнитную обстановку, гарантирующую выход из строя им же произведенных микроэлектронных компонентов.

Образцом использования аппаратных закладок является обнародованная Э. Сноуденом информация о закладках АНБ [389, 390, 394], использующихся для несанкционированного сбора данных в интересах разведывательных служб США. Практически все закладки бы-

ли реализованы на аппаратном или аппаратно-программном уровне (при внедрении в перепрограммируемую память BIOS). Такое внедрение позволяет обеспечить функционирование закладки даже в случае обновления прошивки устройства или переустановки операционной системы, а, кроме того, такая закладка слабо поддается обнаружению [390].

Другим ярким примером использования аппаратной закладки в военном конфликте является факт отключения системы иракской ПВО в Персидском заливе в 1991 г. Тогда при проведении операции «Буря в пустыне» система ПВО Ирака оказалась заблокированной по неизвестной причине. Несмотря на отсутствие исчерпывающей информации, высказывалось предположение, что ЭВМ, входящие в состав комплекса технических средств системы ПВО, закупленные Ираком у Франции, содержали специальные управляемые электронные закладки, блокировавшие работу вычислительных систем по внешней команде [377].

Такое действие закладки актуализирует вопросы обеспечения доверенной аппаратной среды при разработке электронных систем для критической инфраструктуры государства. Так как опыт локальных военных конфликтов показывает, что на первых этапах активных военных действий системы управления войсками и оружием, построенные на импортных компонентах, будут выводиться из строя в первую очередь.

При этом в настоящее время фиксируются факты поставки в Вооруженные Силы России вычислительной техники, которая фактически произведена иностранным изготовителем, снабжена разнообразными аппаратными закладками (например, одновременно в BIOS-е и сетевой карте компьютера), которая, однако пройдя перемаркировку и установку отечественного программного обеспечения считается де-юре отечественного производства. При этом такие отечественные производители, организующие подобные поставки, как правило, не имеют персонала должной квалификации для обнаружения и дезактивации встроенных в импортную технику аппаратных закладок, чем создают угрозу обороноспособности страны [395].

4.6.3.6. Нейтрализаторы тестовых программ и программ анализа кода

Одним из способов противодействия угрозам программных закладок является проверка программ, используемых в информацион-

ных системах управления критической инфраструктуры в процессе сертификационных испытаний и тематических исследований по требованиям безопасности [384, 397].

Сертификационные испытания и тематические исследования проводятся путем [384, 398]:

- функционального тестирования программного обеспечения на соответствие нормативным и методическим документам или документации;
- структурного (статического и динамического) анализа программного обеспечения на отсутствие недекларированных возможностей.

Рассмотрим особенности указанных подходов.

Функциональное тестирование программ касается проверки задекларированных механизмов безопасности, т.е. проверяется сам факт их работы, без глубокого анализа обеспечиваемого ими уровня защищенности. Однако, используя личный опыт, квалифицированные эксперты способны построить тесты, позволяющие выявлять некоторые специфические ошибки безопасности проектирования, реализации, конфигураций, прототипов, интерфейсов и т.д. [384, 397].

При структурном анализе проводится главным образом проверка полноты/избыточности кода, статический и динамический анализ, который заключается в выполнении декомпозиции программной системы, последующем формировании и контроле условной части маршрутов передачи управления в программе, а также потока данных в трассе [384].

При этом эксперты в области тестирования могут использовать дополнительные методы и приемы проверки кода, например: инспекции кода, использование статических анализаторов, изучение бюллетеней безопасности, организация стресс-тестирования и др.

Сложность и размер современных программ таков, что для проведения сертификации используются специальные тестовые программы и анализаторы кода. Как правило, они ведут динамический анализ программного обеспечения, пока оно выполняется на реальном или виртуальном процессоре, фиксируя трассу управления, и формируемые потоки данных.

При использовании атакующих средств, например таких, как программная закладка, требуется обеспечить ее маскировку. В этом случае применяются обеспечивающие средства – нейтрализаторы тестовых программ и программ анализа кода. Цель данных средств –

затруднить анализ трассы исполнения программы и скрыть факт наличия закладки.

Средства нейтрализации тестовых программ и программ анализа кода используются либо на этапе компиляции исходного текста в машинный код, либо уже в процессе выполнения программы.

К основным способам нейтрализации тестовых программ относятся (рис. 4.45) [398, 399, 400, 462]:

- обфускация (запутывание) кода;
- упаковка и шифрование кода;
- определение факта применения тестовых программ и противодействие отладке;
- полиморфизм (самомодифицирующийся код).

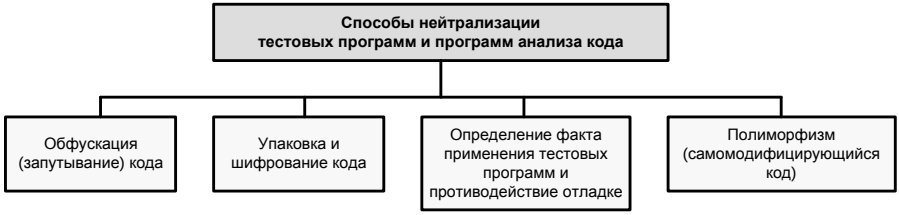


Рис. 4.45. Классификация способов нейтрализации тестовых программ

4.6.3.7. Средства создания ложных объектов информационного пространства

При защите информационных систем большое внимание уделяется вопросам обнаружения и нейтрализации уязвимостей входящего в их состав программного обеспечения. В настоящее время все основные способы решения данной задачи основываются на применении стратегии запрета. Для этого в ручном или автоматизированном режиме проводится поиск уязвимостей ПО информационной системы, информация о которых имеется в открытых или закрытых базах данных. После обнаружения уязвимость нейтрализуется либо за счет обновления ПО, либо за счет использования средств защиты информации, таких как межсетевые экраны, системы обнаружения вторжений, средства антивирусной защиты и т.д., которые делают невозможной эксплуатацию данной уязвимости для реализации несанкционированного доступа [402].

Однако, как показывает практика, такая стратегия оказывается неэффективной против уязвимостей «нулевого дня». Это связано с

тем, что между выпуском ПО и появлением информации об уязвимости, а тем более устранением ее разработчиками, в большинстве случаев проходит большое количество времени, в течение которого система оказывается уязвимой. Несмотря на то, что правильно настроенные средства защиты информации делают эксплуатацию некоторых из таких уязвимостей невозможной, всегда остается вероятность наличия неустраненных уязвимостей, а также уязвимостей в ПО самих средств защиты [402].

В связи с этим в настоящее время актуальным становится применение «стратегии обмана» или отвлечения атаки информационным оружием на ложный информационный ресурс. Как показали исследования [403], реализуя «стратегию обмана» атакующей системы и отвлекая атаку на ложный информационный ресурс, можно не только не позволить получить несанкционированный доступ к защищаемой информации, но и провести ответную информационную атаку, дезинформировав атакующую сторону. Кроме того, в период отвлечения атаки на ложные информационные ресурсы возможен сбор данных об атакующей стороне для компрометации последней.

В общем случае можно выделить два типа ложных ресурсов, ориентированных на различные сферы информационного противоборства:

- ложные объекты и ресурсы в семантической части информационного пространства (например, дезинформация или заведомо ложная информация, размещаемая в СМИ и в сети Интернет);
- ложные объекты и ресурсы в телекоммуникационной части информационного пространства (например, ложные сети, узлы, БД и т.д.).

Ложные объекты и ресурсы, размещаемые в семантической части информационного пространства, ориентированы на ведение информационного противоборства в психологической сфере и направлены, главным образом, на обеспечение информационно-психологических операций.

Ложные объекты и ресурсы в телекоммуникационной части информационного пространства ориентированы на ведение информационного противоборства в технической сфере. Они предназначены для обмана и отвлечения на себя атакующих информационно-технических воздействий.

К ложным объектам и ресурсам в телекоммуникационной части информационного пространства, на которые возможно эффективное отвлечение проводимых противником атак, можно отнести:

- узлы телекоммуникационных сетей;
- вычислительные и информационно-управляющие системы;
- операционные системы;
- прикладное программное обеспечение;
- базы данных и системы управления ими;
- программы управления контентом сайтов, новостных агрегаторов, страниц во внутренней сети или в сети Интернет.

Рис. 4.46. Классификация ложных объектов информационного пространства

В качестве средств создания и использования ложных объектов в телекоммуникационной части информационного пространства можно рассматривать программное обеспечение на основе технологий виртуализации. Такие программные средства виртуализации, как VMware ESX/ESXi, Microsoft Hyper-V, Citrix Xen Server и др., позволят создать виртуальную инфраструктуру, наполнить ее ложными объектами, содержащими дезинформацию, и впоследствии управлять такой системой [402].

4.6.3.8. Средства моделирования боевых действий

Анализ вооруженных конфликтов свидетельствует о том, что успех сопутствует стороне, проявляющей большую активность и инициативу, эффективно управляющей подчиненными силами и сред-

ствами. В свою очередь эффективность управления во многом зависит от решений, принимаемых командирами. Эволюционный путь развития автоматизированных средств управления войсками и оружием привел к разработке и принятию концепции создания системы моделирования военных действий [404].

В связи с развитием современных суперкомпьютерных технологий уже в ближайшее время можно ожидать появления достаточных вычислительных возможностей для моделирования боевых действий с приемлемой степенью адекватности. Средства такого моделирования основаны на манипулировании информацией о составе, формах и способах действий войск (сил). Использование средств моделирования боевых действий позволит точно выбрать оптимальную стратегию действий при заданном составе группировки своих сил и средств, выбрать оптимальную траекторию развития противоборства с учетом вероятных действий противника и тем самым обеспечить подавляющее ассиметричное информационное превосходство над противником при условии отсутствия у него подобных средств. При противоборстве двух сторон, обладающих подобными средствами, может создаться ситуация, при которой конфликт закончится еще в угрожаемый период. Когда сторона, которая по результатам моделирования не сможет найти выигрышной стратегии, самостоятельно признает себя проигравшей.

Вышеуказанные факты, а именно – использование средств моделирования боевых действий для достижения информационного превосходства над противником за счет обработки информации, позволяет отнести данные средства к информационному оружию.

Интенсивные попытки использования математических моделей для военных целей в США предпринимались, начиная с 50-х гг. прошлого столетия. Однако практическое использование моделей и полученных на основе моделирования результатов было незначительным. Начиная с 90-х гг. ведутся масштабные проекты внедрения моделирования в повседневную деятельность с охватом всех видов ВС США. Были созданы органы, обеспечивающие централизованное руководство разработкой и применением моделирования МО США, координацию соответствующих работ как между видами ВС, так и в рамках какого-либо одного из направлений применения моделирования. Совершенствование средств имитации и моделирования в этот период ведется по пути интеграции моделей между собой и с состоящими на вооружении ВВТ, а также в направлении увеличения числа военнослужащих, выполняющих учебно-боевые задачи с использованием

тренажерных комплексов. Значительно возросло количество учений различного уровня с использованием автоматизированных систем моделирования боевой обстановки. С середины 90-х гг. командование американских ВС начало использовать новую форму проведения маневров – компьютерные учения с ограниченным привлечением войск и штатного ВВТ [405].

С начала 2000-х гг. Пентагон при формировании военно-технической политики включил средства имитации и моделирования боевых действий в число приоритетных технологий. В свою очередь военное руководство США выделяет средства имитации и моделирования боевых действий в число приоритетных технологий при формировании военно-технической политики. Высокая динамика развития вычислительной техники, технологий программирования, системотехнических основ моделирования различных реальных процессов вызвала огромный прорыв США в области разработки моделей и имитационных систем [405, 406].

В настоящее время в МО США действует классификация определяющая назначение модели, объекты и процессы, метод моделирования (рис. 4.47) [405, 462].

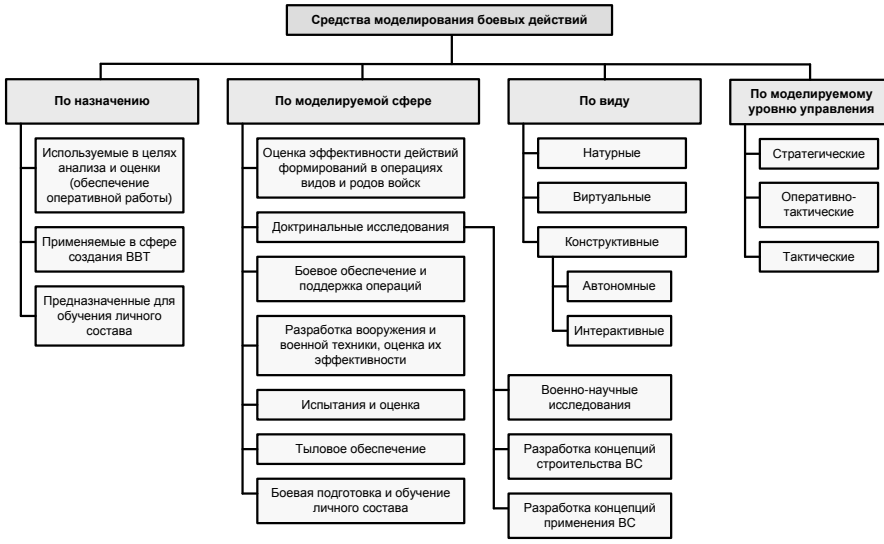


Рис. 4.47. Классификация средств моделирования боевых действий [405, 462]

В последнее время в ряде официальных документов военного ведомства предлагается более подробное подразделение моделей с выделением семи функциональных сфер моделирования таких как [405]:

- оценка эффективности действий формирований в самостоятельных, совместных и объединенных операциях видов и родов сил;
- доктринальные исследования (военно-научные исследования и разработка концепций в области строительства ВС и их боевого применения);
- боевое обеспечение или поддержка операций (разведка, РЭБ и др.);
- создание ВВТ (снижение стоимости новых образцов и сокращение времени их создания, включая сферу НИОКР и закупок);
- испытания и оценка (потребностей ВС, повышение качества принимаемых решений в сфере планирования и разработки бюджетных программ, оценка эффективности новых образцов ВВТ);
- тыловое обеспечение;
- боевая подготовка и обучение личного состава.

При этом в последнее время акцент делается на создание систем моделирования, направленных на решение задач в области строительства и применения объединенных и коалиционных группировок войск (сил).

Научно-технический совет МО США с начала 90-х гг. ввел свой вариант классификации моделей, выделив три основных их вида, подчеркивая различие в степени и характере участия человека в процессе моделирования, а именно[405]:

- натурные;
- виртуальные;
- конструктивные.

К натурным системам относятся традиционные войсковые и командно-штабные учения с привлечением штатной техники и личного состава. В настоящее время отмечается тенденция к сокращению масштабов натурного моделирования и, напротив, расширяется сфера использования других видов моделирования и имитации, особенно это касается виртуальных систем [405].

Виртуальные системы представляют собой человеко-машинные системы, в которых совмещается натурное и компьютерное

моделирование. В первую очередь – это различные тренажеры ВВТ, применяемые для обучения. В настоящее время в большинстве виртуальных систем некоторые из компонент представлены в натурном виде, например реальными образцами вооружения и военной техники, а также обслуживающим их персоналом. В качестве весьма перспективной разновидности виртуальной имитирующей системы может рассматриваться концепция так называемого виртуального прототипа. В таких системах предполагается полная замена реального оборудования его компьютерной имитацией. Данный подход широко используется при создании систем ВВТ [405].

Конструктивные системы могут быть [405]:

- полностью автономными (процесс моделирования не требует участия человека);
- интерактивными человекомашинными системами.

Большинство используемых моделей являются именно конструктивными. Здесь предметная область, характерные для нее объекты и процессы представляются с помощью математического (алгоритмического) описания и соответствующего программного обеспечения. Термин применяется главным образом для того, чтобы подчеркнуть отличие этого класса моделей от натурных и так называемых виртуальных моделей. К конструктивным системам относятся разного рода имитационные модели [405].

Архитектура современных систем моделирования боевых действий стандартизирована. Она включает в себя библиотеки стандартных программных модулей – генерирования случайных чисел, форматирования специфических докладов, выполнения сложных математических вычислений, управления ходом моделирования и др. [405].

Генератор сценария обеспечивает ввод данных в модель. Выходные данные анализируются стандартной системой анализа данных. Запуск модели, выполнение и остановка производятся через управляющий интерфейс. Интерфейс обеспечения обучения личного состава и боевой подготовки позволяет организовать интерактивное взаимодействие пользователей с моделью. Сетевой интерфейс обеспечивает взаимодействие различных компьютеров в составе моделирующего комплекса, в том числе разнородных моделей, а также распределенное моделирование на базе одной модели [405].

Продолжаются работы по развитию объектно-ориентированной архитектуры моделей, призванной обеспечить более эффективное взаимодействие моделей и их использование. Такая архитектура позволяет создать инфраструктуру моделирования, которая может

быть многократно использована в рамках разработки множества проектов создания моделей. При этом потребуется лишь добавить новую функциональность, реализующую решение новой задачи (описание новой среды функционирования или концептуальной схемы реального мира). По расчетам американских специалистов в этой области, возможно сокращение времени разработки моделей на 90% [405].

Важным направлением деятельности МО США в сфере военного моделирования является оценка, подтверждение и сертификация моделей. Данные процедуры предполагают установление степени соответствия моделей процессам реального мира, а также установление применимости модели для решения специфических задач. Тем самым очерчиваются круг проблем или специфические условия существования проблем, для решения которых применима данная модель [405].

Основные направления модернизации объединенных систем моделирования и имитации боевых действий связаны в первую очередь с необходимостью создания новых моделей, а также с совершенствованием существующих систем. Дефицит моделей, вызванный динамизмом и глобальностью изменений в мире, а также появлением новых предметных областей, в значительной степени преодолен за последние годы. Тем не менее актуализация исследований применения ВС США в локальных конфликтах и в различного рода «невоенных» операциях, например при осуществлении миротворчества в борьбе с терроризмом, наркобизнесом и т.п., требует разработки таких моделей, в которых был бы отражен значительно расширившийся спектр возможного применения вооруженных сил. Требуются новые или уточненные модели для использования в таких предметных областях, как: системы управления и связи; вычислительные системы и разведка; системы ПРО; радиоэлектронная борьба; при применении оружия нелетального воздействия; роботизированные комплексы и системы; специальные операции; миротворческие операции; борьба с терроризмом и наркобизнесом и другие [405].

Высказывается мнение, что для нового поколения моделей требуется более полный учет взаимодействия многих военных, политических, экономических, этнических, религиозных и некоторых иных факторов, так или иначе влияющих на глобальную и региональную безопасность в современных условиях [405].

Перспективы развития моделирования связываются с развитием таких ключевых направлений развития науки и технологий, как: высокопроизводительные вычисления; компьютерные сети; визуализация; системы виртуальной реальности; распределенные системы мо-

делирования. Благодаря программе МО США по высокопроизводительным вычислениям ресурсы суперкомпьютеров становятся все более доступными для имитации через облачные вычислительные ресурсы [405].

В целом необходимо отметить, что развитие систем моделирования и имитации в США рассматривается как один из основных факторов обеспечения эффективности строительства и применения вооруженных сил. Громадный потенциал, накопленный в данной области, уже сейчас оценивается как значительно опережающий возможности других стран мира в этой сфере [406].

В перспективе ожидается дальнейшее глобальное комплексирование моделей и внедрение систем виртуальной реальности (искусственного многомерного боевого пространства) на базе телекоммуникационных сетей, призванных обеспечить доступ пользователей как к оперативной, так и к физической моделируемой среде, к стандартизированным моделям и базам данных, а также к различного рода сценариям. Перспективные системы моделирования боевых действий будут имитировать применение вооруженных сил на любом континенте, на море, в воздухе и космическом пространстве, весь спектр их задействования (включая миротворческие операции, борьбу с терроризмом и т. п.). В будущем такие системы смогут с высокой степенью адекватности моделировать действия на фоне искусственно созданной боевой обстановки, воспроизводящей особенности любого ТВД. А в качестве противника будут выступать как полностью, так и частично компьютеризированные аналоги реальных войсковых формирований [406].

Более подробная информация о подходах к моделированию боевых действий представлена в работах [407, 462], а примеры реальных средств моделирования боевых действий применяемых в США в настоящее время – в работах [405, 406, 409, 410, 411]. Кроме того, в работе [404] рассмотрен вариант подобного комплекса, разработанного специалистами Республики Беларусь.

4.6.3.9. Средства технической разведки

Средства технической разведки предназначены для несанкционированного доступа к информации, ее копирования, а также для преодоления подсистем защиты информации у технических и компьютерных систем противника. В связи с этим их с полным основанием можно отнести к одному из видов обеспечивающего информационно-

технического оружия. Средства технической разведки позволяют получить информацию об атакующих средствах информационно-технического оружия противника и способах его применения, что позволяет более рационально сконфигурировать собственные средства информационно-технической защиты. Воздействие средств разведки проявляется как в виде пассивных действий, направленных на добывание информации и, как правило, связанных с нарушением ее конфиденциальности, так и активных действий, направленных на создание условий, благоприятствующих добыванию информации.

Техническая разведка – целенаправленная деятельность по добыванию с помощью технических средств соответствующих сведений в целях обеспечения военно-политического руководства своевременной информацией разведываемых странах и их вооруженных силах [412].

Задачи технической разведки – добывание и последующая обработка сведений [412]:

- о содержании стратегических и оперативных планов вооруженных сил, их боеспособности и мобилизационной готовности, создании и использовании мобилизационных ресурсов;
- о направлениях развития вооружения и военной техники, научно-исследовательских и опытно-конструкторских работах по созданию и модернизации образцов вооружения и военной техники;
- о количестве, устройстве и технологии производства ядерного и специального оружия;
- о тактико-технических характеристиках и возможностях боевого применения вооружения и военной техники;
- о дислокации, численности и технической оснащенности вооруженных сил;
- о степени подготовки территории страны к ведению боевых действий;
- об объемах поставок и запасах стратегических видов сырья и материальных ресурсов;
- о функционировании промышленности, транспорта и связи;
- об объемах, планах государственного оборонного заказа, выпуске и поставках вооружения, военной техники и другой оборонной продукции;

- о научно-исследовательских, опытно-конструкторских и проектных работах;
- о технологиях, имеющих важное оборонное или экономическое значение;
- о сельском хозяйстве, финансах, торговле;
- о внешнеполитической и экономической деятельности государства;
- о системе правительственной и иных видов специальной связи, о государственных шифрах.

Доля технической разведки в общей системе добывания защищаемой информации достаточно велика и по некоторым оценкам может составлять до 50% и более. Причем дальнейшее развитие науки и техники объективно приводит к повышению роли и значимости технической разведки [413].

Классификация технических средств разведки представлена на рис. 4.48 [415, 462]. Дополнительные сведения о средствах технической разведки, а также примеры конкретных технических устройств представлены в работах [412, 414].

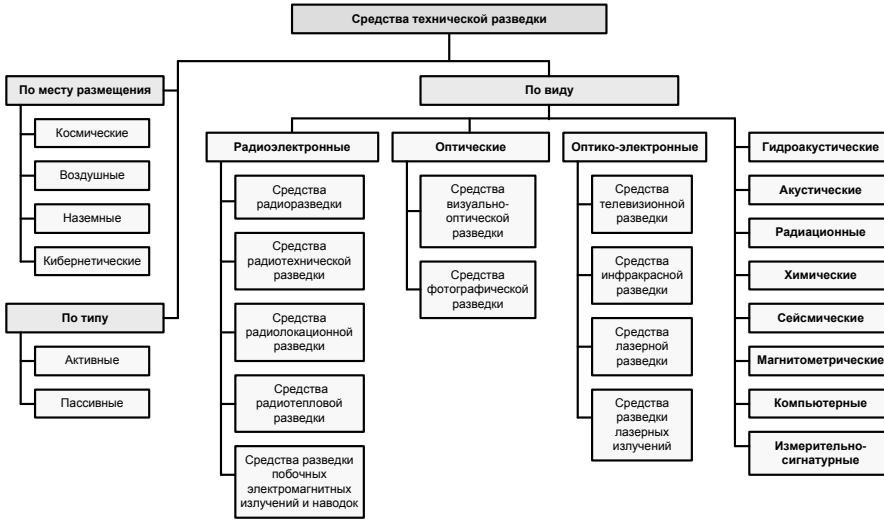


Рис. 4.48. Классификация средств технической разведки [415, 462]

4.6.3.10. Средства компьютерной разведки

Под компьютерной разведкой традиционно было принято понимать получение информации из баз данных ЭВМ, включенных в компьютерные сети, а также информации об особенностях их построения и функционирования [412]. Однако в настоящее время стало общепризнанным, что это слишком узкий, упрощенный подход к компьютерной разведке и поэтому она активно модернизируется и развивается.

Объектами компьютерной разведки являются компьютерные системы и сети, которые включают в себя: отдельные ЭВМ, многопроцессорные ЭВМ и компьютерные системы, информационно-вычислительные сети, программно-аппаратные комплексы, программное обеспечение ЭВМ, периферийное компьютерное оборудование, различное оборудование, содержащее встроенные процессоры и микрокомпьютеры и т.п. [416].

Таким образом, в общем случае под компьютерной разведкой понимается добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей. В связи с этим выделяют три типа источников информации для компьютерной разведки, такие как [416]:

- информация обрабатываемая, передаваемая и хранимая, в компьютерных системах и сетях;
- характеристики программных, аппаратных и программно-аппаратных комплексов;
- характеристики пользователей компьютерных систем и сетей.

Основным способом реализации разведки является атака средств компьютерной разведки. При этом, под атакой средств компьютерной разведки понимаются как пассивные действия, направленные на добывание информации и, как правило, связанные с нарушением ее конфиденциальности, так и активные действия, направленные на создание условий благоприятствующих добыванию информации.

Классификация средств компьютерной разведки представлено на рис. 4.49 по материалам работ [416-418, 462].

К настоящему времени сложился подход к описанию компьютерных атак, основанный на использовании их классификации с учетом множества признаков. В научной литературе представлены различные классификации, отличающиеся полнотой учета признаков. Наиболее полный учет признаков реализован в классификации CAPEC

[419], разработанной корпорацией MITRE и применяемой для ведения базы данных образцов компьютерных атак в интересах защиты киберпространства США. Однако классификация атак CAPEC не выделяет в отдельную категорию атаки средств компьютерной разведки. Учитывая этот недостаток классификации CAPEC, отечественными специалистами в работе [418] была предложена классификация атак средств компьютерной разведки с включением в классификацию образцов конкретных атак. Эта классификация представлена на рис. 4.50.

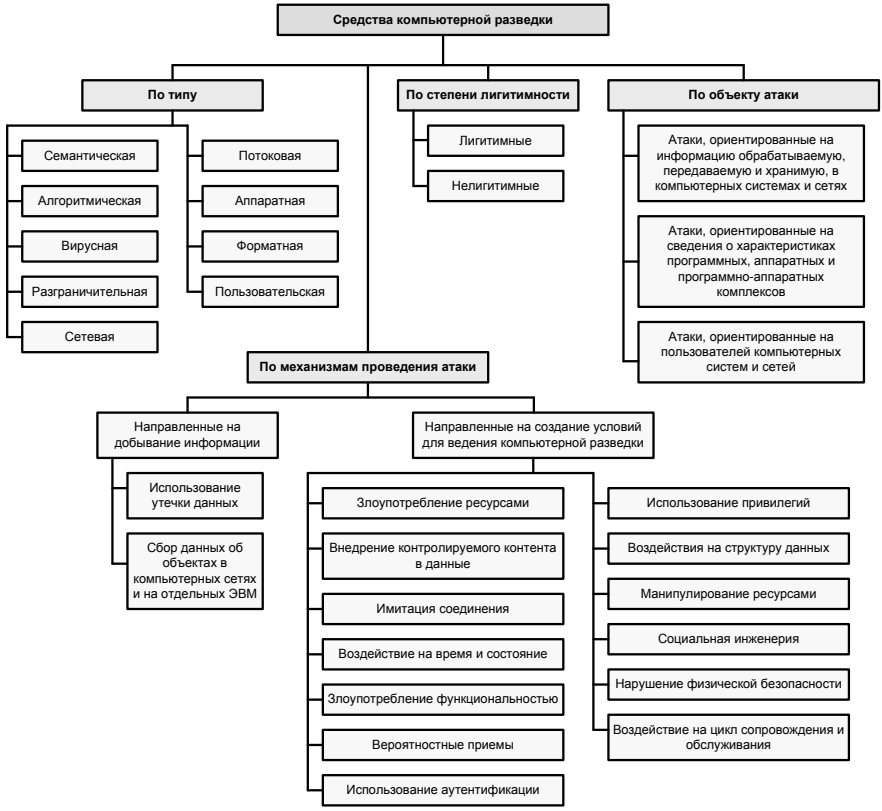


Рис. 4.49. Классификация средств компьютерной разведки

В настоящее время многие технологически развитые страны активно разрабатывают и совершенствуют собственные средства и комплексы компьютерной разведки. Большинство программ по разработке таких комплексов санкционировано на государственном уровне

и применяются для получения стратегического информационного превосходства в военной, политической и промышленной сфере.

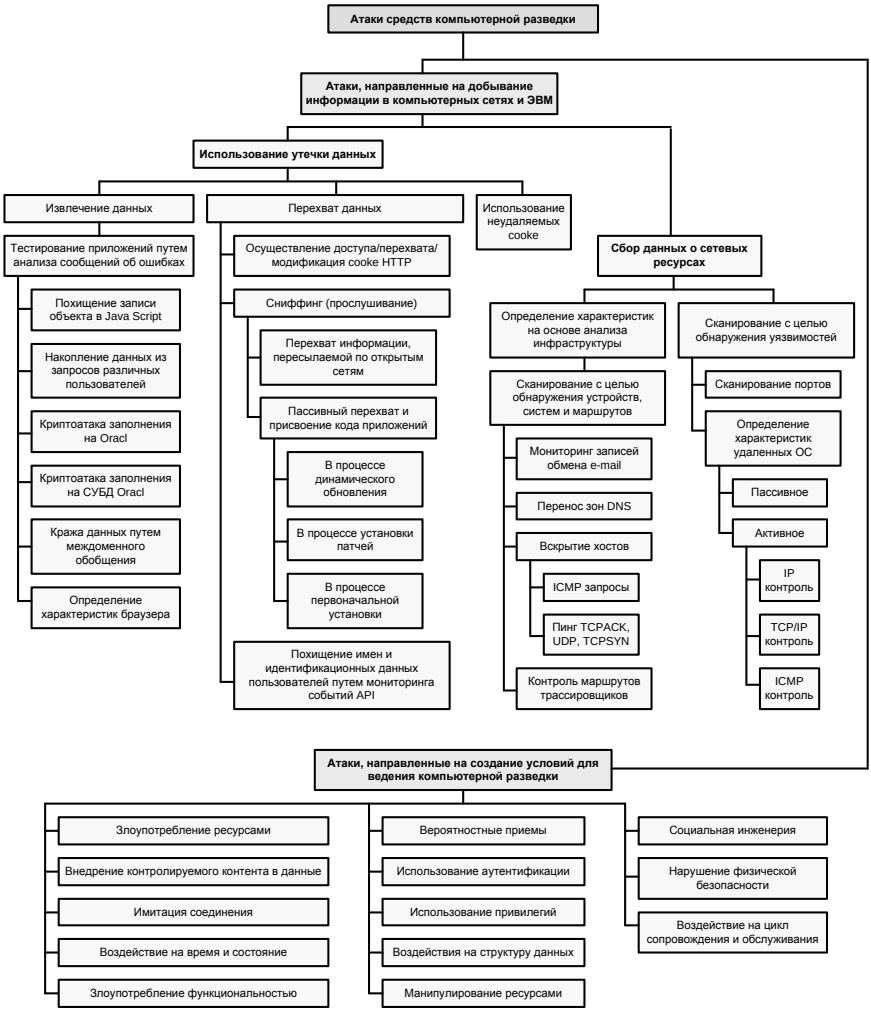


Рис. 4.50. Классификация атак средств компьютерной разведки [418, 462]

К странам, имеющим наибольшие достижения в области создания глобальных комплексов компьютерной разведки необходимо отнести США (программы: «Carnivore», «Eshelon», «NarusInsight», «Turbulence», «CO-TRAVELER», «PRISM», «Dropmire», «XKeyscore»),

Великобританию (программа «Tempora»), Китай (программа «Золотой щит») и Россию (программа СОРМ). Помимо них, другие технически развитые страны также создают свои комплексы компьютерной разведки – Франция (программа «Frenchelon»), Швейцария (программа «Onyx»), Швеция (программы «Titan»), Индия (программы NATGRID, «Central Monitoring System», DRDO NETRA). Подробно эти программы рассмотрены в материалах [420, 421, 422, 423, 424, 425, 426, 462].

Таким образом, современные средства и комплексы компьютерной разведки, как правило, предназначены для сбора данных пользователей путем мониторинга используемых ими компьютерных средств (персональных компьютеров, планшетов, смартфонов, мобильных телефонов) в глобальной сети Интернет, а именно – для сбора данных о размещенной информации в социальных сетях, записях на форумах, отправленных электронных сообщениях, посещенных Интернет-страницах. При этом для сбора данных об объектах разведки, как правило, используются санкционированные на государственном уровне средства добывания информации, реализованные в виде программных или аппаратных закладок в телекоммуникационное оборудование операторов связи, а в отдельных случаях – вирусные средства компьютерной разведки.

4.6.3.11. Средства разведки по открытым источникам в глобальном информационном пространстве

Разведка на основе анализа открытых источников информации (Open Source Intelligence – OSINT) является достаточно старым видом деятельности для военной разведки США, и ее история ведется еще со времен Второй мировой войны. Однако, если ранее OSINT рассматривалась как возможность «закрывать информационные бреши» в случае неспособности других видов разведки выполнить поставленную задачу, то сейчас, в связи с развитием в начале XXI века глобального информационного пространства и сети Интернет, по оценкам американского военного руководства, OSINT резко повысила свою значимость [427, 428].

Во многом повышение значимости разведки на основе анализа открытых источников обусловлено тем фактом, что порядка 10-15% необходимой информации имеется в Интернете уже в готовом виде (необходима только ее верификация), а остальные 85-90% информации могут быть получены в результате сравнения, анализа и синтеза разрозненных и разбросанных по разным источникам фактов. Есте-

ственно, что информация, полученная таким образом, нуждается в верификации [429].

В сферу интересов такой разведки входит добывание и анализ официальных документов, проектов уставов и наставлений, отслеживание новых научных разработок и проектов, баз данных, коммерческих и государственных интернет-сайтов, сетевых дневников и многого другого [427,428].

Рис. 4.51. Вариант классификации средств разведки по отрытым источникам

Для решения задач анализа открытых источников используются аппаратно-программные средства, основу которых составляют алгоритмы поиска и семантического анализа.

Примерами таких программ могут служить программы «Taiga», «Tropes», «Noemic», а также современные комплексы интеллектуального анализа так называемых Больших Данных (Big Date) [429, 462].

Особенностью программ анализа данных на основе семантических поисковых алгоритмов является то, что они могут находить только ту информацию, которая в явном виде имеется в документах, размещенных в сети Интернет, а уже потом, за счет анализа различных документов с совпадающим целевым контентом, начинают собирать информационное наполнение запроса пользователей. Более интерес-

ным направлением развития средств разведки является анализ разнородных, изначально семантически не связанных между собой данных с целью выявления неслучайных совпадений или скрытых закономерностей и последующей их «привязкой» к объектам разведки. Такое направление получило развитие в рамках исследования проблемы Больших Данных (Big Date).

Технологии Больших Данных основаны прежде всего на методах статистического и интеллектуального анализа данных применяемых на огромных, постоянно пополняемых массивах данных. Эти технологии позволяют [430, 462]:

- *проводить самые различные и сколь угодно подробные классификации той или иной совокупности людей, компаний, иных объектов по самым разнообразным признакам*. Такие классификации обеспечивают точное понимание взаимосвязи тех или иных характеристик любого объекта – от человека до компании или организации, с теми или иными его действиями;
- *осуществлять многомерный статистический математический анализ*. Этот анализ позволяет находить корреляции между самыми различными параметрами, характеристиками, событиями и т.п. Корреляции не отвечают на вопрос – почему. Они показывают вероятность, с которой при изменении одного фактора изменяется и другой. В каком-то смысле Большие Данные представляют собой альтернативный традиционной науке метод познания действительности. Теоретические модели отвечают на вопрос – почему, а затем, выявив причинно-следственные закономерности, позволяют формировать рекомендации о порядке действий. В случае выявления корреляционных закономерностей в Больших Данных, стадия выявления первопричины отсутствует, а сразу выявляется закономерная связь различных факторов. При этом, если факторы тесно взаимосвязаны, на один из факторов возможно осуществить воздействие для достижения целенаправленного изменения связанного с ним фактора;
- *прогнозировать*. На основе классификаций и аналитических выкладок осуществляется прогнозирование, суть которого состоит в том, чтобы на основе выявленной корреляционной связи факторов определить наиболее целесообразный способ воздействия для того, чтобы один набор

факторов, характеризующих тот или иной объект, лицо, компанию, событие и т.п., был преобразован в другой.

Большие Данные как прорывная информационная технология были быстро осознаны такими странами как США, Великобритания и Япония. 29 марта 2012 г. администрация Б. Обамы выступила с инициативой «Big Data Research and Development Initiative». Этой инициативой предусматриваются вложение значительных объемов ресурсов и проведение комплексных мероприятий в целях активного использования технологий Больших Данных в интересах ключевых направлений политики США. В сентябре 2013 г. правительство Японии опубликовало информацию о разработке национальной программы по Большим Данным. Летом того же года правительство Австралии заявило, что рассматривает Большие Данные как важнейший национальный стратегический ресурс и выдвинуло задачу стать головной страной в сфере использования технологий Больших Данных как на правительственном уровне, так и на всех других уровнях государственного аппарата в масштабах Британского содружества [430].

4.6.3.12. Средства управления поведением социальных групп

Помимо непосредственно разведки и контрразведки технологии Больших Данных начали использоваться для выявления глубоких паттернов поведении в социальной среде.

В последние годы создана, по сути, новая наука – социодинамика, которая обобщает эмпирические закономерности, полученные в результате применения технологий Больших Данных к огромным массивам информации, содержащейся в архивах крупнейших социальных платформ на основе Web и Web 2.0, таких как Google, Facebook, Twitter и т.п. Эти эмпирические закономерности сегодня используются для отработки практического инструментария внешнего воздействия, управления и манипулирования социальными группами любых масштабов и любого уровня структурированности, а также для сборки и деструкции социальных субъектов. Именно применение Больших Данных к информации, полученной из социальных сетей, позволило осуществить прорыв в отработке инструментария внешнего социального управления поведением [77, 430].

Средства прогнозирования на основе технологий Больших Данных. Одним из направлений эффективного применения технологий Больших Данных является прогноз развития социальных, полити-

ческих, военных и экономических процессов. При этом к началу нулевых годов специалисты, ведущие исследования в этой сфере, сформулировали, по меньшей мере, три фундаментальных положения, из которых следует, что [430]:

- используя самые изощренные и эффективные методы, можно прогнозировать процессы, но не события;
- прогнозы с высокой степенью вероятности можно делать в отношении групп различной размерности, но не отдельных индивидуумов;
- знания о действиях групп и индивидуумов в одной ситуации не позволяют давать точные прогнозы о подобных действиях, осуществляемых в другой ситуации.

Соответственно оказалось, что различного рода прогнозы, базирующиеся на традиционных выборках, построении сценариев, экстраполяции, не обладают высоким уровнем адекватности. Развитие Интернета дало возможность оперировать Большими Данными относительно человеческого поведения, намерений, желаний и т.п. Прогнозирование на основе Больших Данных состоит в извлечении нетривиальных выводов из заранее известных характеристик, признаков и сведений об объектах. Использование Больших Данных из Интернета, как огромного, пополняемого в режиме реального времени поведенческого архива для прогнозирования развивается по таким трем ключевым направлениям, как [430]:

- прямой интеллектуальный анализ общедоступных данных, предоставляемых поисковыми системами и различного рода социальными сетями и платформами;
- создание рекомендательных систем, которые прогнозируют различного рода выбор субъектов и групп и на этой основе рекомендуют им что угодно – от книг до кандидатов в президенты;
- создание сложных прогностических систем, использующих разнородные данные, получаемые из открытой и закрытой части глобальной сети, обрабатываемые с помощью большинства известных методов интеллектуального анализа данных.

В качестве одного из наиболее ярких примеров успешного создания средства разведки как сложной прогнозной системы можно привести проект Recorded Future. В январе 2010 г. проект Recorded Future был запущен при поддержке инвестиций компании Google и

инвестиционного фонда американского разведывательного сообщества In-Q-Tel.

Таким образом, Большие Данные обеспечили появление новых, на порядки более эффективных, чем раньше, методов прогнозирования научно-технических, инженерно-технологических, инвестиционных, политических, социальных и военных процессов. Эти методы в совокупности с методиками глубокого анализа на основе все тех же Больших Данных позволяют говорить о создании принципиально нового вида информационного оружия, а именно – прогностических средств. Этот вид оружия может быть использован как обеспечивающий механизм для разработки и применения традиционных вооружений.

Средства манипуляции и управления поведением социальных групп на основе технологий Больших Данных. Как показано выше, наличие огромного всеобъемлющего поведенческого архива позволило компаниям-владельцам Больших Данных использовать их для предсказания поведения. Вместе с тем прогнозирование поведения социальных групп в тех или иных условиях позволяет решить и другую задачу – выбора условий и воздействий, при которых бы целевая социальная группа действовала бы необходимым, заранее предопределенным, образом. В работе [431] для такой манипуляции в отношении целевых социальных групп введено понятие «подталкивание» (nudge).

Подталкивание представляет собой комплекс способов использования поведенческих стереотипов, психофизиологических реакций и технологий Больших Данных для целенаправленной коррекции поведения тех или иных конкретных социальных групп. При этом выбор тех или иных факторов воздействия, которые обеспечивают реализацию эффекта подталкивания, осуществляется на основе предсказательной аналитики полученной по итогам обработки Больших Данных [431].

Летом 2013 г. было объявлено, что команды по использованию этой технологии создаются в большинстве министерств США, связанных с социальными вопросами. На них возложена задача подталкивания американцев к правильным, с точки зрения правительства, решениям не на основе объяснений, а путем использования поведенческих стереотипов, привычек и психофизиологических реакций. При этом американские СМИ высказали подозрение, что подобные команды создаются и в других, в том числе разведывательных, ведомствах. Однако их финансирование реализуется через секретные статьи бюджета, и поэтому их существование не афишируется [431].

Профессионалы подталкивания, развивая поведенческую политику, исходят из нескольких основных принципов.

- Для решения своих поведенческих проблем люди нуждаются во вмешательстве третьих лиц. Наилучшим кандидатом на эту роль является государство.
- Эксперты, изучая то влияние, которое в реальной жизни оказывают на благосостояние те или иные акты выбора, принимают от имени индивидов решения лучше тех, на которые индивиды способны сами.
- Любые стимулирующие схемы, которые возлагают на людей ответственность за последствия их прошлых действий, неэффективны. Вместо них необходимы схемы, которые немедленно вознаграждают или наказывают людей за будущие последствия их текущих действий – последствия, которые сами они не способны осознать и учесть.
- С точки зрения политики то, как люди ощущают себя в обществе, важнее того, что они желают, или того, что они делают.

Ключевую роль в технологиях подталкивания играют Большие Данные. Именно Большие Данные позволяют в зависимости от поставленной задачи проводить классификацию групп и ситуаций, осуществлять анализ и прогноз, а главное – искать факторы, обеспечивающие нужное поведение целевых групп в конкретных ситуациях. И наконец, они в режиме реального времени позволяют отслеживать эффективность подталкивания [431].

Стоит отметить, что при наличии соответствующих Больших Данных фактически нет никаких ограничений для использования технологий подталкивания не только в отношении граждан собственной страны, но и населения любых государств мира. Таким образом, в настоящее время АНБ и другие государственные структуры США разрабатывают и переходят к практическому использованию технологий управления групповым и массовым поведением в других странах мира – как в странах-союзниках, так и в странах-противниках.

При наличии соответствующих Больших Данных подталкивание может рассматриваться как эффективное информационно-психологическое оружие следующего поколения. Хотя с учетом принципов и технологий, на которых построена система подталкивания, более точным является не привычное наименование информационно-психологического оружия, а скорее отнесение этой технологии к поведенческому оружию, базирующемуся на симбиозе высокопроизводи-

тельных технических средств обработки, технологиях Больших Данных, достижениях объективной психологии и нейронауках [431].

4.6.4. Психологическое и информационно-психологическое оружие

В настоящее время теория информационно-психологического противоборства достаточно широко исследована. Ниже рассмотрены основные аспекты разработки и использования в современных военных конфликтах психологического и информационно-психологического оружия. При этом более подробно различные аспекты информационно-психологического противоборства рассмотрены в работах ведущих ученых этой области – Г.В. Грачева, А.И. Зиновьева, А.Г. Караяни, В.Г. Крысько, В.А. Лисичкина, А.В. Манойло, И.Н. Панарина, В.С. Пирумова, С.П. Расторгуева, П.А. Шелепина, Г.Г. Почепцова, С.Г. Кара-Мурзы, В.В. Цыганова, С.Н. Бухарина, Д.А. Новикова, А.Г. Чхартишвили, В.А. Баришполеца, а также в работах других ученых.

4.6.4.1. Особенности ведения информационно-психологического противоборства

Информационно-психологическое противоборство, психологическая война. Информационно-психологическое противоборство имеет давнюю историю. Оно возникло одновременно с появлением вооруженного противоборства как составная часть вооруженной борьбы в виде психологического средства ослабления боевой мощи противника и поднятия боевого духа своих войск. В настоящее время информационно-психологическое противоборство выделилось в самостоятельную форму борьбы, которая может вестись как без непосредственного применения военного насилия, так и в сочетании с военной силой. Для многих государств информационно-психологическое противоборство, особенно проявляющееся в таких острых и агрессивных формах, как цветные революции, стало крайне опасным явлением [432].

Научно-технический прогресс в области информационно-коммуникационных технологий, стирающих национальные границы, и успехи социальной психологии в сфере изучения поведения масс, вынуждают руководство ведущих мировых держав пересматривать свои военные концепции. Распространяется практика целенаправленного

информационно-психологического давления, наносящего существенный ущерб национальным интересам противоборствующих государств [432].

В настоящее время руководством США проведение мероприятий по информационно-психологическому воздействию на военно-политическое руководство и общественное мнение различных стран, на мировое сообщество в целом возводится в статус основного содержания подготовки к военным действиям [432].

Информационно-психологическое противоборство – процесс, отражающий различные уровни противодействия конфликтующих сторон, осуществляемого информационными и психологическими средствами для достижения политических и военных целей. Такая широкая трактовка рассматриваемого феномена позволяет охватить информационно-психологические акции, осуществляемые [433]:

- на разных уровнях (стратегическом, оперативном и тактическом);
- как в мирное, так и в военное время;
- как в информационной, так и в духовной сфере;
- как среди своих военнослужащих, так и среди войск противника.

В системе информационно-психологического противоборства, осуществляемого в военных целях, можно выделить [433]:

- информационную войну;
- психологическую войну.

Информационная война – борьба сторон за достижение информационного превосходства над противником в своевременности, достоверности, полноте получения информации, скорости и качестве ее переработки и доведения до исполнителей [433].

Эта война включает в себя такие направления деятельности, как [433]:

- добывание необходимой информации;
- переработка полученной информации;
- защита информационных каналов от проникновения противника;
- своевременное и качественное доведение информации до потребителей;
- дезинформация противника;
- вывод из строя или нарушение функционирования систем добывания, переработки и распространения информации противника;

- уничтожение, искажение, хищение информации у противника;
- разработка более эффективных, чем у противника, средств работы с информацией.

Средствами ведения информационной войны могут быть [433]:

- средства информационно-технического оружия;
- средства подавления информационных систем противника, вхождения в них в целях воздействия на циркулирующую информацию;
- средства пропагандистского вмешательства.

Психологическая война – борьба между государствами и их вооруженными силами за достижение превосходства в психологической и духовной сфере, а также за превращение полученного преимущества в решающий фактор достижения победы над противником. При таком подходе информационные возможности, наряду с чисто психологическими акциями, выступают средством решения психологических задач.

Рассматривая атакующие аспекты информационно-психологического противоборства можно сформулировать следующую цель воздействия.

Цель информационно-психологического противоборства – установление контроля над стратегически важными ресурсами страны-противника за счет управления людьми, заставив население страны-жертвы поддерживать агрессора, действуя вопреки своим интересам, не задействуя имеющиеся социально-психологические защитные механизмы [432].

Цель информационно-психологического противоборства в мирное время и угрожаемый период достигается решением таких задач, как [432]:

- подмена у граждан традиционных нравственных ценностей и ориентиров, создание атмосферы бездуховности, разрушение национальных духовно-нравственных традиций и культивирование негативного отношения к культурному наследию противника;
- манипулирование общественным сознанием и политической ориентацией социальных групп населения страны по осуществлению так называемых демократических преобразований в интересах создания обстановки политической напряженности и хаоса;

- дезорганизация системы государственного и военного управления, создание препятствий функционированию государственных институтов и органов управления вооруженными силами;
- дестабилизация политических отношений между партиями, объединениями в целях провокации конфликтов, нагнетания атмосферы недоверия органам государственного управления;
- обострение политической борьбы, провоцирование репрессий против оппозиции – сети неправительственных организаций (так называемых демократических сил) и отдельных независимых активистов;
- снижение уровня информационного обеспечения органов власти и управления в целях затруднения принятия важных решений;
- дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;
- провоцирование социальных, политических, национальных и религиозных столкновений;
- мобилизация протестных настроений и инициирование забастовок, массовых беспорядков и других акций экономического протеста;
- подрыв международного авторитета государства, его сотрудничества с другими странами;
- нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах.

При информационно-психологическом противоборстве в военное время решаются аналогичные задачи, однако объектами воздействия и защиты являются население и личный состав вооруженных сил противостоящих сторон, а также системы формирования общественного мнения и принятия решений, к которым относятся политическое и военное руководство государств.

Психологические операции. В настоящее время в странах НАТО весь комплекс мер информационно-психологического воздействия на войска и население противника обозначается термином «психологические операции» (ПсО) [433].

В вооруженных силах НАТО организация психологических операций регламентируется директивами, уставами и наставлениями,

разрабатываемыми как для армий отдельных государств, так и для блока в целом. Своеобразный тон в определении общих ориентаций, масштабов, интенсивности, форм и методов осуществления информационных и психологических акций в рамках ПсО задают США. Американская система взглядов на ПсО, во-первых, включает в себя все, что наработано в этой области в других странах, во-вторых, сама выступает для них неким эталоном в данной сфере и, в-третьих, демонстрирует в последнее время практические приемы организации воздействий в этой области [433].

Психологические операции – это проводимая в мирное или военное время плановая пропагандистская или психологическая деятельность, рассчитанная на иностранные враждебные, дружественные или нейтральные аудитории с тем, чтобы влиять на их отношение и поведение в благоприятном направлении для достижения как политических, так и военных целей [433].

Как видно из определения, ПсО представляют собой скоординированную пропагандистскую деятельность и психологические действия. При этом под пропагандой понимается систематическое, целенаправленное распространение с помощью средств связи и информации определенных идей с целью оказания влияния на мнения, чувства, состояния и отношения или поведение объектов воздействия с тем, чтобы достичь прямых или косвенных выгод для своей страны. При этом пропаганда может быть: «белой» (если указывается объективный источник информации), «серой» (если этот источник не упоминается) и «черной» (при сфальсифицированном источнике информации). Психологические действия – это осуществление конкретных мероприятий как в мирное, так и в военное время, направленных на подрыв потенциального или действительного престижа и влияния противника во враждебных, нейтральных или союзных странах и укрепление своего влияния и престижа [433].

Разовые мероприятия психологической войны представляют собой кратковременные целенаправленные действия специальных подразделений или отдельных специалистов, которые отличаются ограниченным характером и осуществляются в ограниченных (локальных) масштабах [434].

Психологические операции и разовые мероприятия психологической войны, направленные против войск и населения противника, различаются между собой целями, задачами, объектами воздействия, технологиями и теми условиями, в которых они проводятся [434].

Психологические операции состоят из политических, военных, экономических, дипломатических и собственно информационно-психологических мероприятий, направленных на конкретные группы населения и войск противника с целью внедрения в их сознание чуждых идеологических и социальных установок, формирования ложных стереотипов поведения, трансформации в нужном направлении их настроений, чувств, воли, склонения их к отказу от боевых действий, предательству, сдаче в плен или дезертирству. При правильном планировании психологические операции предшествуют применению военной силы, а затем сопровождают либо дополняют повторное ее использование. Они осуществляются в рамках государственной политики, а их военная и прикладная стороны согласовываются и координируются с деятельностью соответствующих правительственных учреждений [434].

Психологические операции бывают различных видов, которые в свою очередь классифицируют по срокам, условиям осуществления, направленности.

По срокам осуществления и ориентированности на уровни военного управления психологические операции делят [434]:

- на стратегические;
- на оперативные;
- на тактические.

По времени осуществления психологические операции делятся [434]:

- на проводимые в мирное время (угрожающий период);
- на проводимые в военное время;
- на проводимые в ходе миротворческой деятельности.

Психологические операции делят по направленности [434]:

- против гражданского населения;
- против войск противника;
- против командования противника;
- на введение противника в заблуждение;
- на содействие оппозиционным силам и диссидентским движениям;
- на осуществление культурной экспансии и диверсий; консолидирующие психологические операции.

Мероприятия психологических операций проводят ради внедрения в сознание населения и войск противника конкретных взглядов, убеждений или лозунгов, мотивов недоверия или неудовлетворения действиями своего политического и военного руководства, осознания

своего неблагоприятного положения, угрозы жизни и благополучию родственников и для введения их в заблуждение, обмана, склонения к сотрудничеству [434].

Сам термин «психологические операции» указывает на то, что для достижения целей подрывной деятельности широко применяются выводы психологической науки, которые направлены, в первую очередь, на изменение психологических состояний противника [433].

Таким образом, психология как наука в рамках психологических операций [433]:

- указывает на те особенности человеческой и групповой психики, которые целесообразно подвергнуть воздействию;
- разрабатывает эффективные методы оценки психологического состояния противника;
- дает рекомендации специалистам, ведущим психологическую войну, по планированию операций;
- вырабатывает критерии и методы оценки результативности психологического воздействия на людей.

Создавая научный фундамент психологических операций, военные психологи западных стран опираются на достижения различных психологических школ. При этом за основу принимаются следующие положения [433]:

- о решающей роли бессознательного в детерминации человеческого поведения, о функционировании механизмов психологической защиты и способах их преодоления (психоанализ);
- о рефлекторном закреплении («якорении», зомбировании) определенным образом соотносящихся восприятий, переживаний, действий; о внушающей силе структуры, эмоционального тона, пространственно-временных характеристик информации (бихевиоризм, нейролингвистическое программирование);
- о роли ментальных схем в восприятии человеком окружающего мира, происходящих событий и информации (когнитивная психология);
- о структуре и динамике потребностей человека (гуманистическая психология) и др.

Психология помогает организаторам психологических операций выявлять наиболее слабые звенья в морально-психологическом состоянии противника и научно обоснованно строить тактику психологического давления на него. Она рекомендует широко использовать

в этих целях национальные, социальные, религиозные противоречия; трудности, с которыми сталкиваются войска противника (голод, холод, плохое материально-техническое обеспечение и др.); распространять слухи и дезинформацию о значительном превосходстве своих войск, больших потерях противника, различии интересов и целей разных категорий военнослужащих; активно работать с военнопленными и др. Выводы психологии активно используются для придания распространяемой информации свойства легкой и быстрой усваиваемости, просачиваемости в бессознательное человека. Это достигается путем эксплуатации закономерностей человеческого восприятия, так называемых эффектов. Среди них хорошо изученным на сегодняшний день являются эффекты: первичности, авторитета, «голос пророка»; повторения; возложения ответственности и др. Более подробная информация об использовании этих эффектов представлена в работе [433].

Информационно-психологические воздействия. Основным способом ведения информационно-психологического противоборства является использование информационно-психологических воздействий.

Информационно-психологическое воздействие – информационное, энергоинформационное или психофизическое воздействие на психику человека, оказывающее влияние на восприятие им реальной действительности, в том числе на его поведенческие функции, а также в некоторых случаях на функционирование органов и систем человеческого организма [435].

Любой человек как личность, активный социальный субъект, носитель определенного мировоззрения, обладающий определенным правосознанием и менталитетом, духовными идеалами и ценностными установками, может быть подвергнут непосредственному информационно-психологическому воздействию, которое, трансформируясь через его поведение, действия (или бездействие), оказывает влияние на социальные объекты разного уровня общности, различной системно-структурной и функциональной организации. Таким образом, с помощью информационно-психологического воздействия можно влиять не только на индивидуальное сознание, но и на групповое, массовое и общественное сознание. Причем это влияние может носить как позитивный, так и негативный характер [435].

Информационно-психологическое воздействие может осуществляться с помощью различных методов (приемов, форм, методик) и средств, большая часть из которых, непрерывно развиваясь и совершенствуясь, превратилась сегодня в сложные технологии воздействия

на психику людей, обобщенно называемые в литературе *психотехнологиями*. Так, например, к психотехнологиям относятся современные информационные технологии воздействия на индивидуальное, групповое, массовое и общественное сознание с использованием телевизионной и радиовещательной техники, видео- и аудиопродукции, а также компьютерные технологии высокого уровня, позволяющие диагностировать и корректировать психическое и физическое состояние человека путем прямого доступа в подсознание [435].

С точки зрения физической сущности, принципов и механизмов воздействия средства и методы информационно-психологического воздействия могут быть классифицированы следующим образом [435, 436].

1) *Убеждение и суггестивные методы*:

- убеждение – метод открытого вербального (словесного) информационно-психологического воздействия на сознание индивида или группы людей, основу которого составляет система ясных, четко сформулированных доводов (аргументов), выстроенных по законам формальной логики и обосновывающих выдвигаемый субъектом воздействия тезис (точку зрения);
- суггестия или внушение – это процесс неаргументированного информационно-психологического воздействия на сознание человека, связанный со снижением критичности при восприятии и реализации им содержания сообщаемой информации, с отсутствием активного ее понимания, осмысления, развернутого логического анализа и оценки в соотношении с прошлым опытом. В отличие от убеждения внушение основывается не на логике и разуме человека, а на его способности воспринимать слова другого лица как должное, как инструкцию к действию. При внушении сначала происходит восприятие информации, содержащей готовые выводы, а затем на ее основе формируются мотивы и жизненные установки определенного поведения;

2) *Информационно-техногенные методы:*

- пропаганда – распространение политических, философских, научных, художественных знаний (идей) и другой информации в обществе с целью формирования у людей определенного мировоззрения – обобщенной системы взглядов на окружающий мир, место и роль в нем человека, на отно-

шение людей к объективной реальности и к друг другу, а также соответствующих этому идеалов и убеждений, принципов познания и деятельности, ценностных ориентаций.

- средства и методы предъявления неосознаваемой акустической информации;
- средства и методы предъявления неосознаваемой зрительной информации. Предполагается, что визуальные средства в отличие от вербальных позволяют человеку практически мгновенно воспринимать запрограммированное информационно-психологическое воздействие (хотя сработать оно может значительно позднее), причем это воздействие является более глубоким и долговечным, поскольку визуальные системы влияют не только на интеллект, но и на эмоционально-чувственный базис человека.
- гипнотические методы информационно-психологического воздействия – основаны на выявленном факте, что соответствующими внушениями в гипнотическом состоянии можно программировать человека на выполнение тех или иных действий;
- метод нейролингвистического программирования – особая психотерапевтическая техника, сутью которой являлось кодирование (программирование) человека как вербальными «формулами поведения», так и невербальными (мимика, пантомимика и т.д.) средствами воздействия;
- тренинговые методы информационно-психологического воздействия – методы регуляции психического состояния человека, такие как: управление вниманием, оперирование чувственными образами, словесные внушения, регуляция мышечного тонуса, управление ритмом дыхания;
- мистико-эзотерическое внушение.

3) *Информационно-техногенные средства и методы информационно-психологического воздействия:*

- информационные и технические психотехнологии с использованием телевизионной, вычислительной, радиовещательной техники, аудио-, видео-, печатной и кинопродукции;
- воздействие через компьютерные видеоигры и Интернет;
- генераторы специальных излучений;
- акустические системы с «интеллектуальным» сигналом (включая инфразвук и ультразвук);

- оптические средства в видимом, инфракрасном и ультрафиолетовом диапазонах;
- биорезонансная стимуляция работы головного мозга.

Информационно-психологическое воздействие с помощью этих средств и методов достигается по направлению «от техники – к человеку» и наиболее широко осуществляется через средства массовой информации.

4) *Психотропные средства информационно-психологического воздействия:*

- психотропные средства;
- другие биологически активные вещества преимущественно оказывающие влияние на психические функции человека (в том числе на эмоции и поведение), а также способные переводить его в измененное состояние сознания.

5) *«Феноменологические» методы информационно-психологического воздействия* – неосознаваемое информационное взаимодействие через органы чувств относится в первую очередь к биоинформатике, психофизиологии и сенсорной физиологии человека.

6) *Средства и методы манипуляции сознанием* – специфический вид скрытого информационно-психологического воздействия, направленный на программирование идей, мнений, мотивов, жизненных установок, стереотипов, устремлений, настроений и даже психического состояния людей с целью обеспечения такого их поведения, которое нужно тем, кто владеет средствами манипуляции.

7) *Комбинирование средств и методов информационно-психологического воздействия* – одновременное применение двух и более средств (методов) такого воздействия.

Достаточно подробно применение этих средств и методов информационно-психологического воздействия рассмотрено в работах [435, 462].

Применение информационно-психологического воздействия в боевой обстановке имеет свои особенности [434]:

- допускаются не только гуманные, но и антигуманные способы и приемы психологического воздействия;
- психологическое воздействие осуществляется в сочетании с применением средств вооруженной борьбы;
- есть стремление достичь максимальной психогенной результативности воздействия.

Информационно-психологическое воздействие только тогда дает наибольший реальный эффект, когда учитываются присущие

этим конкретным сферам особенности функционирования индивидуального, группового и общественного сознания [434].

4.6.4.2. Психологическое оружие – понятия и классификация

Организация информационно-психологических воздействий производится специальными средствами, позволяющими осуществлять целенаправленное влияние на общественное мнение, сознание, подсознание, поступки людей, их психическое состояние, чувства и здоровье.

Изучение совокупности этих средств позволяет сделать вывод о том, что сегодня в мире ускоренными темпами создается, проходит полевые испытания и практически используется при решении военных задач новый класс мощного, высокоэффективного оружия на основе современных и перспективных психотехнологий, которое может стать одним из решающих средств достижения целей в современной войне [433].

Психологическое оружие – совокупность средств, избирательно влияющих на психическую деятельность людей с целью задания ей необходимых характеристик и целенаправленного управления человеческим поведением в интересах успешного решения боевых задач [433].

Такое оружие, по мнению специалистов ПсО, представляя собой комплекс средств преднамеренного и организованного воздействия на психику и поведение военнослужащих на поле боя, должно обладать определенными свойствами, позволяющими решать следующие задачи [433]:

- обеспечивать достижение целей войны без нанесения непоправимого ущерба экологии, народнохозяйственной инфраструктуре, людским ресурсам государства-противника;
- гарантированно снижать боеспособность войск противной стороны до заданных пределов, на промежуток времени, необходимый для решения тактических, оперативных и даже стратегических задач;
- существенно расширять психические возможности военнослужащих собственных частей и подразделений, что позволит достигать многократного превосходства над противником по критериям морально-психологического состоя-

ния, боевой активности, психологической устойчивости и профессионального мастерства;

- принуждать противника к занятию им невыгодных районов и рубежей посредством постановки «психологических заграждений»;
- поражать личный состав противника на больших площадях и на всю глубину его боевых порядков (оперативного построения);
- применяться оружие по отношению к гражданскому населению в целях стимуляции у него психических состояний и побуждений, благоприятствующих решению войсками боевых задач;
- быть менее затратоемким, чем традиционные средства ведения войны, позволяющие решать задачи аналогичного класса;
- обеспечивать скрытность развертывания, применения и др.

К основным разновидностям психологического оружия можно отнести оружие (табл. 4.6, рис. 4.52) [433, 437, 438]:

- информационно-психологическое;
- лингвистическое;
- психотронное;
- психофизическое;
- психотропное;
- соматопсихологическое.

Табл. 4.6. Классификация типов психологического оружия [433, 437]

Тип оружия	Характеристика
Информационно-психологическое	Информация со средствами ее производства, презентации и распространения, структурированная для обеспечения ее некритического восприятия в качестве побудителя и регулятора поведения объектами воздействия
Лингвистическое	Языковые единицы и специальная юридическая и дипломатическая терминология, обороты речи, имеющие семантическую неоднозначность при переводе на другие языки, предназначенные, главным образом, для использования специалистами при ведении международных переговоров, составлении, подписании и выполнении договоров между сторонами

Психотронное	Технические средства, способные генерировать и направленно излучать электромагнитные волны и другие поля, нарушающие биоэлектрические процессы головного мозга и периферической нервной системы и вызывающие нарушения физического состояния человека и сбои в его психической деятельности
Психофизическое	Совокупность методов и средств (технотронных, суггестивных, психотропных, комплексных и др.) скрытого насильственного воздействия на подсознание человека с целью модификации его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении
Психотропное	Фармакологические препараты, наркотические вещества, химические составы, воздействующие на биохимические процессы в нервной системе человека и задающие уровни его бодрствования, активности, качества восприятия обстановки, характеристики психического здоровья
Соматопсихологическое	Технические устройства, химические составы и биологические рецептуры, вызывающие изменение в соматическом состоянии и физической активности людей и на этой основе стимулирующие развитие астенических психических состояний и импульсивных моделей поведения.

Более подробно эти типы психологического оружия рассмотрены в работе [462], здесь же дадим краткую характеристику этим типам оружия.

Лингвистическое оружие. Лингвистические средства (языковые единицы, специальная терминология, обороты речи, имеющие семантическую неоднозначность при переводе на другие языки и др.) предназначены главным образом для использования высококвалифицированными специалистами при ведении международных переговоров, подписании и выполнении договоров между сторонами. Данные средства могут обеспечить долговременный высокоэффективный результат при использовании их во время заключения международных договоров, написания текстов деклараций, законов и т.д. [437, 439].

Психотронное оружие – это средства техногенного воздействия на физическое состояние и сознание человека. Они полностью решают проблему дистанционного управления физическим состоянием человека, его психикой и сознанием. К наиболее распространенным средствам психотронного оружия относятся [433, 439]:

- генераторы электромагнитных излучений;
- генераторы инфразвука и ультразвука;
- лазерные и световые излучатели;

- генераторы специальных излучений;
- компьютерные технологии и др.

Психофизическое оружие. Средства психофизического оружия предназначены для скрытого насильственного воздействия на подсознание человека с целью модификации его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении [439].

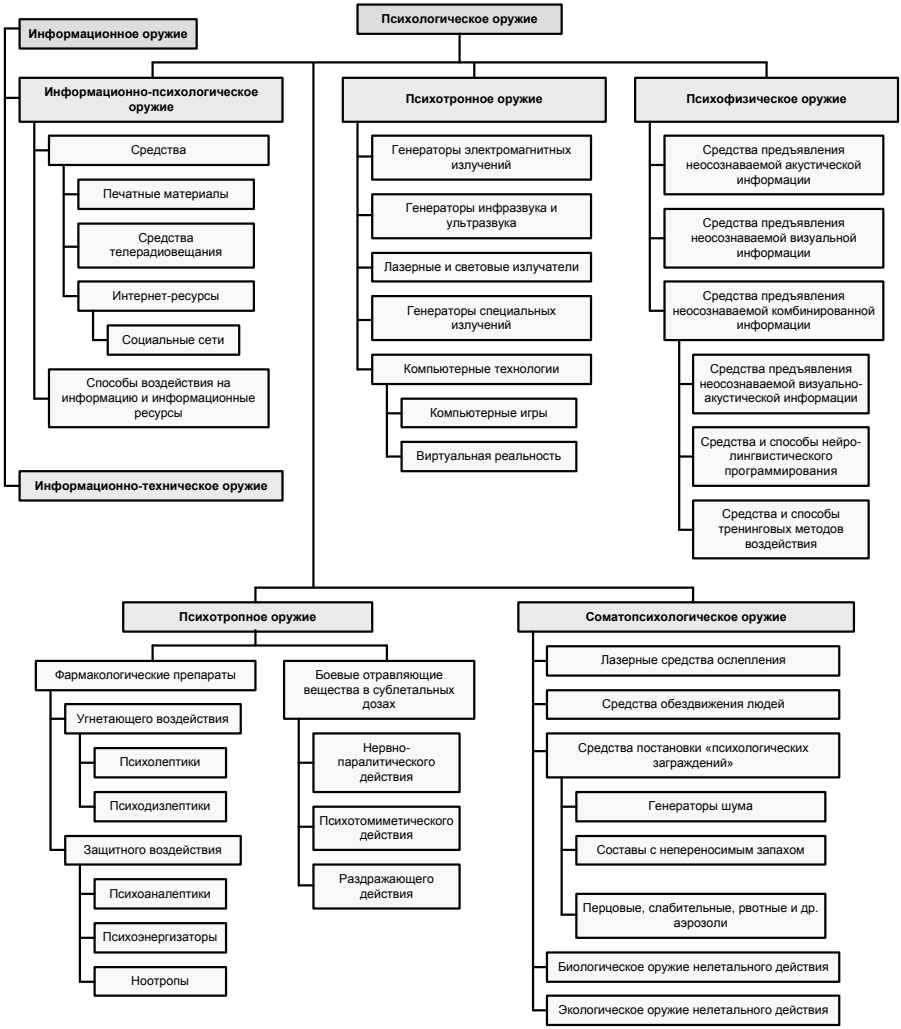


Рис. 4.52. Классификация психологического оружия [462]

Психофизические средства без ведома самого человека лишают его права самостоятельного выбора логически обоснованных решений, свободы выбора своего поведения, исполнения желаний, выражения эмоций и даже психофизиологического состояния организма (настроение, здоровье). В предельном варианте человек, испытавший психофизическое воздействие, превращается в зомби, который безотказно выполняет заложенную в него программу. Психофизические средства основаны на суггестии [439].

Суггестия (или внушение) – это целенаправленное воздействие на личность или группу (массовое внушение), воспринимаемое на уровне подсознания и приводящее либо к появлению определенного состояния духа, чувства, отношения, либо к совершению определенных поступков [439].

В результате суггестивного воздействия у объекта внушения возникает склонность подчиняться и изменять поведение не на основании разумных, логических доводов или мотивов, а по одному лишь требованию или предложению, исходящему от другого внушающего лица. При этом сам человек не отдает себе отчета в такой подчиняемости, продолжая считать свой образ действия как бы следствием собственной инициативы или собственного выбора.

Наиболее распространенными являются такие типы психофизического оружия основанные на различных видах суггестии, как средства предъявления [435, 439]:

- неосознаваемой акустической информации;
- неосознаваемой визуальной информации;
- неосознаваемой комбинированной информации.

Психотропное оружие – базируется на использовании механизма изменения биохимических характеристик процессов нервной системы человека, посредством введения в его организм фармакологических препаратов, наркотических веществ, ядов в концентрациях, вызывающих необходимые психические реакции, состояния и поведение [433].

Те группы психотропных веществ и составов, которые с наибольшей вероятностью могут быть привлечены для использования в ходе войны приведены в табл. 4.7.

Таблица 4.7. Психотропные средства, пригодные для использования в военных целях [433]

Название средства	Назначение средства
Фармакологические препараты	
Психолептики	Лекарственные препараты, подавляюще и успокаивающе воздействующие на центральную нервную систему, а в случае увеличения дозы, препятствующие эмоционально-волевой мобилизации личного состава противника перед боем, вызывающие состояние сонливости, вялости и даже сон в процессе решения боевых задач
Психодизлептики	Вещества, дезорганизующие деятельность мозга, процессы восприятия обстановки, принятия решений, выполнения действий
Психоаналептики	Стимуляторы активности, боеспособности, стенического настроения своих войск
Психоэнергизаторы	Средства, позволяющие военнослужащим быстро восстанавливать израсходованную энергию, мобилизовать внутренние ресурсы для поддержания высокой боевой активности
Ноотропы	Препараты, способствующие быстрой адаптации воинов к сложным условиям боевой обстановки
Боевые отравляющие вещества в сублетальных дозах	
Нервно-паралитического действия	Отравляющие вещества, препятствующие осуществлению психической деятельности военнослужащего, ведущие к полной утрате возможности управлять своим поведением
Психотомиметического действия	Отравляющие вещества, дезорганизующие работу мозга, вызывающие психические расстройства, сопровождающиеся галлюцинациями, нарушениями памяти, мыслительных и эмоциональных процессов, общим психомоторным возбуждением, бредом
Раздражающего действия	Отравляющие вещества, вызывающие раздражение слизистых оболочек органов чувств военнослужащих и временно лишающие их способности ориентироваться в элементах боевой обстановки

Как видно из таблицы, психотропные средства способны решать широкий спектр задач по снижению боевых возможностей противника и оптимизации психических характеристик военнослужащих своих частей и подразделений. При этом психотропные средства могут применяться в виде аэрозолей, порошков, таблеток в газообразном состоянии [433].

В последнее время появляются новые классы психотропных средств, весьма дифференцированно воздействующих на психические функции и поведение человека, его память и умственную деятельность, повышающие устойчивость мозга к агрессивным воздействиям (нейропептиды, ноотропы и др.) [435].

Способность некоторых психотропных средств резко снижать защитные функции организма открывает широкие возможности для повышения эффективности других средств и методов информационно-психологического воздействия, в первую очередь, для манипулятивных технологий на основе психофизических и психотронных средств [435].

Психотропные средства с помощью несложных приемов могут применяться для скрытого информационно-психологического воздействия. В сложившихся сегодня условиях трудно осуществить контроль за продуктами питания и средствами гигиены, поставляемых населению. Все больше товаров ввозится из-за рубежа. Многие психотропные средства могут скрыто вводиться в организм людей через эти товары или через кожу при вдыхании аэрозолей [435].

Исходя из свойств психотропных средств, можно представить их возможности при использовании для информационно-психологического воздействия на человека [435].

Во-первых, психотропные средства модифицируют психику человека, который в большинстве случаев остается работоспособным и продолжает принимать решения, не отражающие адекватно окружающую обстановку, не соответствующие реальности. Для окружающих человека с модифицированной психикой неизвестно, что его решения и поступки неадекватны ситуации. Если такой человек является руководителем, то его решения остаются обязательными для членов руководимого им коллектива и их ошибочность становится понятной для большинства или слишком поздно, или не осознается коллективом вообще. В этом случае коллектив не связывает свои неудачи, поражения с неправильным принятием решений и считает, что все это произошло в силу каких-то иных причин [435].

Во-вторых, психотропные средства могут применяться как против конкретного человека, так и против большого количества людей. В случае применения против конкретного человека учитываются его личностные особенности и его положение в социальном коллективе. Ожидаемое изменение психики в случае применения психотропных средств может быть связано с ожидаемым изменением в поведе-

нии, поступках, действиях малых групп людей и в поведении больших социальных групп [435].

В-третьих, люди, на которых было произведено воздействие психотропными средствами, сохраняют свое соматическое (телесное) здоровье. Более того, модификация психики со временем, исчисляемом в неделях или месяцах, прекращается или автоматически, или с помощью направленного психотерапевтического воздействия [435].

Таким образом, использование психотропных средств вышло далеко за рамки психиатрической клиники. Они могут широко применяться для достижения определенных политических, экономических, военных и других целей.

Соматопсихологическое оружие. В основе соматопсихо-логического оружия лежит принцип психофизического параллелизма, определяющий взаимосвязь внутренних (психических) процессов и внешних (физических) проявлений по виду: «внутреннее проявляется во внешнем, внешнее отражается во внутреннем». Другими словами, речь идет о том, что конкретное состояние организма, тела человека во многом обусловливают его психические состояния, эмоции, мотивы и модели поведения. Следовательно, целенаправленно изменяя соматическое состояние человека можно, в известной степени, корректировать его психологические характеристики. Необходимо подчеркнуть, что к сомато-психологическому оружию следует относить только те формы воздействия на людей, которые ориентированы именно на целенаправленное изменение его психических состояний и поведения и в которых телу отводится роль средства [433].

Основные средства соматопсихологического оружия представлены в табл. 4.8 по данным работы [433].

Оружие соматопсихологической группы можно считать одним из наиболее разработанных по сравнению с другими средствами воздействия на психику людей в военных целях.

Например, психологическое действие лазера основывается на особом страхе человека перед слепотой. Так в США создан лазерный ослепитель для гранатомета, условно названный «Sabor 203». Он состоит из лазерного диода, помещенного в твердую пластиковую капсулу, и панели управления, которая посылает в нее импульсы. Нажатием кнопки на панели управления стрелок переводит лазер в режим непрерывного излучения, что позволяет ослепить противника ярко-красным световым лучом. По мнению создателей установки, она имеет эффективную дальность действия до 300 м. В Сомали американцы испытали этот вид сомато-психологического оружия на гражданском

населении. Направленный в толпу враждебно настроенных местных жителей лазерный луч ослепителя вызвал среди них панику [439].

Таблица 4.8. Основные средства соматопсихологического оружия [433]

Название оружия	Краткая характеристика оружия
Лазерное оружие	Лазерные генераторы и устройства, применяемые для временного ослепления военнослужащих войск противника
Средства обездвижения людей	Быстрозатвердевающие суперклеевые составы, распыляемые над войсками противника и приклеивающие людей к боевой технике, почве, друг к другу. Суспензии, многократно снижающие коэффициенты трения и делающие невозможными передвижения людей и боевой техники, что порождает чувства бессилия, страха, отчаяния
Средства постановки «психологических заграждений»	Генераторы трудноперенесимого шума, составы с непереносимым запахом, перцовые, слабительные, рвотные и другие аэрозоли, распыляемые над определенной территорией и создающие условия, невозможные для пребывания на ней войск противника и других людей
Биологическое оружие нелетального действия	Микроорганизмы, искусственно выведенные насекомые, вызывающие недомогания (плохое самочувствие, чесотку, нестерпимый зуд, обширные язвы и др.) и заболевания, препятствующие ведению войсками противника активных боевых действий и способствующие их деморализации
Экологическое оружие нелетального действия	Средства создания и поддержания в течении длительного времени погодно-климатических условий, крайне неблагоприятных для жизнедеятельности войск противника

Отдельные виды соматопсихологического оружия (акустические, перцовые, слезоточивые и др. средства) давно и широко используются в практике проведения военно-полицейских операций против повстанцев, для разгона несанкционированных митингов и демонстраций во многих странах. Также отмечаются факты применения против мирного населения так называемых мягких средств воздействия – воздушных и водяных пушек, действие которых носит явно выраженный психологический эффект [433].

В качестве примера можно привести средство LRAD – устройство испускающие звуковые импульсы, которые вызывают у людей сильное головокружение и тошноту. Установка весит порядка 20 кг, имеет антенну полусферической формы диаметром около 1 м и внешне похожа на прожектор или локатор. Она производит узконаправленный пронзительный звук высокой частоты, похожий на вой пожарной сирены, но гораздо громче. Громкость LRAD достигает 150 дБ и может даже повредить слуховой аппарат человека (для сравнения: у пожарной сирены 80-90 дБ). При этом частота звуковых колебаний составляет 2100-3100 Гц. Но такие характеристики звук имеет только внутри узкого луча, так что звуковой удар не вредит оператору, а поражает только врагов. LRAD воздействует на противника силой звука, оглушая его и вызывая болевой шок [436].

Естественно, не могут не сказаться на настроениях, впечатлениях, боевой активности и случаи применения противником других видов нелетального оружия, сопровождающихся остановкой и «омертвением» боевой техники, выходом из строя систем связи и управления, приборов наблюдения и разведки. Однако в этом случае психологический эффект будет носить побочный характер и не рассматривается в качестве основной цели использования данных средств [433].

4.6.4.3. Информационно-психологическое оружие

Информационно-психологическое оружие – средства и способы воздействия на потенциального противника за счет манипуляции информацией в интересах формирования элит с заданным мировоззрением, привития населению определенных ценностей и стереотипов, позволяющих, с одной стороны, прогнозировать его поведение и играть на внутренних противоречиях, а с другой – влиять на процессы принятия решений на всех уровнях управления.

Анализ ведения на современном этапе психологических операций в рамках информационного противоборства позволяет выделить несколько основных тенденций развития средств информационно-психологического оружия и способов его применения, которые в ближайшем будущем будут определять его сущность и характер [432].

К основным средствам информационно-психологического оружия получившим широкое распространение можно отнести [432, 433]:

- печатные материалы – листовки, плакаты, информационные бюллетени и др., средства их производства (полиграфическая база) и распространения;
- средства массовой информации – газеты, радио и телевидение;
- интернет-ресурсы и социальные сети;
- когнитивное оружие.

Ниже данные средства рассмотрены более подробно.

Средства массовой информации (СМИ) – включают в себя расширенный функционал способов воздействия на психику индивида и масс с целью внедрения в подсознание психологических установок и формирования паттернов поведения в бессознательном психики. К средствам массовой информации относятся: телевидение, пресса, радио, театр, цирк, все зрелищные мероприятия и литература, видеофильмы, щитовая реклама и реклама на транспорте, звукозаписи и видеозаписи и т. п., с помощью чего можно воздействовать на массовую аудиторию. Из всех этих СМИ наивысшей эффективностью обладает телевидение [432].

При просмотре телепередач любой направленности у человека работает преимущественно правое полушарие головного мозга. Правое полушарие мыслит образами и отвечает за комплексное видение мира, то есть компонует отдельные кадры увиденного в единую целостную композицию. При этом отключается работа левого полушария с его аналитическим мышлением. Таким образом, вся увиденная посредством просмотра телевизора информация беспрепятственно проникает в подсознание, где формирует соответствующие психологические установки и паттерны поведения. Кроме того, нужная информация обязательно часто повторяется. Повторение резко усиливает силу внушения, низводя в итоге поведение многих людей до уровня обычных рефлексов нервной системы [432].

Особую опасность представляет телевидение для детей. В отношении манипулятивного воздействия, направленного на детей, следует говорить, что у детей в силу возраста не сформирован навык осмысления информации, которая подается посредством телепоказа [432].

Не меньшую опасность телевидение представляет оказывая воздействие на психику взрослых людей. Телевидение с его огромным

потоком зрительной информации, быстрой сменой изображений не дает возможность вернуться назад и еще раз просмотреть недостаточно понятые кадры, а значит – осмыслить их. Во время просмотра телепередачи мозг зрителей подключается к единой системе, которая посредством видеозвуковых знаков и символов формирует соответствующие психологические установки в подсознании человека. Таким образом, зрители начинают мыслить в заданных манипуляторами алгоритмах [432].

Смонтированные и отретушированные в подразделениях ПсО репортажи «с места событий» позволяют создавать атмосферу массового психоза, способствовать дестабилизации обстановки в мире, формировать соответствующее мировое общественное мнение. Основными способами манипулирования информацией, используемыми СМИ, являются:

- откровенная ложь в целях дезинформации;
- сокрытие критически важной информации;
- погружение ценной информации в массив информационного мусора;
- упрощение, утверждение и повторение (внушение);
- подмена терминологии: применение понятий и терминов, смысл которых неясен или претерпел качественные изменения, что затрудняет формирование реальной картины события;
- введение запрета на определенные виды информации и разделы новостей;
- узнавание образа: известные политические деятели, представители шоу-бизнеса могут участвовать в заказных политических акциях, оказывая тем самым определенное влияние на мировоззрение их поклонников;
- подача негативной информации, которая лучше воспринимается аудиторией по сравнению с позитивными новостями.

Телевидение и другие СМИ (радио, кинематограф, газеты, журналы и проч.) своей деятельностью изменяют привычки людей, вводя им в подсознание новые установки, инициируемые агентами влияния [432].

Средства на основе интернет-ресурсов и социальных сетей. В интересах психологических операций все активнее и масштабнее применяются электронные СМИ, а также глобальная компьютерная сеть Интернет. Диапазон использования сети Интернет весьма широк.

Он предоставляет широкие возможности для оказания влияния на формирование общественного мнения, принятия политических, экономических и военных решений, воздействия на информационные ресурсы противника и распространения специально подготовленной информации (дезинформации) [95].

Существенные преимущества использования сети Интернет перед обычными средствами обусловлены следующими факторами представленными в работах [95, 440].

1. Оперативность. Размещение и регулярное обновление информации на отдельных страницах, в интернет-изданиях и различного рода новостных рассылках, форумах и конференциях требуют минимальных затрат времени на подготовку материалов. При этом пользователи получают ее в режиме реального времени, а целенаправленное воздействие на информационные ресурсы противостоящей стороны может осуществляться не только в заранее запланированное время, но и по мере возникновения необходимости.

2. Экономичность. Для решения поставленных задач привлекается минимальное количество персонала и материальных средств. Кроме того, применение компьютерных технологий для вывода из строя систем управления противника при определенных условиях может привести к более значительному эффекту при существенно меньших затратах по сравнению с использованием традиционных средств огневого поражения и радиоэлектронной борьбы.

3. Скрытность источника воздействия. Поскольку акт агрессии в глобальной сети трудно, а порой невозможно отличить от обычных несанкционированных действий, то подготовить и провести психологическую операцию с использованием ресурсов сети Интернет может достаточно широкий круг лиц – от специальных структур иностранных государств до партизанских формирований.

4. Дистанционный характер воздействия на информационные системы в различных регионах мира. Для осуществления информационно-психологического воздействия не обязательно находиться непосредственно в месте воздействия. Удаленно комментируя местные новостные каналы, манипулируя подачей и эмоциональным восприятием информации можно обеспечить целевое информационно-психологическое воздействие в заданном месте и в заданное время из любого места Земли.

5. Масштабность возможных последствий. Использование глобальной сети для деструктивных информационно-психологических воздействий может привести к нарушению нормальной работы орга-

нов государственного и военного управления, спровоцировать масштабные протесты, акции гражданского неповиновения в отдельных районах, странах либо регионах.

6. Комплексность подачи информации и ее восприятия. Текстовая и графическая информация на интернет-страницах размещается в наиболее удобном для восприятия виде, а ее объем может быть во много раз больше, чем у любого печатного издания, радиопередачи или телевизионной программы. Помимо того использование современных мультимедийных технологий, позволяющих демонстрировать документальные свидетельства и факты, фото- и видеоматериалы при специально подобранном сопровождении (комментарии, музыка), оказывает на пользователей дополнительное эмоциональное и психологическое воздействие.

7. Доступность информации. По имеющимся данным, общее количество пользователей Интернета к началу 2015 г. составляет около 3,3 млрд человек. Эти люди практически мгновенно могут получить доступ к информации, имеющейся на серверах различных стран, минуя пограничные, цензурные и иные барьеры. При этом любой пользователь может разместить собственную информацию на серверах, зарегистрированных в других государствах, или организовать рассылки сообщений по всему миру. После цветных арабских революций в СМИ активно продвигалась мысль о том, что эти события стали возможными, в том числе исключительно благодаря новейшим интернет-технологиям информационно-психологического воздействия.

Таким образом, можно приписывать Интернету большую или меньшую зависимость в современных психологических операциях, но отрицать ее невозможно [95].

Социальные сети в сети Интернет являются новым современным инструментом, используемым в интересах активации протестных настроений, координации действий протестующих, информирования международной общественности о происходящих событиях [432].

Информационные потоки из социальных сетей Facebook и Twitter посредством рассылки сообщений о протестных акциях на электронную почту и мобильные телефоны пользователей позволяют собирать критическую массу людей в нужное время и в нужном месте [432].

По оценке специалистов, общение в сетях Facebook или Twitter создает у людей чувство сопричастности, а выкладывание фотографий или видеороликов обеспечивает эффект присутствия. Благодаря этому о событиях мгновенно узнают миллионы людей за рубежом, которые

могут включиться в борьбу, потребовав от своих правительств решительных действий в поддержку той или иной противоборствующей стороны [432].

Таким образом, вовлечение населения в социальные виртуальные сети является новым перспективным методом манипулирования сознанием людей, позволяющим мобилизовать граждан на нужные действия, находясь вдалеке от эпицентра событий [432].

В настоящее время в США разработана программа по управлению личностями (Persona Management Software), с помощью которой можно создавать и управлять фиктивными аккаунтами социальных сетей, чтобы искажать правду и создавать впечатление, будто существует общепринятое мнение по спорным вопросам. Программа позволяет небольшому числу людей сообщать и пропагандировать ложные сведения, создавая при этом за счет большого числа фиктивных пользователей впечатление всеобщего их признания. С помощью программы можно также следить за общественным мнением и находить подлинные точки зрения, чтобы затем с помощью «фиктивных» людей проводить грязные кампании по искажению этих точек зрения и дискредитации «реальных» людей, их исповедующих [432].

Кроме того, в современном мире дезинтеграция государственности происходит в результате деятельности транснациональных медиакорпораций (ТНК-медиа), осуществляющих трансграничную деятельность через многоступенчатую сеть филиалов, дочерних предприятий, аффилированных компаний и других ресурсов. Будучи взаимосвязанными с международными политическими и экономическими структурами, ТНК-медиа способствуют ослаблению национальной роли и самоидентичности государств-противников посредством информационно-психологического воздействия. Для воздействия на принятие решений государственными и межгосударственными структурами ТНК-медиа используют, например, информационное давление или контроль «глобальной политической повестки дня». Для этого они стремятся приобретать наиболее популярные интернет-ресурсы, социальные сети и другие медиа. В результате возрастает их «информационная сила», под которой понимается бесконечный, но управляемый поток информационных ресурсов в сфере глобальной политики и международных отношений. Воздействие этой силы способно привести к дезинтеграции общества, децентрализации государственной власти, виртуализации жизни, асимметрии между экономической и политической сферами социума, революции в средствах обеспечения безопасности [432].

Политики США, которые только в феврале 2011 г. выделили 25 млн долларов на поддержку блогеров и интернет-активистов в авторитарных странах, подчеркивают значимость этого явления. По результатам исследования на предмет активности интернет-пользователей в странах Арабского Востока утверждается, что только за год – с февраля 2010 по февраль 2011 г. – число посещений наиболее популярных на Ближнем Востоке интернет-ресурсов (Facebook, Google и Youtube) увеличилось на 233%. В этот же период наибольший рост пережил уровень обмена информацией – объем переданных данных увеличился на 259% [95].

В целях достижения перечисленного США противодействуют попыткам ряда стран передать Интернет под контроль какой-либо международной организации, например ООН, а в 2011 г. госдепартамент планировал открыть микроблоги на сайте «Твиттер» на китайском, русском языках и хинди [95].

Американская администрация считает, что формирование единой глобальной информационной инфраструктуры под контролем США позволит им решить задачу стратегического использования информационно-психологического оружия «...вплоть до блокирования телекоммуникационных сетей государств, не признающих реалии современной международной системы» [95].

Таким образом, аналитики Пентагона признают, что в войне будущего маневр на «информационном поле боя» может занять главенствующее место по отношению к маневру силами и средствами вооруженной борьбы. При этом необходимо отметить, что в настоящее время применение информационных технологий в военных целях фактически не регулируется международным правом [95].

Когнитивное оружие. Отдельным подтипом информационно-психологического оружия является когнитивное оружие, которое несколько отличается по своему воздействию от вышерассмотренных типов.

Когнитивное оружие – это внедрение в интеллектуальную среду страны-противника ложных научных теорий, парадигм, концепций, стратегий, влияющих на ее государственное управление в сторону ослабления оборонно-значимых национальных потенциалов [432].

В практическом применении ложные научные теории, парадигмы, концепции, стратегии превращаются в оружие огромной разрушительной силы, поражающее национальную науку и образование, государственное управление, экономику, оборону [432].

Примерами когнитивного оружия являются: теория постиндустриализма; теория монетаризма; теория радикального либерализма в экономике; концепция опережения производительности труда по отношению к оплате труда (в условиях заниженной оплаты труда); миграционная тематика; тематика реорганизации контура образования и др. Кроме того, наряду с ложными политически-экономическими теориями специалистами по психологическим операциям может осуществляться вброс ложных сведений о тенденциях в развитии современной науки вообще и военной науки в частности с целью направить научные исследования по неверному пути [432].

4.6.4.4. Средства информационно-психологического воздействия в военных конфликтах (на примере средств ВС США)

К основным средствам информационно-психологического воздействия в военных конфликтах относятся:

- средства распространения листовок и других печатных материалов;
- средства телерадиовещания.

Рассмотрим эти средства более подробно на примере средств используемых в ВС США.

Средства распространения листовок и других печатных материалов. Специалистами аппарата психологических операций вооруженных сил США разработано большое количество способов и технических средств доставки материалов печатной пропаганды до избранных объектов психологического воздействия. Простейшими способами их распространения являются, во-первых, сброс листовок с низколетящих вертолетов и самолетов, во-вторых – раздача листовок военнослужащими частей ПсО непосредственно избранным объектам. К техническим средствам распространения материалов печатной пропаганды относятся: специальные авиационные бомбы, авиационная тара, парашютные контейнеры, воздухоплавательные летательные аппараты (парапланы, аэростаты, воздушные змеи и шары), артиллерийские боеприпасы, гранаты, мины, плавучая тара [441].

Согласно наставлению СВ США по проведению ПсО способы распространения материалов печатной пропаганды (листовок, брошюр, газет и т.п.) подразделяются [441]:

- на наземный (распространение военнослужащими, в том числе ССО, агентами среди местных жителей);

- на воздушный (авиабомбы, авиационная тара, парашютные контейнеры, воздухоплавательные ЛА, разброс непосредственно экипажами летательных аппаратов);
- на морской (плавучая тара);
- на артиллерийский (снаряды, гранаты, мины).

Несмотря на разнообразие современных технических средств распространения печатных материалов информационно-психологического воздействия, в руководящих документах ВС США раздача военнослужащими листовок и другой пропагандистско-печатной продукции расценивается как «один из лучших и самых эффективных способов воздействия на объекты ПсО». Раздача материалов информационно-психологического воздействия населению страны пребывания позволяет не только установить с ним доверительные отношения, но и немедленно оценить эффективность печатной пропаганды, ее приемлемость для данных адресатов [441].

Личный состав сил специальных операций, действующий за линией фронта, в тылу, на территории противника, также участвует в распространении материалов информационно-психологического воздействия в местах скопления группировок войск противника, на маршрутах их предполагаемого движения, сосредоточения и развертывания. К аналогичным мероприятиям могут привлекаться представители резидентур, повстанческих группировок и мирные жители, завербованные или пожелавшие сотрудничать с военнослужащими ВС США. Практиковалось распространение листовок и других печатных материалов и отступающими войсками в расчете на то, что оставленные ими позиции будут заняты противником и до личного состава его войск дойдет хотя бы небольшая часть пропагандистских материалов [441].

Средства телерадиовещания. Авиационные средства телерадиовещания. В локальных конфликтах последнего десятилетия с участием США значительно возросла роль психологических операций, направленных на деморализацию войск противника и гражданского населения. Результат достигался путем целенаправленного влияния на сознание и образ мышления людей. Образ мыслей современного человека весьма зависим от масс-медиа: телевидения, радио, печатных изданий. Поэтому при создании средств ведения психологической войны именно на них и делается ставка. Таким образом, основным оружием ПсО являются радио- и телепередатчики, установленные на мобильных средствах. Из последних наиболее гибким и удобным оказался специализированный самолет. Он способен оперативно прибыть в

нужный регион и автономно действовать там длительное время, располагает мощной силовой установкой, часть энергии которой можно использовать для питания электронной аппаратуры. А главное, действуя с большой высоты, он является не только «крылатой телерадиостудией», но и «летающей антенной», обеспечивающей хорошее покрытие сигналом даже в условиях сильно пересеченной местности [443].

Такие специализированные самолеты появились в конце 80-х годов в США. В качестве носителя теле- и радиовещательного оборудования был выбран транспортный самолет С-130 Самолет ПсО получил индекс ЕС-130Е RR и наименование «Rivet Raider», однако оно не прижилось и вскоре повсеместно (в т.ч. на официальном уровне) изменилось на «Commando Solo». Такое наименование, по мнению экипажей, лучше отражает специфику применения: «Commando» указывает на принадлежность к силам специальных операций, а «Solo» – на то, что самолет всегда действует в одиночку [443].

Самолет ЕС-130Е в средине 90-х прошел несколько модернизаций и в нынешнем варианте «Commando Solo II» имеет комплекс аппаратуры для радиовещания в широком спектре частот и трансляции телепрограмм в общемировом цветном формате WWCTV. Шесть передатчиков, работающих в диапазоне от 450 кГц до 350 МГц, излучают сигналы с помощью девяти передающих антенн, установленных по всему самолету. Так, продольная проволочная антенна над фюзеляжем обеспечивает максимальную мощность радиовещания в боковых направлениях, а комплекс из четырех телевизионных антенн на киле – вниз. Выпускаемая из хвостового отсека приемопередающая антенна переменной длины предназначена для особо точной настройки параметров сигналов – от этого, в частности, сильно зависит качество телевизионного вещания. Восемь радиоприемников работают в еще более широком диапазоне – от 200 кГц до 1000 МГц. Улавливаемое ими излучение поступает на четыре анализатора спектра частот, определяющих параметры принятых сигналов и позволяющих с высокой точностью настроить собственные передачи на частоту работающих радио- и телецентров противника. В состав оборудования входят также две связных радиостанции (AN/ARC-186 и AN/ARC-164) с аппаратурой засекречивания KY-58 и система пеленгации работающих станций противника [443].

В качестве оборонительных средств на самолете ЕС-130Е Commando Solo установлена аппаратура предупреждения об облучении РЛС противника AN/AAR-47 с системой отстрела ловушек для

защиты от ракет как с тепловыми, так и с радиолокационными головками самонаведения и генераторы инфракрасных помех AN/ALQ-157. Оборудование для дозаправки в полете позволяет находиться над зоной вещания по 10-12 часов непрерывно [443].

Экипаж состоит из двух пилотов, штурмана, офицера – руководителя ПсО и семи специалистов: инженера, специалиста по радиоэлектронному оборудованию и пяти операторов [443].

Как правило, самолеты EC-130E «Commando Solo» прибывали в зону назревающего конфликта еще до начала военной фазы, чтобы в спокойной обстановке определить рабочие частоты военных линий связи и вещательных теле- и радиостанций противника. После изучения местных особенностей формировалась общая стратегия психологических операций, и в наземных студиях готовились конкретные, направленные на определенные социальные группы передачи. Затем они транслировались на всех языках, на которых говорят в данном регионе [443].

Самолеты EC-130E Commando Solo обычно ведут вещание с максимальной высоты, летая по замкнутой эллиптической траектории. Этим достигается наилучшее покрытие сигналом, так как наиболее мощно излучение направлено вниз и в стороны от самолета. Если бы было возможно огневое противодействие противника, то зоны вещания располагались вдоль границ, вне досягаемости средств ПВО (Югославия, Ирак). При отсутствии угрозы (Панама, Гаити, Афганистан) самолеты действовали непосредственно над территорией страны. Заняв эшелон в зоне, EC-130E включает приемники и выпускает хвостовую антенну. После точной настройки на диапазоны, используемые вооруженными силами и местным телерадиовещанием, Commando Solo начинает трансляцию собственных передач, причем сразу на нескольких волнах. Вещание ведется в прямом эфире, в записи либо во время ретрансляции телевизионного сигнала в режиме реального времени [443].

За время своего существования 193-я эскадрилья ВВС США оснащенная EC-130E «Commando Solo» успела поработать над большинством известных горячих точек. В операции «Буря в пустыне» (1991 г.) самолеты EC-130E обрабатывали иракцев с двух сторон одновременно – из Турции и Саудовской Аравии. Их программы, известные как «Голос Персидского залива», способствовали массовой сдаче в плен иракских солдат [443].

В 1994 г. EC-130E «Commando Solo» использовались во время операции по поддержке демократии в Гаити, где вели вещание для

гражданского населения. Психологические операции с участием самолета EC-130E проводились также в Гренаде, Панаме, Югославии и Косово [443].

За время боевых действий в Ираке в 2003 г. было выполнено 58 вылетов EC-130E «Commando Solo», организовано соответственно 306 и 204 ч радио- и телевещания, а для трансляции записано более 100 радиопрограмм [444].

В Афганистане EC-130E «Commando Solo» интенсивно применялись для информационно-психологического воздейтсвия на афганцев после двух недель интенсивного огневого воздействия. В передачах между музыкой и новостями ненавязчиво внедрялись мысли о неизбежном поражении талибов и просьбы держаться подальше от их позиций и военных объектов. При этом бортовые телепередатчики здесь не использовались – Талибан запретил телевидение еще в 1996 г. как противоречащее Корану [443].

Кроме своего прямого назначения – ведения психологических операций, самолет EC-130E «Commando Solo» можно использовать в качестве самолета радиоэлектронной разведки и РЭБ, для нарушения работы систем связи, телевидения и радиовещания противника. Кроме того, эти самолеты вполне могут применяться и для сугубо гражданских целей – обеспечения местного вещания в случае стихийных бедствий и катастроф, доведения до пострадавшего населения инструкций и рекомендаций по эвакуации и т.п., временной замены региональных масс-медиа либо расширения спектра их вещания [443].

В 1998 г. США решили пополнить парк 193-й эскадрильи, состоявшей на тот момент из четырех EC-130E «Commando Solo II». На основе «Геркулеса» нового поколения – C-130J, получившего новые высокоэкономичные двигатели и суперсовременную авионику [443].

Самолет EC-130J «Commando Solo III» является первой модификацией, разработанной на базе планера C-130J для решения задач в ходе специальных операций. Он предназначен для информационно-психологического воздействия на живую силу противника путем радиовещания в диапазонах УКВ, КВ и СВ, в том числе в сетях министерства обороны противника, а также для трансляции телепрограмм в общемировом цветном формате WWCTV в ОВЧ- и УВЧ-диапазонах. Другие задачи включают в себя противодействие сетям управления и ограниченное ведение разведки. Кроме решения военных задач, этот самолет может быть использован для стабилизации обстановки при возникновении чрезвычайных ситуаций, например природных катастроф [445].

Первый EC-130J был построен в 2000 г. на предприятии компании «Локхид-Мартин» на базе военно-транспортного самолета C-130J, поступившего в распоряжение ВВС США в октябре 1999 г. Самолет EC-130J «Commando Solo III» можно идентифицировать по двум подкрыльевым блокам размером 7,01×1,82 м, в которых размещены антенны широковещательных телепередатчиков ОВЧ- и УВЧ-диапазонов. На киле находятся четыре характерных обтекателя телеантенн более низких частот. Самолет оснащен системой дозаправки в воздухе и более совершенной системой электропитания. Получая питание от установленных на двигателях генераторов, оборудование EC-130J позволяет вести трансляцию одновременно на восьми частотах [445].

Первые три машины унаследовали оборудование от своих предшественников EC-130E. Первый укомплектованный EC-130J был поставлен на вооружение в сентябре 2004 г. Следующие четыре самолета перед укомплектованием электронным оборудованием были доработаны на заводе компании «Локхид-Мартин» до так называемой конфигурации «Супер J». На них были установлены штанга дозаправки топливом в воздухе, усовершенствованные автоматизированные рабочие места операторов бортового оборудования, самолетное переговорное устройство и более мощные генераторы переменного тока с изменяемой в диапазоне от 60 до 90 кВА мощностью. Бортовое радиоэлектронное оборудование (БРЭО) исполнено по модульной схеме, позволяющей осуществлять обмен элементами оборудования между самолетами [445].

Последний самолет EC-130E «Commando Solo II» был списан в 2006 г., и в настоящее время в строю находятся семь EC-130J «Commando Solo III». При выполнении психологических операций в небе над Ираком начиная с середины 2007 г, эти самолеты за восемь месяцев налетали в общей сложности около 1350 ч [445].

В состав экипажа EC-130J входят десять членов: два летчика, оператор бортовых систем, оператор целевого оборудования, старший по погрузочно-разгрузочным работам и пять операторов электронных систем связи.

Бортовой комплекс обороны включает РЛС предупреждения об облучении ALR-56M, систему предупреждения об облучении пассивными средствами наведения УР AAR-54, автомат отстрела дипольных отражателей ALE-47 и блок отстрела ИК-ловушек AAQ-24 [445].

В бюджете МО США на 2011 финансовый год было заложено 6,7 млрд долларов на модернизацию средств ПсО в течение пяти лет.

При этом значительная часть данной суммы предназначена для обновления парка машин типа С-130 путем поставок самолетов новых модификаций [445].

Как показал опыт применения самолетов психологических операций ЕС-130 «Commando Solo», они по своей боевой эффективности не уступают стратегическим бомбардировщикам. Боевое применение В-1, В-52 и даже В-2 просто приводит к гибели солдат и офицеров, к чему на войне быстро привыкают. Передачи же ЕС-130Е (J) сокрушают веру в цели борьбы и грядущую победу, без которой любая воюющая сторона теряет волю к сопротивлению [443, 445].

В настоящее время планируется расширение авиационных средств ведения ПсО и использование для этих целей БПЛА. Так в интересах проведения ПсО планируется использовать беспилотный летательный аппарат вертолетного типа S-100. Этот БПЛА может задействоваться для распространения листовок, ретрансляции теле- и радиосигнала, а также для ведения сеансов звуковещания. В стандартной конфигурации S-100 способен находиться в воздухе с полезной нагрузкой массой 35 кг в течение 6 ч. Дальность полета без дозаправки составляет 200 км. БПЛА может выполнять задачи по заранее заложенной программе, а также по командам оператора [446].

Наземные средства телерадиовещания. Кроме авиационных средств телерадиовещания в интересах ПсО используются и наземные средства. В частности, к таким средствам относятся мобильные комплексы телерадиовещания SOMS-B (Special Operations Media System B), успешно применяемые ВС США в Ираке и Афганистане. Комплекс SOMS-B включает в себя два основных модуля [441]:

- мобильной системы радиовещания (Mobile Radio Broadcast System);
- мобильной системы телевещания (Mobile Television Broadcast System).

Каждый из этих модулей смонтирован на двух бронемашинах HMMWV «Хаммер»: аппаратной и грузовой. Кроме того, в состав каждого модуля входит прицеп с генератором мощностью 30 кВт, блок контроля окружающей среды и сборный комплект тентов. Модули полностью автономны и могут использоваться как вместе, так и по отдельности. Аппаратная часть комплекса SOMS B обеспечивает теле- и радиовещание в СВ-, КВ- и УКВ- диапазонах [441].

4.7. Средства радиоэлектронной борьбы

Важным и исторически развитым направлением информационных операций является противоборство с системами управления противника за счет использования средств радиоэлектронной борьбы. В связи с этим данное направление развития информационного оружия рассмотрено отдельно.

4.7.1. Роль и способы применения средств радиоэлектронной борьбы в сетецентрической войне (на примере ВС США)

Анализ оперативных учений, локальных войн и вооруженных конфликтов последних лет позволяет сделать вывод о том, что радиоэлектронная борьба в вооруженных силах США прочно утвердилась как одно из важных средств информационного противоборства. Она стала неотъемлемой частью вооруженной борьбы и информационных операций [95].

Опыт проведения учений и участия вооруженных сил США в вооруженных конфликтах показал, что даже подавляющее превосходство в области высокоточного оружия не гарантирует благоприятного исхода операции в том случае, если системы управления различного уровня управления оставались неподавленными [95, 256].

Объектами первоочередного воздействия РЭБ в ходе операции являлись [95]:

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

Аналитики Пентагона полагают, что основными причинами повышения роли РЭБ в современных сетецентрических войнах являются [95, 256]:

- возрастание факторов своевременности и устойчивости управления войсками и оружием в ходе боевых действий;

- рост масштабов использования радиоэлектронных средств различных типов для передачи информации на значительные расстояния в целях оперативного, непрерывного и гибкого управления войсками и оружием;
- возможность практически мгновенно дезорганизовать средствами РЭП процессы боевого управления противника и тем самым обеспечить коренное изменение соотношений сил в свою пользу;
- повышение маневренности вооруженных сил, увеличение масштаба глубины проведения операций, автоматизация всех процессов управления (войсками, боевой техникой и оружием);
- создание функциональных интегрированных систем управления, разведывательного обеспечения, РЭБ и ВТО привели к количественному перераспределению в операции ударных и обеспечивающих сил. Так, по заключению экспертов, в операциях начала XXI в. 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 полувековой путь эволюционного развития РЭБ существенно изменилось 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 сети ЭВМ противоборствующей стороны и воздействовать на них [95].

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 в. 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 [95, 231].

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» (CyberWar), «ведение боевых действий и управление вооруженными силами в едином информационно-коммуникационном пространстве». Все эти термины предполагают организацию управления вооруженными силами 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 [95].

В настоящее время аналитиками Пентагона отмечается, что в современных условиях именно РЭБ является основой информационного противоборства [95].

Анализ эволюции РЭБ в ВС США и ОВС НАТО позволил выявить возникшие в последние годы различия между характером, содержанием мероприятий и ролью РЭБ, которые сводятся к тому, что [256]:

- РЭБ ВС США и ОВС НАТО имеет различные объекты воздействия и защиты. Если мероприятия РЭБ вооруженных сил ряда государств связаны только с воздействием на радиоэлектронные средства противника, то в ВС США, а в перспективе и ОВС НАТО они направлены на воздействие и защиту РЭС, а также распространяются на боевую технику, объекты ВС и системы оружия. В рамках проведения мероприятий РЭБ в американских вооруженных силах уже

сегодня кроме использования источника излучения электромагнитной энергии противорадиолокационных ракет предусматривается задействование других видов летального и нелетального оружия, базирующегося на излучении направленной энергии. Одной из основных целей радиоэлектронной атаки РЭБ ВС США является преодоление системы ПВО противника;

- в мероприятиях РЭБ ВС США имеется такой самостоятельный элемент, как радиоэлектронное обеспечение операции (боевых действий), который отсутствует в подобных мероприятиях ВС ряда других государств НАТО;
- мероприятия РЭБ ВС США и ОВС НАТО являются основой противодействия системам боевого управления, то есть РЭБ 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 оружия [95].

Анализ эволюции характера, содержания и роли РЭБ в операциях конца XX – начала XXI века дает возможность вскрыть и сформулировать основные тенденции развития РЭБ ВС США и ОВС НАТО до 2025 г., наметившиеся в ходе интеграции сил и средств разведки, РЭБ и борьбы с системами боевого управления. К ним следует отнести такие [256]:

- частичная утрата самостоятельной роли РЭБ, которая становится одним из важных элементов информационного противоборства, в основном для борьбы с системами связи и управления при проведении информационных операций;
- коренное поэтапное изменение характера, содержания и роли РЭБ и операции (боя). Так, на первом этапе она явля-

лась 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 ВС 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;

При этом в ВС США практически решен, а в ВС ведущих стран НАТО поставлен на повестку дня вопрос об обеспечении полной информатизации и автоматизации процесса РЭБ.

В настоящее время в США РЭБ 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 РЭБ является признание ее комплексности и тесной связи с другими видами боевой деятельности войск [256].

Мероприятия РЭБ составляют основу новой активно внедряемой в Вооруженных силах США концепции борьбы с системами боевого управления (СССМ или С3СМ – 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» [95].

Как отмечается в программе, радиоэлектронное поле боя (Electromagnetic Field of Battle) РЭБ в ближайшем будущем претерпит значительные изменения с учетом расширения спектра используемых рабочих радиочастот РЭС, который станет более насыщенным и менее доступным для противника. Подразделения и части разведки и РЭБ нового типа, действуя в информационных операциях в составе сил информационных операций, будут способны добывать, мгновенно обрабатывать, хранить и распределять информацию, а также в масштабе времени, близком к реальному, воздействовать на противника, привлекая для этого штатные силы разведки и РЭБ наземного и воздушного базирования, а также средства разведки и РЭБ, забрасываемые на его территорию, в первую очередь роботизированные и устанавливаемые личным составом сухопутных войск [256].

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 [256].

Практическая реализация упомянутой концепции «радиоэлектронное поле боя» в информационной операции с участием сил и средств РЭБ предполагает последовательное выполнение таких четырех основных задач, как [95]:

- 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 [95].

Основными принципами ведения РЭБ в информационных операциях, по взглядам руководства США, являются [95]:

- 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, радиоэлектронное подавление, организация утечки ложной информации [95].

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 [95].

В интересах достижения решающего военно-технического превосходства средств РЭБ в США проводятся такие мероприятия, как [95]:

- создание качественно новых средств «силового» радиоэлектронного подавления, предназначенных для кратковременного и необратимого вывода из строя информационных и радиоэлектронных систем 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 в направлении повышения чувствительности приемников, увеличения пропускной способности и быстродействия аппаратуры, а также точности определения частоты подавляемой РЭС;
- совершенствование технических характеристик средств радиоэлектронного подавления.

Доктринальными документами ВС США определены следующие основные задачи РЭБ в информационной операции, такие как [95]:

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

В перечне задач выделяется воздействие не только на радиоэлектронные средства, но и на боевую технику, системы оружия и личный состав органов управления и обслуживания противника [95].

Классификация мероприятий РЭБ принятая в ВС США представлена на рис. 4.53 по материалам [95, 250, 253, 256, 462].

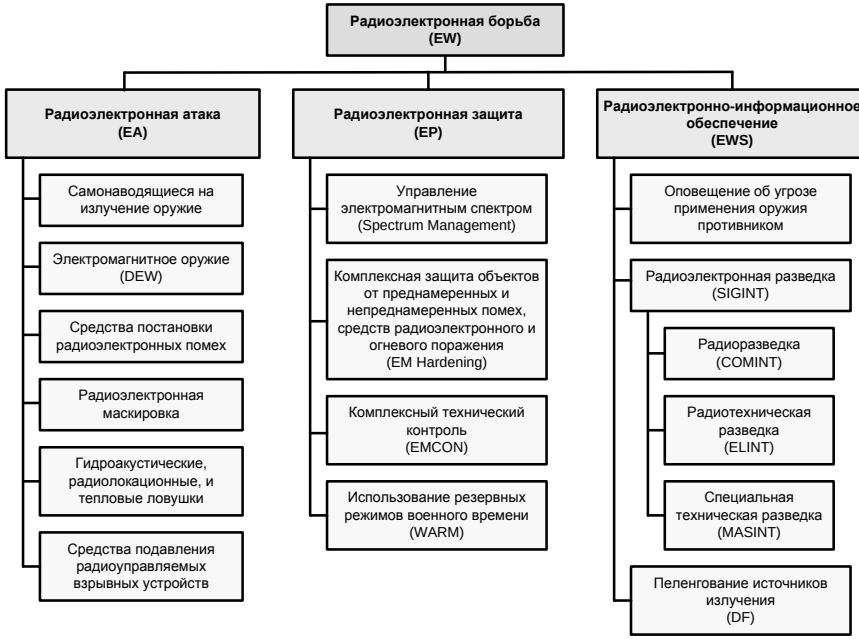


Рис. 4.53. Классификация мероприятий РЭБ в ВС США [462]

Необходимо отметить, что вышеизложенная методология РЭБ является общепринятой преимущественно для ВС США, и более подробно она представлена в работах [213, 462]. Вместе с тем в отечественной теории РЭБ принят несколько другой подход к целям, задачам и классификации мероприятий РЭБ, которые более полно изложены в работах [245, 248, 254, 255, 462].

4.7.2. Типовой сценарий применения сил и средств радиоэлектронной борьбы в сетецентрической войне

На примере операций многонациональных сил в зоне Персидского залива в 1991 и в 2003 гг. рассмотрим, насколько была важна РЭБ в качестве одной из основных составляющих современной военной кампании, основанной на сетецентрических принципах управления. Информация о сценарии применения сил и средств РЭБ в конфликте приводится по материалам работы [250].

На рис. 4.54 и 4.55 представлены схемы постановки помех с началом воздушной и воздушно-наземной операций многонациональных сил.

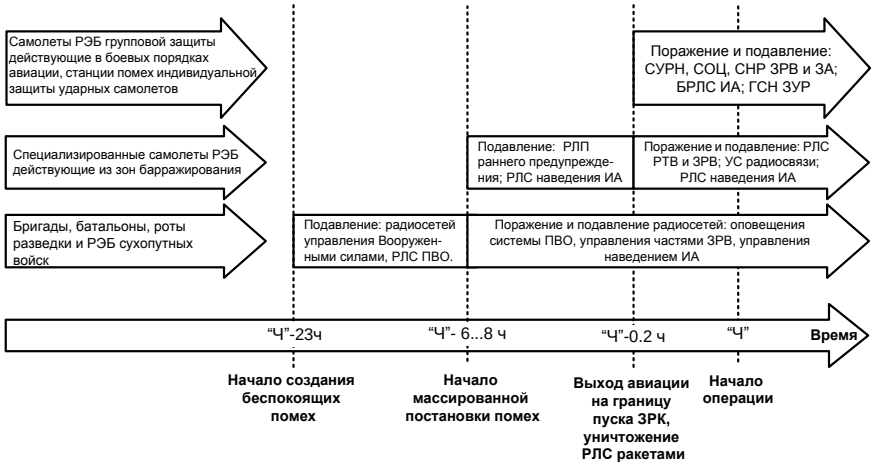


Рис. 4.54. Сценарий применения РЭБ с началом воздушной операции в сетецентрической войне [250]

На схеме показано, что заблаговременная постановка помех была начата за 4-6 ч до начала активных военных действий. В операции были задействованы средства РЭБ индивидуально-взаимной за-

щиты самолетов ударной авиации, самолеты и вертолеты РЭБ в зонах барражирования, забрасываемые передатчики помех полевой артиллерии и авиации, средства РЭБ бригад, батальонов, а также рот разведки и РЭБ сухопутных войск [250].

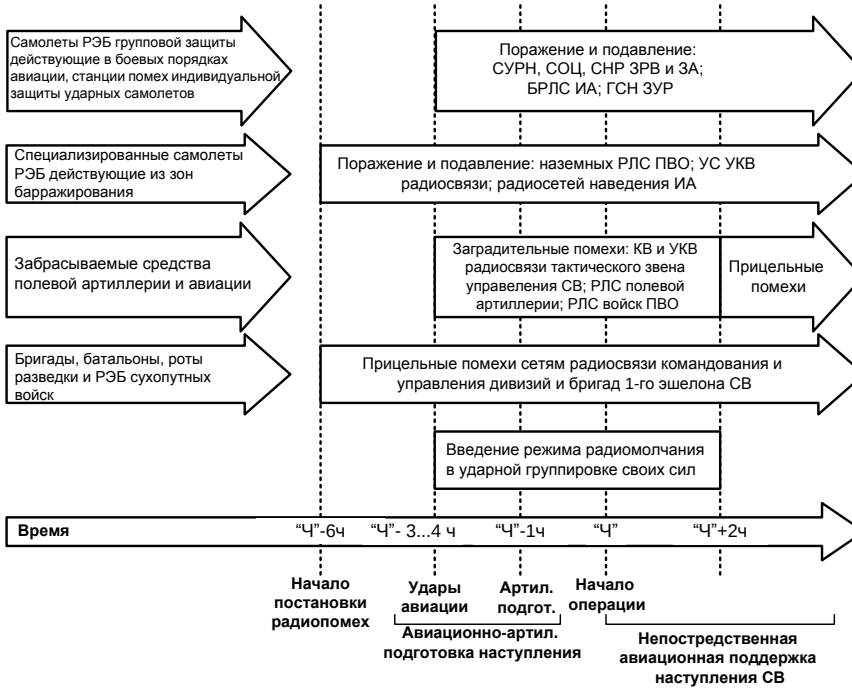


Рис. 2.55. Сценарий применения РЭБ с началом воздушно-наземной операции в сетецентрической войне [250]

Специализированные самолеты РЭБ (такие как ЕС-130Н), способны за один вылет произвести разведку и подавить до 150-200 РЛС и до 15-18 радиосетей УКВ в системах управления ПВО. При этом практически все самолеты ударных групп тактической авиации ВВС оснащены аппаратурой РЭБ (аппаратурой радио- и радиотехнической разведки, станциями активных помех коллективной защиты, станциями активных помех индивидуальной защиты, станциями пассивных помех, ИК-аппаратурой разведки и оповещения, станциями оптико-электронного подавления, противорадиолокационными ракетами). Противорадиолокационные ракеты оснащены головками самонаведения, которые могут работать в узкой полосе частотного диапазона

0,39-20 ГГц на нескольких частотах. Число этих частот — 10-20 и более [250].

Кроме того, в военных операциях широко применялись БПЛА РЭБ для постановки помех системам ПВО и средствам связи системы управления ВС. Запуск большинства из них производился с самолетов и кораблей [250].

Широко применялись забрасываемые передатчики помех (ЗПП), которые работали в частотном диапазоне 30-11000 МГц. Основной целью поражения в начале воздушной операции являлись РЛС систем ПВО, а также каналы управления оружием. Основной целью в воздушно-наземной операции, помимо вышеуказанных, являлись УКВ и КВ каналы радиосвязи системы управления ВС.

Следует отметить, что в большинстве современных войн силы и средства РЭБ до начала первого массированного удара ВТО создавали сильные помехи для РЭС противника, и прежде всего для РЭС системы ПВО. Под прикрытием радиопомех, предваряя удары самолетов из эшелона прорыва ПВО, в несколько этапов наносились удары крылатыми ракетами морского и авиационного базирования по объектам критической инфраструктуры. Прорыв системы ПВО противника, как правило, обеспечивался за счет широкого применения ВТО — крылатых ракет, а также большого числа управляемых ракет «воздух — РЛС» в сочетании с эффективными радиопомехами для РЭС противника [245].

Опыт применения средств РЭБ в локальных войнах показывает, что для подавления систем связи использовались следующие виды активных электромагнитных помех [235]:

- прицельные по одной частоте;
- скользящие в широком участке диапазона частот;
- дискретные на относительно небольшом участке диапазона частот (подавляющие одновременно несколько частот);
- сплошные заградительные, перекрывающие полностью относительно узкий участок диапазона частот.

Помимо этих видов помех применялись ответные помехи, которые ставились при появлении сигнала противника, а также ретрансляционные помехи [235].

Для подавления систем радиолокации были использованы импульсные, непрерывные или изменяющиеся по определенному закону электромагнитные помехи, а для подавления систем радионавигации – прицельные, маскирующие и имитирующие, изменяющие мощность и направление излучения радиомаяка [235].

4.7.3. Авиационные комплексы РЭБ (на примере комплексов ВС США)

4.7.3.1. Тенденции развития и применения авиационных комплексов РЭБ в условиях перехода к концепции сетецентрической войны

Результаты анализа боевых действий, в последнее время имевших место в Европе и на Ближнем Востоке, показывают, что системы и средства РЭБ воздушного базирования остаются одними из ключевых элементов в достижении превосходства над противником и, как следствие, в обеспечении успеха проводимых информационных операций [222].

Несмотря на то, что США имели господство в воздухе во всех ведущихся ими военных операциях, уже в обозримом будущем это превосходство ставится под вопрос в связи с дальнейшим совершенствованием средств ПВО. Для того чтобы сохранить инициативу, военное руководство США определило ряд ключевых областей развития технологий, включая технологии в области РЭБ, революционные достижения в которых гарантируют завоевание господства в воздухе для выполнения задач военной авиацией в обозримом будущем [222].

Традиционно самолеты авиации ВВС и ВМС США оборудуются системами и средствами индивидуальной защиты от средств ПВО и ГСН ракет. К ним относятся:

- авиационные бортовые системы предупреждения об облучении РЛС комплексов ПВО (системы: AN/ALR-56M, AN/ALR-67, AN/ALR-69, AN/ALR-74, SCR-2100, AN/ALQ-78) [250];
- авиационные бортовые системы РТР комплексов ПВО (системы: ES-5000, AN/ALQ-61, WJ-1740, LR-100, «FASTHAT», LR-5200) [250];
- бортовые средства и комплексы РЭБ для индивидуальной защиты самолетов от систем ПВО (системы: AN/ALQ-119, AN/ALQ-135, AN/ALQ-137, AN/ALQ-184, AN/ALQ-165, AN/ALR-94, AN/AAQ-24(V)13 LAIRCM, TEWS, IDECM, «INEWS», AN/ASQ-239 «Barracuda») [223, 250, 450];
- авиационные передатчики помех одноразового использования [250];

- бортовые средства и комплексы РЭБ для индивидуальной защиты самолетов от средств в оптическом и ИК-диапазонах (системы: AN/ALQ-212(V) ATIRCM, TADIRCM, AN/AAR-57(V) CMWS, AN/AAQ-24 «Немезис», LAIRCM) [223, 250];
- автономные и буксируемые ложные воздушные цели (системы: ADM-160B MALD, MALD-J, AN/ALE-55) [219, 222, 223, 257];
- противорадиолокационные ракеты (ракеты: AGM-45 Shrike, AGM-78 Standart ARM, AGM-88 HARM и др.) [245, 250, 251].

С 2002 г. в США реализуется программа AEA (Airborne Electronic Atack) по применению авиационных групповых средств РЭБ в рамках единой системы. Программа AEA предполагает разработку способов применения, оценку эффективности, формирование требований и распределение задач между средствами РЭБ в рамках единой системы их применения. Кроме того, программа AEA включает в себя исследования и снижение технологических рисков при создании средств РЭБ, разработку и корректировку плана их финансирования [222].

Современные принципы организации РЭБ в ходе проведения крупномасштабных военных операций предполагают не только оснащение системами радиоэлектронной борьбы индивидуальной защиты каждого ЛА, но и наличие специализированных самолетов РЭБ, предназначенных для осуществления групповой защиты, а также специализированных систем РЭБ, размещенных на БПЛА [218].

В связи с этим в программе AEA задействованы:

- специализированные самолеты РЭБ: EA-6B, EA-18G, EC-130H;
- маневрирующие авиационные ложные воздушные цели MALD/MALD-J;
- ресурсы БРЛС с АФАР на самолетах тактической авиации, привлеченных для решения задач РЭБ;
- БПЛА, оснащенные средствами РЭБ, действующие в зонах поражения средств ПВО.

При этом основными объектами воздействия авиационных средств РЭБ США являются РЭС управления войсками и оружием систем ПВО противника [222].

В рамках программы AEA рассматривается также возможность применения авиационных средств РЭБ при ведении асимметричных

боевых действий. Здесь основными объектами воздействия будут являться мобильные средства связи, передачи данных и АСУ, дистанционно управляемые радиовзрыватели, РЭС управления оружием мобильных зенитных средств малой дальности и ближнего действия [222].

Для решения задач РЭБ в ходе операций с участием средств воздушно-космического нападения в период до 2025 г. в ВС США рассматриваются два компонента.

1. Основной компонент – образован пилотируемыми носителями средств РЭБ, действующими в пределах воздушного пространства противника либо за его пределами. Они решают задачи по ведению РТР, РЭП, поражению РЭС самонаводящимся на излучение оружием, боевому управлению авиационными силами и средствами РЭБ.
2. Вспомогательный компонент – включает в себя беспилотные носители средств РЭБ, действующие в пределах воздушного пространства противника, недоступного для средств РЭБ основного компонента (например, в пределах зон гарантированного поражения), которые решают задачи по имитации средств воздушного нападения, РТР и РЭП радиоэлектронных средств противника.

В настоящее время реализуются четыре основных способа применения авиационных групповых средств РЭБ [222]:

- за пределами воздушного пространства, обороняемого противником (как правило, из зон барражирования);
- в пределах обороняемого противником воздушного пространства без входа в зоны поражения зенитных средств с известным местоположением их позиций (модифицированное сопровождение боевых порядков прикрываемых сил);
- в пределах зон поражения зенитных средств в одном боевом порядке с прикрываемой авиацией (проникающее сопровождение боевых порядков прикрываемых сил).
- в пределах зон поражения средств ПВО (автономное применение).

При этом, интеграция всех сил и средств РЭБ в единое информационно-коммуникационное пространство, как это предусмотрено программой АЕА, позволяет управлять ресурсами РЭБ, осуществлять оптимальное распределение этих средств по объектам подавления в зависимости от обстановки в реальном масштабе времени [222].

Функциональные задачи, возлагаемые на системы и средства радиоэлектронной борьбы воздушного базирования, могут быть конкретизированы и сведены в соответствующие четыре группы:

- подавление из района барражирования радиоэлектронных средств противника вне зоны действия его ПВО (сфера ответственности ВВС);
- подавление в целях групповой защиты РЛС противника самолетом РЭБ, следующим совместно с ударной группой (сфера ответственности ВМС);
- подавление в целях индивидуальной защиты от ракет классов «земля-воздух» и «воздух-воздух» (собственные программы ВВС и ВМС);
- подавление РЛС противника с помощью беспилотных летательных аппаратов посредством расходуемых маневрирующих ложных целей или боевых БПЛА, способных помимо нанесения высокоточных ударов по системам управления противника и радиоэлектронным средствам проводить «радиоэлектронную атаку» (совместные программы ВВС и ВМС).

Как показано в работе [235], опыт локальных войн конца XX – начала XXI века показывает, что основными способами применения специализированных самолетов РЭБ авиации США, будут являться следующие:

1. Радиоэлектронная атака из района барражирования самолетами РЭБ типа EA-6B Prowler, EC-130H CompassCall и самолетами стратегической авиации, которые будут находиться вне досягаемости средств ПВО противника. Этот способ используется для подавления РЛС и систем УКВ-радиосвязи, систем дальнего обнаружения, управления ПВО и авиации как для подавления систем воздушно-космической обороны противника (разведки, навигации, радиолокации и связи), так и в целях групповой защиты эшелонов ударной группы авиации при ее полете к объектам удара.
2. Радиоэлектронная атака методом сопровождения ударной группы авиации самолетами EA-6B и EA-18G ВМС США, которые находятся вне боевого порядка ударной группы и следуют за ней на некотором удалении. Задачи и объекты подавления являются теми же, что и в первом способе.

Этот метод постановки электронной помехи используется для обеспечения живучести специальных самолетов РЭБ.

3. Радиоэлектронная атака непосредственно из боевого порядка ударных групп, например такими самолетами РЭБ, как EA-18G Growler. Этот способ используется для постановки помех радиолокационным станциям различного назначения систем УКВ-радиосвязи ВВС, ПВО и ПРО противника, а также в целях групповой и коллективной защиты самолетов ударной группы авиации на маршруте полета к цели.
4. Радиоэлектронная атака при сближении с целью. Этот способ используется для подавления систем управления и наведения истребительной авиации и ПВО противника как для поражения (подавления) цели, так и для индивидуальной защиты атакующих цель самолетов тактической авиации.
5. Радиоэлектронная атака против систем радиолокации, связи и навигации ВВС и ПВО противника отдельными самолетами стратегической авиации ВВС США при полете к цели. Этот способ используется для подавления систем воздушно-космической обороны противника как для поражения (подавления) цели, так и для обеспечения индивидуальной защиты авиации на маршруте полета и в районе нанесения удара по объектам противника.

С конца 1990-х гг. единственным обладателем специализированной воздушной платформы РЭБ для подавления несвязных РЭС в ВС США являются ВМС, на вооружении которых более 30 лет стоит самолет РЭБ EA-6B Prowler. В связи с этим он активно используется как в ВМС, так и в ВВС и в корпусе морской пехоты [257].

Наличие в ВС США только одного типа специализированного авиационного комплекса РЭБ ориентированного на подавление систем ПВО связано с выводом из эксплуатации других самолетов РЭБ, стоявших на вооружении в ВВС – F-4G Wild Weasel (в 1996 г.) и EF-111 Raven (в 1998 г.) [257].

Одной из причин снятия их с вооружения были экономические соображения, а также уверенность, что созданные по технологии «Stealth» («Стелс») самолеты в гораздо меньшей степени нуждаются в поддержке при подавлении РЭС противника. Однако позже это мнение было изменено в связи с постоянным совершенствованием систем и средств ПВО возможного противника. Технология «Stealth» дей-

ствительно позволяет снизить заметность самолетов, сокращая тем самым радиус действия вражеских систем и средств обнаружения. Таким образом, образуются коридоры, по которым самолеты «Stealth» могут достичь цели. Но, с другой стороны, противник способен просчитать возможные маршруты и дополнительно использовать комплексы и системы ПВО. Кроме того, планы ВВС по укомплектованию к концу текущего десятилетия парка самолетов преимущественно платформами «Stealth» не выдерживаются, что требует еще большего развития систем и средств РЭБ групповой защиты от ПВО [257].

В 2001 г. ВМС США совместно с ВВС приняли решение о снятии с вооружения в период 2009-2012 гг. самолета EA-6B Prowler, что вызвало необходимость в поиске адекватной замены. На рубеже 2004-2005 гг. ВВС и ВМС получили от Объединенного совета по контролю потребностей (JROC) одобрение на разработку новых платформ, способных решать в полном объеме все возложенные на самолеты РЭБ задачи [257].

Такой совместный подход к разработке и приобретению новых, современных платформ ставит ВВС, ВМС, а также корпус морской пехоты США в зависимость друг от друга. В процессе изучения вопросов, связанных с разработкой новых самолетов РЭБ, ВВС и ВМС сместили акцент с выбора конкретных платформ на формирование требований к ожидаемым результатам их использования. При этом главной задачей становится создание взаимно дополняющих систем, удовлетворяющих потребностям не одного, а сразу нескольких видов ВС, и ориентированных на взаимодействие в составе единой многоплатформной сети. Такая сетевая организация воздушных компонентов РЭБ позволяет обеспечить перекрытие всего спектра возлагаемых на них задач и в отдельных случаях допускает дублирование функций в целях гарантированного достижения целей применения [257].

Американские специалисты считают, что даже обычные боевые самолеты, оборудованные РЛС с АФАР типа AN/APG-77(V) истребителя F/A-22 Raptor и AN/APG-81(V) истребителя F-35A, смогли бы также вносить свой вклад в подавление РЭС противника на соответствующих частотах. При этом общее руководство ими может осуществляться с борта разрабатываемого самолета E-10A – связующего звена между наземным центром управления и воздушными платформами [257].

В перспективе на период до 2030 г. задачи по обеспечению групповой защиты авиационных порядков от ПВО при нанесении ими ударов будут возложены на самолеты EA-18G Growler, EA-6B Prowler,

а после 2024-го – на разрабатываемый на базе F-35B самолет РЭБ [218].

С первой половины 1980-х гг. по настоящее время самолет EC-130H Compass Call остается единственной платформой в ВВС США выполняющий преимущественно задачи подавления систем связи противника из зоны барражирования за пределами досягаемости средств ПВО. В настоящее время предполагается переоборудовать эти самолеты для решения задач, возникающих в ходе боевых действий против иррегулярных формирований, а также оснастить EC-130H Compass Call новым комплексом подавления УКВ-радиосвязи SPEAR. Программой модернизации самолетов EC-130H предусмотрено, что работы по их замене будут завершены к 2018 г. [223, 257].

По планам командования ВВС США всего планируется иметь на вооружении 12-15 модернизированных самолетов EC-130H Compass Call, которые могут эксплуатироваться еще не менее 10-15 лет. Предполагается, что эти самолеты будут находиться на вооружении до 2025 г. При этом часть задач по радиоэлектронному подавлению сетей радиосвязи и радиолиний управления систем ПВО планируется возложить на EA-18G Growler за счет оборудования его станцией активных помех AN/ALQ-227. При этом эти задачи, наряду с задачами групповой зашиты от ПВО, EA-18G Growler будет решать, находясь в боевых порядках авиации [223].

4.7.3.2. Специализированные авиационные комплексы РЭБ

Рассмотрим более подробно характеристики и боевое применение основных специализированных самолетов РЭБ, стоявших и стоящих на вооружении ВВС и ВМС США.

Самолет EA-6B Prowler – палубный самолет ВМС США, базирующийся на многоцелевых авианосцах (до четырех на каждом), предназначенный для ведения радиоэлектронной борьбы и разведки, решающий задачи РЭП и огневого поражения корабельных и наземных РЛС и срыва работы сетей радиосвязи систем ПВО противника. При выполнении задач прикрытия корабельных группировок, авиационных ударных групп он обеспечивает эффективную постановку помех радиоэлектронным средствам противника на дальности до 250 км. При этом эффективная дальность подавления с высоты 9 км достигает 400 км. Кроме того, они обеспечивают и подавление каналов радиосвязи управления истребителями-перехватчиками противника. Эти

самолеты в основном действуют над морем без захода в зону ПВО противника [95, 219].

Базой при создании EA-6B Prowler послужил палубный штурмовик A-6 Intruder. При создании машины была увеличена длина фюзеляжа, за счет чего был увеличен экипаж. Так же при создании самолета использовался опыт эксплуатации аналогичных по задачам самолетов EA-6A. Первый полет самолета состоялся 25 мая 1968 г., а уже в 1971 г. самолет поступил на вооружение ВМС США. Экипаж машины состоит из четырех человек — пилота и трех офицеров-операторов систем РЭБ. Когда Prowler был принят на вооружение, на нем установили тактическую систему постановки помех, способную подавлять сигналы сразу с пяти РЛС. Первые 23 самолета EA-6B имели стандартное оборудование в виде станций РЭП ALQ-92 и ALQ-99.

В 1973 г. было выпущено 25 машин EA-6B Prowler с измененной по программе EXCAP конструкцией фюзеляжа и новой тактической системой постановки помех ALQ-99A. В 1976 г. 45 новых и 17 ранее изготовленных самолетов оснастили средствами индивидуальной защиты AN/ALQ-126 для подавления средств управления оружием и системой поражения противника. 55 оставшихся самолетов EA-6B Prowler вновь модернизировали, установив на них системы постановки помех, способные идентифицировать и отслеживать цели. Эти самолеты EA-6B Prowler были особенно эффективны в комплексе с управляемыми ракетами AGM-88A, которыми они также оснащались.

В конце 1980-х самолеты Prowler варианта EA-6B были снова модернизированы по программе ADVCAP. Модернизация велась по двум направлениям, а именно:

- были установлена новая станция постановки помех AN/ALE-39, системы пассивного слежения и подавления сигналов;
- была проведена модернизация авионики, что привело к оснащению машин EA-6B новыми индикаторами на жидких кристаллах, более мощной РЛС, цифровым автопилотом и системой связи AN/ALQ-19.

Кроме того, было проведено улучшение летных характеристик самолета EA-6B в ходе реализации программы VEP (программа технической модернизации). На усовершенствованных EA-6B усилена конструкция фюзеляжа, установлены новые закрылки, аэродинамические тормоза и др.

Для продления срока службы самолета EA-6B реализуется программа ICAP III, целью которой является совершенствование систем и средств вскрытия боевой обстановки. При этом отмечается, что, помимо подавления РЛС систем управления оружием противника, все большее значение в перечне решаемых самолетом EA-6B задач придается подавлению связных радиоэлектронных систем, а также вопросам обеспечения безопасности прибрежных районов путем подавления корабельных навигационных РЭС [218].

Одним из основных РЭС, разработанных и устанавливаемых на EA-6B в рамках программы ICAP III, является цифровой приемник радиолокационных сигналов AN/ALQ-218 с диапазоном частот до 20 ГГц, обеспечивающий обнаружение, идентификацию и определение местоположения источника излучений. AN/ALQ-218 – первый приемник, обеспечивающий избирательное подавление РЭС противника станцией постановки помех на конкретных частотах и позволяющий ставить помехи РЛС со скачкообразной перестройкой частоты. Кроме того, он может использоваться для наведения на цель противорадиолокационных ракет типа AGM-88 HARM [218].

В настоящее время ВМС США проходят перевооружение в рамках которого самолеты EA-6B Prowler заменяются на EA-18 Growler. Самолеты EA-6B Prowler планируются к выводу из эксплуатации к 2020 г. [222].

Самолет EC-130H Compass Call. Особая роль в информационных операциях с участием ВВС отводится специализированному постановщику помех системам связи и управления противника EC-130H Compass Call, действующему из так называемых «безопасных зон» района барражирования, находящихся за пределами зоны поражения ЗРК [95, 218].

Самолет EC-130H благодаря многочисленной группе операторов и способности пеленговать цели во всех диапазонах волн обеспечивает [95]:

- вскрытие дислокации узлов связи и пунктов управления;
- сбор и анализ содержания радиообмена;
- радиоэлектронное подавление радиоканалов и радиосетей систем управления войсками и оружием.

EC-130H несет мощные передатчики нижнего, среднего и высокого диапазонов электромагнитных волн. На фюзеляже и под крылом этого самолета смонтировано множество ножевых антенн, а в контейнерах на концах крыла находятся выпускаемые в полете буксируемые проволочные антенны большой длины [95].

Комплекс РЭБ самолета ЕС-130Н предназначен для подавления радиоканалов управления истребителей-перехватчиков противника, бортовых и наземных средств навигации и опознавания. Типовая схема применения предусматривает барражирование самолетов ЕС 130Н на высоте 9000 м по замкнутым маршрутам над своей территорией в 70 км от линии соприкосновения войск с ведением подавления РЭС противника на глубину до 300 км. Основу бортового оборудования ЕС-130Н Compass Call составляет автоматизированный комплекс РЭП «Ривет Файр». Он обеспечивает ведение радиоразведки в диапазоне 20-1500 МГц, постановку шумовых помех прицельных по частоте, а также передачу дезинформирующих сообщений. Комплект передатчиков помех мощностью по 800 Вт обеспечивает одновременную постановку помех до 20 радиолиниям (радиосетям), работающим в диапазоне частот от 20 до 1000 МГц. Виды помех: шумовые; дезинформирующие; ответные каналам радиосвязи сетей управления ПВО и ответные импульсные радиотехническим устройствам. Основным направлением модернизации аппаратуры РЭБ этого самолета является повышение уровня ее автоматизации [219, 250].

Аппаратура системы РЭП самолета ЕС-130Н Compass Call непрерывно совершенствуется, при этом основное внимание уделяется разработке новых алгоритмов анализа радиопередач и управления подавлением, а также повышению точности пеленгования.

Командование ВВС США в интересах расширения возможностей по радиоэлектронному подавлению на ТВД с 2001 г. проводит модернизацию самолета РЭП ЕС-130Н Compass Call, находящегося на вооружении с 1982 г. [219].

Проводимая модернизация предусматривает оснащение самолета более совершенными радиоэлектронными средствами в интересах расширения существующих и приобретения принципиально новых возможностей. Программой модернизации самолетов ЕС-130Н предусмотрено обновить весь парк самолетов до модификации «Block 35». Предполагается, что работы по модернизации будут завершены к 2018 г. Представители ВВС заявляют, что планируется иметь 15 таких машин, что позволит снизить нагрузку на каждый самолет, а также увеличить возможности по ведению РЭБ [257].

При этом рассматриваются следующие дополнительные задачи, возлагаемые на ЕС-130Н Compass Call после модернизации, такие как [219, 223]:

- РЭП систем коротковолновой, радиорелейной и спутниковой связи военного и государственного управления;

- РЭП радиосетей управления тактической авиацией, управления комплексами ПВО, современных помехозащищенных систем радиосвязи и передачи данных оперативно-тактического звена сухопутных войск;
- РЭП гражданских и коммерческих систем подвижной сотовой и транкинговой радиосвязи;
- РЭП из зон барражирования РЛС обнаружения функционирующих в МВ- и ММВ- диапазонах;
- ведение радио- и радиотехнической разведки с целью формирования в реальном масштабе времени целеуказаний по вскрытым узлам связи и РЛС противника для применения систем и средств высокоточного оружия классов «воздух-земля» и «земля-земля».

Таким образом, в ходе модернизации EC-130H расширяются его возможности – от подавлений сетей систем управления военного назначения до подавления сетей сотовой связи, которые могут использоваться террористическими группировками.

После модернизации самолет EC-130H может решать задачу выявления и подавления помехозащищенных мобильных средств радиосвязи (за единицы минут меняющих свое местоположение), кратковременно выходящих в эфир, а также выдачи в реальном масштабе времени высокоточного целеуказания по вскрытым узлам связи противника системам оружия классов «воздух-земля» и «земля-земля» для их огневого поражения. Эта задача будет решаться путем объединения в ходе выполнения боевого задания в сеть пары самолетов EC-130H Compass Call и самолета РРТР RC-135V/W «Rivet Joint». При этом высокоскоростной обмен данными в реальном масштабе времени между ними будет производится с помощью терминалов системы «Link-16», что позволит совместно с самолетом RC-135V/W вести высокоточную разведку и определение местоположения радиостанций противника [219].

Новый вариант самолета EC-130H Compass Call будет более эффективно решать задачи РЭП современных мобильных средств радиосвязи, систем ПВО противника, а также сможет выдавать в реальном масштабе времени данные по целеуказанию для огневого поражения [219].

По планам командования ВВС США всего планируется иметь на вооружении 12-15 модернизированных самолетов EC-130H Compass Call, которые могут эксплуатироваться еще не менее 10-15

лет. Предполагается, что эти самолеты будут находиться на вооружении до 2025 г. [219, 223].

Самолет EA-18G Growler – палубный самолет РЭБ в ВМС США, разработан фирмой Boeing на базе истребителя F/A-18F Super Hornet. Первый полет совершил 15 августа 2006 г. Серийное производство самолета началось в 2007 г. На флоте EA-18G заменит устаревшие самолеты EA-6B Prowler.

Самолет РЭБ EA-18G Growler ВМС США предназначен для огневого поражения и РЭП наземных и корабельных РЛС, а также РЭП сетей радиосвязи и радиолиний управления систем ПВО противника при его нахождении преимущественно в боевых порядках. Самолет обладает большей маневренностью по сравнению с EA-6B Prowler. Он может сопровождать ударную группу, состоящую из истребителей типа F/A-18, F-16 и F-15E [223].

Комплекс РЭБ на самолете EA-18G Growler включает в себя [218, 219, 223]:

- станцию РТР AN/ALQ-218(V)2;
- три контейнера со станциями активных помех средствам радиолокации AN/ALQ-99F(V), которые могут работать одновременно;
- станцию активных помех средствам радиосвязи AN/ALQ-227;
- перспективный многоцелевой тактический терминал MATT спутниковой связи;
- терминал многофункциональной системы распределения информации MIDS, который позволит обеспечить интеграцию в систему связи прямой видимости «Link-16», а также перенацеливание и проведение скоординированной атаки несколькими боевыми платформами (пилотируемыми и БПЛА);
- устройство исключения собственных помех INCANS;
- дополнительные устройства отображения информации в кабине экипажа.

Помимо указанного БРЭО в состав вооружения EA-18G включены две противорадиолокационные ракеты AGM-88 HARM [218].

Станция радиотехнической разведки AN/ALQ-218(V)2 является средством информационного обеспечения станций активных помех и имеет в своем составе 10 радиоэлектронных и 12 антенных блоков. Она установлена в носовой части самолета (за АФАР РЛС AN/APG-79). Многоканальные приемные устройства обеспечивают

прием сигналов в диапазоне частот от 64 МГц до 40 ГГц. Приемные антенны станции (36 шт.) размещены в контейнерах (длина 3 м, диаметр 0,33 м), установленных на законцовках крыла. Такая компоновка обеспечивает пеленгование с точностью до нескольких метров, позволяет значительно повысить точность определения координат источников радиолокационных излучений и целеуказания противорадиолокационным ракетам, входящим в боекомплект самолета. Станция обеспечивает круговой обзор в азимутальной плоскости с разрешающей способностью по азимуту 2°. Точность определения дальности составляет 5-10%. Потребляемая станцией мощность 1,21 кВт, среднее время наработки на отказ 620 ч (по результатам лабораторных испытаний), масса аппаратуры 224 кг [218, 219].

Станция активных помех средствам радиолокации AN/ALQ-99F(V) предназначена для постановки помех бортовым радиолокационным станциям и управляемым ракетам противника, а также для обеспечения групповой защиты боевых порядков самолетов от средств ПВО. В состав каждого из трех подвесных контейнеров станций AN/ALQ-99F(V) входят следующие элементы [218]:

- две антенные системы (передней полусферы и задней полусферы);
- два усилителя мощности (передней полусферы и задней полусферы);
- турбогенератор;
- универсальный задающий генератор UUEU;
- блок управления.

Размеры каждого из подвесных контейнеров станции AN/ALQ-99F(V) – 4,7×0,7×0,5 м. Универсальный задающий генератор UUEU позволяет оборудовать станции усилителями мощности различных частотных диапазонов в разных комбинациях. Кроме того, для постановки помех используется антенная система РЛС AN/APG-79 [218].

Вместо станции помех связным РЭС AN/USQ-113, которая используется на самолете EA-6B, на EA-18G устанавливается станция AN/ALQ-227. Ее основу составят приемное устройство CCSR (Communication Countermeasures Set Receiver) и процессорный блок. AN/ALQ-227 представляет собой отдельный приемник, а не приемник с передатчиками помех, как AN/USQ-113. Для излучения сигналов помех будет использоваться передатчик контейнерной станции помех РЛС УКВ-диапазона ALQ-99(V). При этом в передатчиках новой контейнерной станции постановки помех вместо ламп бегущей волны бу-

дут использоваться твердотельные элементы. Кроме этого, она будет связана с двумя антенными устройствами, что позволит эффективнее управлять режимами подавления РЭС. В настоящее время разработчики решают вопрос об использовании бортового генератора сигналов помех AN/ALQ-214 для подавления РЭС противника при одновременном применении РЛС с АФАР AN/APG-79(V) [219, 223].

Устройство исключения собственных помех INCANS (INterference CANcellation System), разработанное фирмой EDO, обеспечивает возможность одновременного осуществления радиосвязи и создания помех в УВЧ-диапазоне. Оно будет одним из главных улучшений в области оборудования РЭБ самолета EA-18G по сравнению с EA-6B, так как наличие системы INCANS позволит использовать до 85% бортового связного оборудования одновременно с постановкой помех для РЭС противника (применение систем связи при режиме подавления на EA-6B Prowler являлось сложной проблемой) [219, 223].

По мнению американских специалистов, оснащение самолета терминалом систем связи и распределения данных MIDS является наиболее важным этапом усовершенствования. Это позволит им совместно работать в единой сети цифровой передачи данных «Link-16» с другими средствами РЭП и РТР, в частности с самолетами RC-135 V/W «Rivet Joint», в целях формирования и обмена данными единой картины радиоэлектронной (тактической) обстановки в районе боевых действий [219].

Впервые самолет EA-18 Growler был применен в боевых условиях 23 марта 2011 г., во время военной операции «Одиссея. Рассвет» в Ливии. Тогда пять самолетов EA-18G Growler ВМФ США приняли непосредственное участие в подавлении объектов ПВО и установлении бесполетной зоны в стране [223].

При ведении боевых действий авиационными группировками значительное внимание уделяется своевременному выявлению мест дислокации, параметров и режимов работы РЛС систем ПВО противника для последующего подавления или снижения их эффективности. На современном этапе авиацией ВВС США это достигается не только благодаря использованию специализированных самолетов РЭБ, но и других воздушных средств – тактических истребителей F-16CJ или F 4G, оснащенных противорадиолокационными ракетами AGM-88 HARM, а также автономных ложных воздушных целей, сбрасываемых с самолетов-носителей [219, 250].

Кроме того, ресурсы перспективных многофункциональных БРЛС с АФАР самолетов тактической авиации могут также использо-

ваться для решения задач РЭБ. Так, многофункциональные БРЛС с АФАР могут применяться в качестве индивидуальных или групповых средств РЭБ. По оценкам зарубежных специалистов, в случае задействования таких БРЛС в качестве групповых средств РЭБ основным способом их применения станет проникающее сопровождение прикрываемой авиации, а их основной задачей будет радиоэлектронное подавление РЭС управления оружием зенитных средств и головок самонаведения управляемых ракет [222].

Перспективная система РЭБ следующего поколения NGJ для самолета F-35B. После закрытия программы по разработке специализированного самолета РЭБ на основе стратегического бомбардировщика B-52 самолет EC-130H является единственным носителем многофункциональных средств РЭБ, ориентированных как на применение против каналов управления оружием и РЛС средств ПВО, так и на РЭП каналов и сетей радиосвязи. В связи с этим среди разрабатываемых и модернизируемых авиационных средств РЭБ в США наибольший интерес с точки зрения внедрения новых технологий и объема финансирования представляет разрабатываемая система РЭП следующего поколения NGJ (Next Generation Jammer), первоначально предназначавшаяся для замены системы РЭП AN/ALQ-99 ICAP III на самолетах EA-18G [222].

В рамках реализации мероприятий по программе NGJ проводятся [222]:

- исследование перспективных технологий;
- НИОКР по созданию прототипа;
- испытания в лабораторных условиях;
- разработка специального программного обеспечения.

Целью наращивания возможностей в разработке системы NGJ является достижение предельных возможностей по противодействию перспективным угрозам в радиодиапазоне. Порядок работ определен в три этапа согласно приоритетам противодействия и важности различных РЭС управления войсками и оружием [222].

Так, наиболее важным и перспективным для РЭБ считается средний диапазон (ориентировочно 2-18 ГГц), НИОКР по которому проводятся в рамках первого этапа. В данном диапазоне работает большинство известных РЛС обнаружения, наведения, целеуказания и управления оружием систем ПВО различных стран мира. На втором этапе работ исследуется низкий диапазон (0,2-2 ГГц), соответствующий диапазону работы РЛС обнаружения, наведения, и целеуказания, средства связи и обмена данными и др. На третьем этапе – высокий

поддиапазон (18-40 ГГц), в котором функционируют РЛС управления огнем ряда современных и перспективных ЗРК, ГСН и дистанционные радиовзрыватели управляемых ракет [222].

В середине 2015 г. было принято решение о начале разработок опытного образца. При этом для создания системы NGJ планируется использовать военные и коммерческие технологии не только национального, но и совместного производства, а также импортные технологии [222].

Основные требования, предъявляемые к системе NGJ как к технологическому решению следующего поколения [222]:

- возможность одновременного прицельного по частоте и направлению воздействия на разные РЭС с различным местоположением;
- высокий энергетический потенциал, примерно в 10 раз превышающий аналогичный показатель системы AN/ALQ 99;
- управляемая поляризация помеховых сигналов;
- возможность адаптивного РЭП;
- модульность и открытая архитектура конструкции.

Одновременное прицельное по частоте и направлению подавление нескольких РЭС с различными позициями может быть обеспечено путем реализации системы NGJ на основе широкополосных АФАР со схемой формирования независимо управляемых лучей диаграммы направленности. Такая схема позволяет формировать несколько независимых лучей диаграммы направленности различных по частоте, структуре и поляризации сигналов. Количество одновременно подавляемых РЭС будет зависеть от ряда условий (типа РЭС, их характеристик и режимов работы, наклонных дальностей и угловых положений относительно носителя системы РЭП, ЭПР прикрываемых ЛА и др.). Для обеспечения необходимого сектора сканирования АФАР могут быть применены такие технологии, как задержка сигнала в реальном масштабе времени TTD (True Time Delay) [222].

Высокий энергетический потенциал планируется достигнуть за счет применения в качестве усилительных приборов твердотельных усилителей на основе нитрида галлия GaN в составе монолитных интегральных схем. По ряду характеристик нитридгаллиевые усилители превосходят широко используемые в настоящее время в АФАР усилители на основе арсенида галлия GaAs. Однако для эффективного задействования потенциальных возможностей GaN-усилителей в составе контейнерной системы РЭП необходимы мощные источники энергии.

При этом выходная мощность автономных генераторных турбинах набегающего потока RAT (Ram Air Turnbine), используемых в настоящее время в составе системы РЭП AN/ALQ-99 не превышает 27 кВт. Этой мощности недостаточно для системы РЭП NGJ. Для энергетического обеспечения новой системы РЭП предполагается использовать высокомощные генераторные турбины набегающего потока HIRAT (High-power Ram Air Turbine) [222].

Управляемая поляризация помеховых сигналов может быть реализована путем взаимного расположения излучателей на полотне АФАР, при котором поляризация сигнала будет результатом сложения ортогональных векторов поляризации каждого канала [222].

Для обеспечения модульности и открытой архитектуры конструкции АФАР рассматривается технология SMART. Модули планарной АФАР, выполненной по данной технологии, являются СВЧ интегральными схемами, представляющими собой отдельные линейные АФАР. В состав таких СВЧ интегральных схем входят широкополосные излучатели и диаграммообразующие модули, которые включают в себя широкополосные усилители и линии задержки. В качестве излучающих элементов могут служить широкополосные излучатели «Вивальди» [222].

Адаптивные способы РЭП на основе системы NGJ будут реализовываться за счет создания мощных вычислительных средств, дальнейшего совершенствования технологий создания цифровых устройств сохранения и воспроизведения (DRFM) сигналов, а также новых алгоритмов их обработки.

Появление системы NGJ позволит США осуществить значительный технологический прорыв в области создания средств РЭБ. NGJ может стать основой для разработки средств РЭБ различного назначения и базирования [222].

В зарубежных СМИ отмечается, что станцией активных помех, разрабатываемой по программе NGJ, планируется оснащать самолет F-35B, который самолет разрабатывается как самолет РЭБ, его поступление в войска планируется в 2024 г. Как отмечают зарубежные эксперты, его создание обеспечит выполнение задач сопровождения боевых порядков в зоне обнаружения РЭС управления войсками и оружием. Программа предполагает размещение в подвесных контейнерах передатчиков низкого, среднего и высокого частотных диапазонов. Таким образом, ведение РЭБ в ходе воздушных операций рассматривается военным руководством США как неотъемлемый компонент боевого обеспечения и интеграция авиационных групповых

средств РЭБ в единую эшелонированную систему, что позволит успешно решать весь комплекс задач по обеспечению действий военной авиации [222].

4.7.3.3. Перспективы использования комплексов РЭБ на основе БПЛА

Обсуждение вопросов о разработке боевых БПЛА в ВС США было начато во второй половине 1990-х гг. Предложение об использовании БПЛА в качестве платформы РЭБ возникло во время ведения США боевых действий в Афганистане, при борьбе с иррегулярными воинскими формированиями. Применение БПЛА из-за его низкой стоимости, отсутствия летного состава позволяет установить дополнительное вооружение и использовать его в самых опасных районах боевых действий. Разработка БПЛА, способных вести разведку, наносить огневые удары по различным целям и при необходимости применять средства РЭБ, ведется в США, Франции, Швеции, Великобритании и других странах [250, 257].

Кроме того, ведущие фирмы США и НАТО разрабатывают БПЛА нового класса – разведывательно-ударные. К подобному классу относится многоцелевой БПЛА RQ-1 Predator (США) и его последние модификации, которые должны нести современную разведывательную аппаратуру (БРЛС TESAR, СРТР LR-100, оптико-электронный комплекс «Скайболл», телевизионную ТВ- и ИК-аппаратуру и др.), мощное бомбовое и ракетное вооружение. Рассматриваются варианты, в соответствии с которым на перспективные модификации разведывательно-ударных БПЛА будет также устанавливаться и аппаратура РЭБ [257].

Так, в 2014 г. США успешно апробировали в операциях в Ираке и в Афганистане комплексы РЭБ NERO (Networked Electronic Warfare, Remotely Operated), предназначенные для БПЛА MQ-1C «Grey Eagle», которые являются модификацией комплекса CEASAR (Communications Electronic Attack with Surveillance And Reconnaissance), устанавливаемого на самолете С-12. Комплекс NERO позволил вести радио- и радиотехническую разведку РЭС и средств связи, а в режиме излучения помех – успешно подавлять транкинговые и сотовые средства связи, беспроводные радиосети (типа Wi-Fi), а также радиовзрыватели мин. Успешная апробация комплекса NERO дала возможность применить средства РЭБ на БПЛА с учетом решения задач его авто-

номного полета и управления, а также задач электромагнитной совместимости комплекса РЭБ и радиоканалов управления БПЛА.

Назначением БПЛА, оснащенных комплексами РЭБ, является решение таких задач, как:

- проведение первоначальной разведки в оперативной глубине;
- формирование целеуказаний для пилотируемых летательных аппаратов и высокоточного оружия;
- проведение электронной атаки на системы управления и связи противника;
- нанесение высокоточных ударов по объектам противника и подавление/уничтожение систем и средств ПВО.

В настоящее время БПЛА применяются преимущественно для ведения разведки, наблюдения и организации связи. На стратегическом уровне управления основной функцией БПЛА является РРТР, в ходе которой они должны осуществлять перехват сигналов, их анализ и формирование карты радиоэлектронной обстановки. Одновременно происходит пополнение баз данных/библиотек РЭС, расположенных в районе патрулирования. На оперативном уровне решаются задачи по ведению разведки, в том числе видовой, формированию целеуказаний системам оружия и выполнению радиоэлектронных атак на РЭС противника. На тактическом уровне БПЛА с помощью систем и средств РРТР могут собирать и передавать пользователям критически важные данные о радиоэлектронной обстановке и формировать целеуказания на их подавление в соответствии с замыслом командования. В перспективе размещенные на БПЛА системы и средства РЭБ должны получить наибольшее распространение именно на тактическом уровне, где они могут применяться с максимальной эффективностью, дополняя возможности систем и средств видовой разведки и РЭП, более удаленных от цели [396].

Все существующие и разрабатываемые БПЛА подразделяются на три основных класса: малые, средние, большие. Применительно к малым БПЛА оборудование РЭБ для постановки помех может размещаться на отдельных образцах при решении этими БПЛА специальных задач. Аппаратуру радиоэлектронной защиты устанавливать на них считается нецелесообразным из-за их небольших размеров и сравнительно низкой стоимости аппаратов. Наиболее перспективными с точки зрения оснащения системами и средствами РЭБ считаются средние БПЛА. Сравнительно небольшие размеры и высокая маневренность наряду с достаточной грузоподъемностью делают их эффек-

тивными средствами для проникновения в защищенные районы и проведения радиоэлектронных атак на РЭС противника. При этом для повышения степени живучести они могут оборудоваться и средствами индивидуальной радиоэлектронной защиты. На больших БПЛА из-за их высокой стоимости считается целесообразным устанавливать средства индивидуальной радиоэлектронной защиты, причем в ряде случаев постановка помех может осуществляться такими аппаратами из относительно безопасных районов [396].

Отдельно необходимо отметить маневрирующие автономные ложные воздушные цели (АЛВЦ). Они представляют собой летательные аппараты, отображающие на экране РЛС метку, идентичную отметке атакующего самолета. Корпус АЛВЦ выполнен из композиционных материалов. В ее состав входит миниатюрная станция РЭБ, генерирующая помехи для РЛС противника, что затрудняет захват и сопровождение атакующих средств ПВО самолетов. Маневрирующие АЛВЦ, оборудованные средствами РЭБ, в перспективе должны найти самое широкое применение [396].

Основные ограничения при разработке систем и средств РЭБ для БПЛА – это их массогабаритные параметры и потребляемая мощность. Поскольку оборудование РЭБ с жидкостным охлаждением требует дополнительного пространства и увеличивает массу, то для БПЛА в настоящее время разрабатывается преимущественно оборудование с воздушным охлаждением. Тем не менее продолжается исследование возможности применения на этих аппаратах систем с жидкостным охлаждением. Так, на стратегическом БПЛА RQ-4 Global Hawk модификации Block 30 проводятся испытания перспективной системы PPTP ASIP, оборудованной жидкостным охлаждением [396].

Большое влияние на перспективы использования БПЛА для ведения РЭБ оказывает такой показатель, как стоимость/эффективность. Оборудование РЭБ является достаточно дорогим. Поскольку аппараты должны часто выполнять свои функции в условиях повышенного риска, то все фирмы работают над снижением стоимости оборудования, так как именно стоимость жизненного цикла БПЛА РЭБ может в итоге оказаться решающим фактором, определяющим перечень устанавливаемого на него радиоэлектронного оборудования [396].

Необходимо отметить уровень развития вычислительной техники по созданию высокоэффективных БПЛА РЭБ. Вычислительные средства, используемые на таких БПЛА, предназначены в первую очередь для таких функций, как [396]:

- анализ перехваченных сигналов по целевым параметрам (частота, направление на источник сигнала, время регистрации сигнала и т. д.);
- преобразование и классификация перехваченных сигналов для оценки радиоэлектронной обстановки, группирование сигналов и запись их в запоминающие устройства;
- идентификация РЭС (в основу которой положено использование баз данных), разработанной для использования в системах РЭБ;
- прием, преобразование сигнала РЭС и формирование помехи, наилучшим способом подходящей для ее подавления.

При этом быстродействие современных малогабаритных специализированных сигнальных процессоров является недостаточным для решения всех этих задач. При этом предполагается, что необходимый уровень при отсутствии качественных скачков в развитии вычислительной техники может быть достигнут не ранее 2025-2030 гг. [396].

Обобщая вышесказанное можно утверждать, что в ближайшем будущем комплексы РЭБ на основе БПЛА вытеснят и заменят специализированные самолеты РЭБ. Однако для этого разработчиками систем и средств РЭБ для БПЛА необходимо решить такие основные задачи технического и тактического характера, как [396]:

- определение оптимальной дистанции для эффективного проведения радиоэлектронной атаки и обеспечения должной степени живучести БПЛА;
- оснащение БПЛА радиоэлектронной аппаратурой согласно требованиям малой сигнатурной заметности. Собственные излучения являются сильными демаскирующими признаками, что повышает вероятность поражения БПЛА (например, наводящимися на излучение ракетами);
- обеспечение устойчивой связи с удаленными абонентами во время проведения радиоэлектронной атаки (собственные помехи могут привести к невозможности оперативной корректировки задач БПЛА и срыву передачи разведывательной информации другим потребителям). Одной из возможных мер является повышение степени автономности аппарата. Линии связи должны быть защищены также и от воздействия средств РЭП со стороны противника;
- обеспечение передачи больших объемов информации в реальном масштабе времени. Практически невозможно за-

программировать БПЛА на все те изменения боевой обстановки, которые могут возникнуть в ходе выполнения задачи. Решение о корректировке задач может быть принято человеком на станции управления, но для этого он должен получить исчерпывающую информацию об обстановке;

- обеспечение высокой степени надежности бортовых систем, поскольку от успешного применения БПЛА зависит безопасность пилотируемых платформ. Кроме того, БПЛА должны в значительной степени обладать свойствами автономности, чтобы функционировать в условиях временно потерянной или неустойчивой связи со станцией управления;
- возможность формирования помех необходимой мощности. Повышение мощности сигналов помех приводит к увеличению размеров БПЛА и его стоимости;
- достижение согласованности действий с экипажами пилотируемых летательных аппаратов;
- обеспечение минимального временного интервала между обнаружением цели и ее радиоэлектронным подавлением.

Таким образом, результаты анализа работ, проводимых в настоящее время в ВС США в рамках формирования новой межвидовой структуры платформ РЭБ воздушного базирования, позволяют сделать следующие выводы [257].

1. Большинство современных систем и средств воздушных платформ РЭБ в ВС США представляют собой не отдельные разрозненные элементы, а целый взаимосвязанный комплекс, в котором объем решаемых задач распределяется между платформами по принципу достижения максимальной эффективности в соответствии с текущей обстановкой. При этом наблюдается расширение перечня задач от традиционного подавления систем управления оружием, управления войсками и связью противника до подавления его систем навигации, сотовой связи и др., функционирующих в электромагнитном спектре.
2. Происходит существенное расширение номенклатуры используемых платформ, включающих пилотируемые летательные аппараты от модифицированного стратегического бомбардировщика до истребителей тактической авиации и беспилотные летательные аппараты, способные нести по-

лезную нагрузку, состав которой варьируется от средств физического уничтожения цели до средств радиоэлектронного подавления. При этом делается акцент не на создание новых пилотируемых платформ, а на модификацию существующих с максимально возможным сохранением их первоначальных тактико-технических характеристик и вооружения.

4.7.4. Наземные средства радиоэлектронной борьбы (на примере средств ВС США)

Как показано в работах [215, 249, 361, 396], основным воинским формированием, который решает задачи РР и РЭБ в США, являются батальоны разведки и РЭБ мотопехотных и бронетанковых дивизий, которые предназначены для выявления и радиоэлектронного подавления систем и средств КВ и УКВ радиосвязи и РЛС в тактическом звене, прежде всего систем разведки управления огнем наземной артиллерии, войсковой ПВО, дивизий первого эшелона взаимодействия частей сухопутных войск с армейской и фронтовой авиацией на дальности до 100 км. Кроме того, средства разведки батальона могут определять координаты РЛС наземной артиллерии войсковой ПВО и ВВС для целеуказания средствам поражения.

Ниже представлена информация о средствах РЭБ сухопутных войск США более подробно.

4.7.4.1. Современные наземные средства РЭБ

Наземная станция радиоподавления КВ и УКВ радиосвязи AN/TLQ-17A (V)1 Traffic Jam обеспечивает ведение радиоразведки в диапазоне 1,5-80 МГц и постановку радиопомех рациональной структуры в диапазоне 20-80 МГц.

В составе станции радиоразведки и радиоподавления имеются:

- радиоприемник R – 2107/TLQ-17A диапазона 1,5-80 МГц;
- радиопередатчик T – 1386/TLQ-17A диапазона 20-80 МГц;
- блок питания, комплект радиопеленгаторных антенн, радиостанция.

Станция автоматически контролирует 256 радиочастот и обеспечивает создание рациональной радиопомехи на одной частоте с контролем эффективности радиоподавления. Выходная мощность передатчика радиопомех составляет 550 Вт. Станция радиоразведки и ра-

диопомех размещается на 0,25-тонном автомобиле повышенной проходимости М-151А1/А2, прицепе М-416, М-569.

Вертолетный автоматизированный комплекс радиоразведки и радиоподавления AN/ALQ-151(V)2 Quick Fix II предназначен для поиска, радиоперехвата, радиопеленгования и постановки радиопомех средствам тактической радиосвязи.

Носителем средств комплекса является вертолет ЕН-60А (модификация вертолета UH-60A Black Hawk) или вертолет ЕН-1Х и ЕН-1Н (модификация вертолета UH-1H).

Комплекс AN/ALQ-151(V)2 Quick Fix II включает в свой состав [401, 408]:

- радиоприемник радиоперехвата R-2017/U, работающий в диапазоне 20-150 МГц;
- приемопеленгатор AN/ALQ-151, работающий в диапазоне 1,5-80 МГц;
- станцию радиопомех AN/TLQ-27A, работающую в диапазоне 20-80 МГц;
- электронно-вычислительную машину AN/UYK-19(V);
- радиостанцию AN/ARC-164.

Комплекс обслуживается одним оператором.

Среднеквадратическая угловая ошибка радиопеленгования составляет 2^0. Радиопеленгование осуществляется путем засечек радиостанции на маршруте полета (три и более засечек) или последовательным разворотом вертолета. Мощность станции радиопомех составляет 40-150 Вт в зависимости от диапазона при ширине полосы 10-25 кГц. Обеспечивается контроль эффективности постановки радиопомех [401, 408].

Радиоразведка и постановка радиопомех вертолетным комплексом осуществляются с высоты полета 60-180 м в течение 2-2,5 ч на удалении 5-15 км от линии соприкосновения войск и на глубину противника до 30 км. При этом основные помехи планируется создавать тактической радиосвязи противника преимущественно в звене «батальон-полк», т.е. в боевых единицах, действия которых, по мнению американских экспертов, в наибольшей степени сковываются при потере управления [401, 408].

Комплекс Quick Fix II взаимодействует с наземной системой радиоразведки AN/TSQ-114A Trailblazer, которая включает в себя 3 автоматических дистанционно управляемых пеленгатора и 2 станции радиоперехвата и управления синхронным пеленгованием, производимым со скоростью 6 целей в минуту [408].

Планы модернизации комплекса предусматривали создание системы Advanced Quick Fix AN/ALQ-151(V)3, которая должна была стать составной частью воздушного компонента перспективной системы разведки и электронной войны IEWCS (Intelligence and Electronic Warfare Common Sensor). Однако в связи со сворачиванием программы IEWCS, система AN/ALQ-151(V)3 эксплуатируется как самостоятельный вертолетный компонент РЭБ [401].

Мобильная система радиоэлектронной борьбы EFVS (Electronic Fight Vehicle System) наземного базирования была разработана фирмой «FMC» (США) и установлена на гусеничном БТР. Система EFVS снабжена телескопической антенной высотой 20 м. В этой системе используется часть комплекса универсальных датчиков разведки и РЭБ IEWCS, созданного для обеспечения радиоэлектронной поддержки, радио- и радиоэлектронной разведки [250].

Системами EFVS и AN/ALQ-151 оснащены бронетанковые и механизированные дивизии. Воздушно-десантные и «легкие» дивизии оснащены системами GBCS-L и AN/ALQ-151 [250].

В состав системы EFVS входят [250]:

- оборудование объединенной системы распределения тактической информации JTIDS;
- оборудование скрытных систем передачи больших объемов информации в речевой форме;
- оборудование передачи данных усовершенствованной системы определения местоположения войсковых объектов EPLRS.

В дополнение к системе EFVS в ВС США по-прежнему используются наземные системы РЭБ, которые дополняют систему EFVS, а именно [250]:

- тактическая система помех средствам связи в ОВЧ-диапазоне AN/MLQ-34 TACJAM, размещенная на гусеничном шасси M1015;
- система обнаружения средств связи ВЧ, ОВЧ и УВЧ-диапазонов и создания для них помех AN/TLQ-17A Traffic Jam, установленная на грузовой автомашине;
- система перехвата сигналов радиосвязи и их анализа AN/TRQ-32 Teammat», размещенная в аппаратной кабине машины M1028;
- система обнаружения и идентификации РЛС противника AN/MSQ-103 Team Pac», установленная на шасси M1015;

- система перехвата сигналов средств связи и пеленгации их источников AN/TSQ-114 «Trailblazer», также установленная на шасси M1015.

Наземно-воздушный комплекс разведки и радиоэлектронной войны AN/MLQ-40 Prophet. В основу структурно-схемных решений системы Prophet положены наработки по программе IEWCS, которая после девяти лет реализации была закрыта. Основу системы «Prophet» составляют наработки полученные по программам наземного (GBCS-H/L) и воздушного (AN/ALQ-151(V)3 Advanced Quick Fix) компонентов IEWCS. При этом система Prophet строится преимущественно на базе использования коммерчески доступных компонентов и технологий, что, по мнению разработчиков, позволит существенно снизить общую стоимость системы и сократить время на ее модернизацию [453].

Главной задачей наземно-воздушного комплекса разведки и радиоэлектронной войны AN/MLQ-40 «Prophet» является предоставление командирам тактического звена управления точных и своевременных данных о радиоэлектронной обстановке в зоне боевых действий, а также обеспечение полного информационного превосходства над противником. В настоящее время это основной перспективный многосенсорный разведывательный комплекс тактического звена управления (поступает на вооружение формируемых бригад, а также отдельных полков), предназначенный для ведения радио- и радиотехнической, специальной технической разведки, а также радиоэлектронной войны [452].

Комплекс AN/MLQ-40 Prophet выполняет следующие задачи:

- ведет радио- и радиотехническую разведку;
- предварительно обрабатывает данные для формирования карты текущей радиоэлектронной обстановки;
- определяет координаты источников радиоизлучений для обеспечения целеуказания и оценки нанесенного ущерба;
- осуществляет радиоэлектронное подавление средств радиолокации и связи в зоне своей ответственности.

Комплекс AN/MLQ-40 Prophet состоит из подсистем: управления и контроля РЭО.

Подсистема контроля. С помощью нее осуществляется постановка задач и контроль за компонентами воздушного и наземного базирования, а также сбор, обработка и предварительная оценка поступающих от них данных. Аппаратура подсистемы контроля обеспечивает обмен информацией с оперативными разведывательными органа-

ми дивизионного звена управления (группой анализа и управления, бригадной группой анализа и управления ASAS), а также позволяет использовать комплекс Prophe» в качестве удаленной станции разведки системы ASAS. При этом планируется объединить подсистему контроля Prophet с перспективной системой сбора, обработки и распределения разведывательной информации СВ (DCGS-A) [452, 453].

Подсистема контроля позволяет в реальном масштабе времени отображать данные об обнаруженных излучающих объектах для формирования карты радиоэлектронной обстановки на поле боя. Кроме того, данная подсистема имеет возможность отслеживать перемещение радиоизлучающих объектов во время их передислокации. Подсистема контроля комплекса AN/MLQ-40 Prophet состоит из двух идентичных комплектов аппаратно-программных средств, что обеспечивает эффективную защиту подсистемы, раздельное базирование, работу в движении и непрерывность функционирования при передислокации [452, 453].

Воздушная подсистема обеспечивает РРТР и РЭП формирований, находящихся на удалении 15-20 км от переднего края района боевых действий. В качестве носителей для этой подсистемы рассматриваются вертолет ЕН-60 Quick Fix и тактические БПЛА – Hanter и Shadow 200. Воздушная подсистема Prophet способна обнаруживать, идентифицировать, определять местоположение, а также осуществлять радиоэлектронное подавление источников радиоизлучения. С помощью воздушной подсистемы предполагается обеспечить эффективное ведение радиоразведки в диапазоне частот 20-2000 МГц в зоне ответственности размером 150×50 км. Точность определения местоположения целей будет зависеть от дальности до них и составит на расстоянии до 40 км – 150-500 м, на расстоянии 80-120 км – от 450 до 1500 м [452, 453].

Наземная подсистема предназначена для непосредственной поддержки боевых бригад. Основой наземной подсистемы данного комплекса, получившего обозначение AN/MLQ-40(V)2, являются приемо-пеленгаторная станция AN/PRD-13, состоящая из одного пеленгаторного приемника, работающего в диапазоне частот от 20 МГц до 2 ГГц, и двух контрольных (для перехвата радиосообщений) приемников. AN/MLQ-40, в отличие от предыдущих станций, имеет увеличенную полосу обзора, что позволяет проводить пеленгацию с автоматическим нанесением полученных данных на цифровую карту местности, осуществлять в движении обнаружение и пеленгацию целей, а также более низкие акустическую и тепловую сигнатуры. Аппаратура

комплекса монтируется на автомобиле HMMWV, оснащенном антенной на 6- метровой выдвижной мачте. Время развертывания станции составляет 2 мин [452].

Последняя модификация наземных станций AN/MLQ-40(V)3, может функционировать в трех вариантах: стационарно с 6-метровой телескопической антенной, в движении, а также в виде переносной станции PPTP с пеленгатором AN/PRD-13(V)2. Аппаратура AN/MLQ-40(V)3 позволяет перехватывать обычные сигналы с амплитудной и частотной модуляцией, а также более сложные типы сигналов. Оборудование станции AN/MLQ-40(V)3 включает блок аппаратуры PPTP в кузове машины и переносную станцию AN/PRD-13(V)2. Встроенная аппаратура состоит из приемника-анализатора MD-405A, трех антенн: телескопической, пеленгаторной MA-723 и направленной (логопериодической) антенны MA-458, а также из переносного компьютера и трех рабочих мест операторов. Вместе с тем помимо радиостанции AN/PRD-13(V)2 к AN/MLQ-40(V)3 может подключаться и другая аппаратура связи, имеющая возможность передачи как голосовых сообщений, так и цифровых данных [452].

Планами командования сухопутных войск предусматривается, что комплекс «Prophet» будет функционировать как составная часть ВВТ перспективных боевых формирований FCS, боевых бригад различного функционального предназначения, а также формирований разведки и РЭБ, непосредственно подчиненных органам управления дивизионного уровня. Он позволит осуществлять визуализацию боевого пространства, проводить разведывательную подготовку боевых действий, выполнять мероприятия по выявлению и определению приоритетности целей, проводить подготовку и давать целеуказания, а также решать задачи радиоэлектронного подавления РЭС противника [452].

Дальнейшая модернизация комплекса Prophet велась за счет разработки станции AN/MLQ-40(V)4, в состав которой входит станция помех AN/USQ-146(V) (2-2500 МГц), а также приемо-пеленгаторный комплекс станции «Prophet» Block I (20 МГц – 3 ГГц) с возможностью отображения в реальном масштабе времени источников излучения на цифровой карте радиоэлектронной обстановки. Модернизация комплекса «Prophet» Block I в вариант Block II/III завершилась в 2005 г. Дальнейшее совершенствование комплекса «Prophet» велось за счет разработки следующих двух версий – это Block IV и Block V. Block IV состоит на вооружении разведывательных формирований бригадного уровня и обеспечивает ведение радио- и радиотехнической, а также

специальной технической разведки, а Block V – на вооружении бригад разведки поля боя перспективных формирований сухопутных войск и дополнительно оснащается миниатюрными необслуживаемыми датчиками. Эти модификации, которые приняты на вооружение после 2008 г., и представляют собой многофункциональные разведывательные комплексы с акустическими, инфракрасными и радиолокационными датчиками [452].

Полностью развернутый наземный комплекс будет состоять из пяти машин: двух машин РРТР и РЭБ, двух машин специальной технической разведки и одной машины управления [452].

По оценке американских специалистов, перспективный комплекс РРТР и РЭБ «Prophet» будет способен обнаруживать все современные типы сигналов, определять местоположение целей с точностью, необходимой для их поражения средствами летального воздействия, осуществлять радиоэлектронное подавление средств связи, радиолокации и сигналов КРНС противника, подготавливать точные данные об излучающих объектах на поле боя, обеспечивать защиту своих войск. Данные комплексы будут обладать необходимой в современных условиях боевой обстановки универсальностью и мобильностью, что позволит быстро их перебрасывать в районы предназначения [452].

4.7.4.2. Перспективные наземные средства РЭБ

В конце XX века под влиянием концепции сетецентрического управления в вооруженных силах США начали прорабатываться проекты построения единых децентрализованных многоэшелонированных систем разведки и РЭБ. При этом наибольших успехов в этом направлении добились производители авиационных комплексов РЭБ. В таких системах специализированные самолеты РЭБ, предназначенные для групповой защиты боевых порядков, дополняются режимами излучения помех встроенными в АФАР самолетов истребительной и штурмовой авиации. В самое ближайшее время к этой связке будут добавлены специализированные БПЛА РЭБ, которые будут действовать в зонах ПВО противника. Подобное объединение планировалось и для сухопутных систем РЭБ, однако практика боевых действий в Ираке и Афганистане внесла свои коррективы.

Придорожные осколочно-фугасные самодельные взрывные устройства направленного действия инициировались звонком на установленные в них простейшие мобильные телефоны. Именно от них

американский войсковой контингент в Ираке и Афганистане понес наибольшие безвозвратные потери [455].

К 2005 г. сухопутные войска США в экстренном порядке разработали и приняли на вооружение систему РЭБ «Duke», предназначенную для радиоэлектронного противодействия радиоуправляемым самодельным взрывным устройствам за счет подавления сигналов мобильной связи и беспроводных радиосетей (типа Wi-Fi), используемых для дистанционного управления этими устройствами. В дальнейшем командование сухопутных войск перешло к проработке вопросов создания «Интегрированной системы электронной войны» «IEWS» (The Integrated Electronic Warfare System), которая частично заимствует наработки программы «IEWCS», закрытой в 1998 г., но с учетом новейших тенденций, ориентированных на использование децентрализованных сетецентрических технологий.

Интегрированная система электронной войны «IEWS». Система «IEWS» (Integrated Electronic Warfare System) является наземной системой РЭБ, основанной на модульной масштабируемой открытой архитектуре, которая предназначена для проведения радиоэлектронных атак против противника и обеспечения радиоэлектронной защиты сухопутных войск в тактическом и оперативно-тактическом звеньях управления [456].

Система «IEWS» включает в себя три подсистемы [456]:

1. многофункциональный комплекс РЭБ «MFEW» (Multi-Function Electronic Warfare);
2. комплекс планирования и управления радиоэлектронной борьбой «EWPMT» (Electronic Warfare Planning and Management Tools);
3. комплекс радиоэлектронной защиты «DEA» (Defensive Electronic Attack).

Многофункциональный комплекс РЭБ «MFEW» объединит единым управлением наземные средства РЭБ, а также средства РЭБ воздушного базирования на самолетах и БПЛА и обеспечит проведение радиоэлектронных атак, а также радиоэлектронную защиту подразделений оперативно-тактического звена до бригады включительно. Основные усилия разработчиков комплекса направлены на разработку программного обеспечения, которое позволит организовать совместные действия разнородной территориальнораспределенной группировки средств РЭБ наземного и воздушного базирования. Кроме того, большое внимание уделяется разработке новых маломощных режимов

излучения помех при совместном использовании различных средств РЭБ [456, 457].

Комплекс планирования и управления радиоэлектронной борьбой «EWPMT» в автоматизированном режиме обеспечит подготовку решения по планированию электромагнитного спектра между различными средствами связи, РРТР и РЭБ, а также по скоординированным режимам работы вышеуказанных средств, в зависимости от решаемых боевых задач и воздействия средств РЭБ противника. Комплекс EWPMT представляет собой систему интеграции данных о возможных и текущих режимах работы различных РЭС – РЛС управления огнем, РЛС опознавания и наведения, средств связи, средств РРТР и РЭБ и т.д. Комплекс EWPMT позволяет в режиме реального времени сформировать и визуализировать общую картину электромагнитной оперативной обстановки с учетом режимов работы своих радиоэлектронных средств и аналогичных средств противника. Американские эксперты считают, что комплекс «EWPMT» выступит своеобразной АСУ, интегрирующей в себе функции управления режимами работы своих РЭС (радиолокации и связи), функции координации режимов работы средств РРТР и РЭБ, а также функции хранения, идентификации и моделирования текущих и возможных режимов работы РЭС противника. Это позволит обеспечить информационное превосходство сухопутных войск США при планировании электромагнитного спектра, а также решение задач радиоэлектронного подавления противника при одновременной электромагнитной совместимости своих радиосредств [456, 457].

Комплекс радиоэлектронной защиты «DEA» основан на разработках, выполненных по программе «Duke», и обеспечивает защиту сил и средств, передвигающихся на транспортных средствах, а также находящихся на стационарных местах дислокации от радиоуправляемых самодельных взрывных устройств. Фактически комплекс «DEA» является распределенной интегрированной системой управления носимыми и возимыми индивидуальными и групповыми средствами защиты от самодельных взрывных устройств. Индивидуальные средства предназначены для защиты отделения или отдельных военнослужащих, а возимые групповые средства, размещаемые на машинах в составе – для защиты передвижных групп, эшелонов или мест постоянной дислокации подразделений. Эти средства были разработаны по программе «Duke» и ориентированы на обнаружение, идентификацию и подавление помехами средств мобильной и транкинговой связи, радиосредств Wi-Fi и других подозрительных излучений, которые могут

быть использованы иррегулярными воинскими формированиями для подрыва самодельных взрывных устройств. Объединение таких средств защиты в единую распределенную систему позволит получать оперативную информацию о подозрительной активности в радиодиапазоне, определении координат источников радиоизлучения, привязке этих данных к цифровой карте местности, коррекции маршрутов движения подразделений и воинских эшелонов в реальном масштабе времени, а также вести целеуказание для нанесения огневых ударов [456, 458].

Таким образом, развитие современных наземных средств РЭБ ведется по пути интеграции разнородных наземных систем в единые территориальнораспределенные разведывательно-ударные комплексы РЭБ. При этом в наземные системы активно интегрируются воздушные компоненты – самолеты и БПЛА, которые ведут РРТР и РЭП на больших расстояниях в интересах подразделений сухопутных войск.

4.7.5. Функциональное поражение радиоэлектронных средств электромагнитным излучением

4.7.5.1. Общие принципы функционального поражения радиоэлектронных средств электромагнитным излучением

Функциональное радиоэлектронное поражение электромагнитным излучением (ЭМИ) – функциональное поражение РЭО, заключающееся в разрушении и/или повреждении элементов РЭО противника электромагнитным излучением. Оно может проводиться путем использования однократных или многократных импульсных электромагнитных воздействий, приводящих к необратимым изменениям электрофизических параметров в полупроводниковых или оптико-электронных элементах РЭС в результате их перегрева или пробоя [251, 255].

Основным отличием функционального радиоэлектронного поражения от РЭП являются физические принципы нанесения РЭС ущерба. При функциональном радиоэлектронном поражении ущерб причиняется путем необратимого (катастрофического) или обратимого (восстанавливаемого) изменения физико-химической структуры элементов РЭС вследствие воздействия электромагнитных полей на материалы, входящие в состав электронных и полупроводниковых приборов и других компонентов этих систем. Эффект воздействия средств функционального радиоэлектронного поражения на РЭС основан на

возможности изменения физико-химических свойств электро- и радиоматериалов при облучении их сильными ЭМП. Необратимые изменения свойств вещества, приводящие к качественно новым образованиям с иной электромагнитной структурой, происходят при значительной энергии воздействующего ЭМИ [248].

В зависимости от мощности, длительности импульсов, рабочей частоты источника ЭМИ и расстояния до РЭС эффекты от электромагнитного воздействия могут быть различными – от кратковременного снижения качества функционирования и временной потери работоспособности РЭО до его полного повреждения или разрушения за счет перегрева или полевого пробоя [248].

Поражающее воздействие ЭМИ на РЭС осуществимо как в полосе их рабочих частот, так и по побочным каналам [248].

При воздействии ЭМИ на метровых и более длинных волнах на металлических корпусах РЭС наводятся значительные ЭДС, отказывают различные электронные схемы и исполнительные элементы. При воздействии ЭМИ в дециметровом или сантиметровом диапазоне волн, совпадающем с рабочим диапазоном РЭС, повреждаются входные устройства (в частности, СВЧ-диоды). Миллиметровые волны проникают в щели экранов, повреждая как входные цепи, так и экранированные микропроцессорные устройства. При взаимодействии мощных СВЧ-колебаний с элементами и узлами РЭС могут наблюдаться два эффекта [251]:

1. наведение на контурных элементах (выводах полупроводниковых приборов, печатных проводниках и т.д.) СВЧ-мощности, которая приводит к электрическим перегрузкам;
2. непосредственное взаимодействие СВЧ-импульсов со структурой полупроводникового элемента.

Мощности ЭМИ, формируемых известными средствами функционального радиоэлектронного поражения, могут превышать десятки гигават, длительности импульсов ЭМИ лежат в пределах от миллисекунд до наносекунд. При этом в большинстве практических случаев функциональное поражение РЭС при применении ЭМИ имеет место при отказе хотя бы одного из основных его полупроводниковых элементов.

Основными недостатками средств функционального поражения ЭМИ являются [245, 248, 251]:

- плохая электромагнитная совместимость (этот недостаток может быть ограничен разнесением РЭС в пространстве, использованием направленных антенн и внедрением инди-

видуальных устройств защиты собственных РЭС от мощного ЭМИ);
- негативное воздействие мощного ЭМИ на биологические объекты.

К достоинствам средств функционального поражения ЭМИ можно отнести [245, 248, 251]:
- расширение круга решаемых задач, за счет возможности выведения из строя РЭС, не излучающих в пространство;
- очень высокую степень универсальности поражения, эффективное воздействие на РЭС с высокой помехозащищенностью;
- снижение в ряде случаев требований к качеству развединформации (по местоположению, частотному диапазону, параметрам сигналов), которая необходима для поражения РЭС противника;
- отказ от сложнейших средств анализа и имитации сигналов подавляемых РЭС, которые традиционно используются в РЭП;
- внеполосность (способность ЭМИ проникать внутрь РЭС помимо их полосы пропускания);
- эффективность функционального поражения ЭМИ практически не зависит от функционального назначения этих РЭС.

Электромагнитное оружие (ЭМО). Принцип действия электромагнитного оружия основан на кратковременном электромагнитном излучении большой мощности, способном вывести из строя РЭС, составляющие основу любой информационной системы. Элементная база РЭС весьма чувствительна к энергетическим перегрузкам. Поток электромагнитной энергии достаточно высокой плотности способен выжечь полупроводниковые переходы, полностью или частично нарушив их нормальное функционирование. Даже у кремниевых сильноточных биполярных транзисторов, обладающих повышенной стойкостью к перегревам, напряжение пробоя составляет 15-65 В, а у арсенид-галлиевых приборов – 10-12 В. Запоминающие устройства имеют пороговые напряжения порядка 7 В, типовые логические интегральные схемы на МОП-структурах – 7-15 В, а микропроцессоры обычно прекращают свою работу при 3,3-5 В [248].

Кроме того, анализ результатов отечественных и зарубежных исследований воздействия импульсов ЭМИ наносекундного диапазона напряженностью 2-10 кВ/м (при частоте следования импульсов поряд-

ка 1 МГц) на вычислительные блоки и микропроцессоры РЭС показал, что уровни наводимых напряжений приводят к отказам этих элементов и ложным срабатываниям в них, что делает практически невозможным корректное функционирование в них программного обеспечения [83, 128].

Перспективность этого вида оружия, прежде всего, связана с широким распространением в мире электронной техники, которая решает весьма ответственные задачи, в том числе и в сфере безопасности. В настоящее время, когда войска и инфраструктура многих государств до предела насыщены электроникой, внимание к средствам ее поражения стало весьма актуальным. Хотя электромагнитное оружие характеризуется как несмертельное, специалисты относят его к категории стратегического, которое может быть использовано для выведения из строя объектов системы государственного и военного управления [300].

Электромагнитное оружие может быть создано как в виде стационарных и мобильных электронных комплексов направленного излучения, так и в виде электромагнитных боеприпасов, доставляемых к цели с помощью снарядов, мин, управляемых ракет, авиабомб и т.п.

Таблица 4.9. Характеристика некоторых видов электромагнитного оружия [14]

Вид оружия	**Вероятность применения**	**Радиус поражения**	**Поражаемые цели (в зависимости от частоты излучения)**	**Потенциальные пользователи**
Ядерный генератор электромагнитного излучения большой амплитуды	Умеренная	В радиусе до 2400 км	Электронное оборудование, компьютеры, датчики, связь, автомобили, системы передачи энергии, элементы гражданской инфраструктуры.	Ядерные державы, обладающие баллистическими ракетами.

Окончание табл. 4.9

Вид оружия	Вероятность применения	Радиус поражения	Поражаемые цели (в зависимости от частоты излучения)	Потенциальные пользователи
СВЧ-оружие	Низкая	Существующие СВЧ средства пока не излучают энергии, достаточной для поражения интегральных схем на достаточном расстоянии.	Интегральные схемы, печатные платы, переключательные реле.	США, Англия, Австралия, Россия, Швеция.
Электромагнитные бомбы (взрывомагнитный генератор)	Высокая	~ 175 м	Незащищенные радиоэлектронные системы, соединенные проводами длиной более 75 м.	Террористы.
Осциллирующий виртуальный катод, СВЧ-генератор типа «варикатор»	Умеренная	~ 150 м	Интегральные схемы, переключательные реле.	Любая страна.

Более подробные сведения о функциональном поражении на основе ЭМИ представлены в работах [83, 128, 213, 245, 248, 251, 462].

4.7.5.2. Особенности радиоэлектронного поражения СВЧ-излучением

Основу оружия функционального поражения составляют мощные СВЧ-генераторы сантиметрового и миллиметрового диапазонов [250].

Сверхвысокочастотное оружие (СВЧ-оружие) – электромагнитное оружие, поражающим фактором которого является сверхмощное электромагнитное излучение СВЧ-диапазона (0,3-300 ГГц). Ввиду того что к СВЧ- диапазону довольно часто применяется обобщенное понятие «микроволновое излучение», то иногда СВЧ-оружие называют «микроволновым оружием».

СВЧ-оружие (или микроволновое, HPM – High Power Microwave) является разновидностью радиочастотного оружия (RFW – Radio Frequency Weapon) и использует принцип функционального радиоэлектронного поражения ЭМИ.

Вместе с тем СВЧ-оружие специально выделяется из радиочастотного оружия вследствие ряда его существенных преимуществ [14]:

- малая длина волны позволяет передавать поражающую энергию с меньшими потерями;
- большинство целей имеют так называемые «окна уязвимости» в определенных диапазонах частот, что позволяет реализовывать малоэнергоемкие механизмы поражения.

Источниками мощного ЭМИ для СВЧ-оружия могут быть энергия ядерного взрыва, мощные релятивистские СВЧ-генераторы (взрывомагнитные, магнитокумулятивные), обычные электровакуумные СВЧ-генераторы (усилители), в том числе с временной компрессией излучаемых импульсов, твердотельные генераторы с полупроводниковыми коммутаторами, генераторы с газовыми коммутаторами и др. В качестве излучателей также могут применяться аппретурные антенны (зеркальные, рупорные), а также ФАР и АФАР [14].

В конце 70-х гг. в связи с исследованиями термоядерного синтеза за рубежом активизировались работы в области средств функционального поражения. В лаборатории вооружения ВВС США была создана полигонная установка «Джипси» с диапазоном частот 0,8-40 ГГц, с импульсной выходной мощностью виркатора до 1 ГВт, предназначенная для исследования воздействия мощных СВЧ-излучений на образцы вооружения и РЭС различного назначения [250].

Основным показателем устойчивости элементной базы к воздействию ЭМИ являются критериальные уровни поражения, определяемые величиной мощности, при которой возникают восстанавливаемые и невосстанавливаемые отказы в элементах РЭС.

Критериальные (критические для поражаемого оборудования) уровни функционального поражения широкой номенклатуры РЭС отличаются большим разбросом и могут составлять от 10 до 5000 Вт/см^2. Типовые критериальные уровни различных полупроводниковых приборов приведены в работах [245, 251]. При этом наиболее уязвимыми элементами РЭС являются СВЧ-диоды, работающие во входных трактах преобразователей частоты, интегральные микросхемы и диоды с точечным контактом.

Развитие направления исследований по функциональному поражению РЭС за счет СВЧ ЭМИ привело к разработке так называемых взрывомагнитных генераторов (ВМГ) мощных импульсов электрического тока. Якорь такого генератора представляет собой сосредоточенный металлический проводник (лайнер), перемещаемый продуктами разлета мощного взрывчатого вещества и компрессирующий магнитное поле из объема генератора в электрическую нагрузку. Однако недостатком такого генератора является то, что он уничтожается в каждом эксперименте. Замена металлического лайнера на компактный сгусток электропроводящей плазмы позволила создать неразрушимый генератор, способный работать в режиме генерации серии мощных электрических импульсов. Взрывомагнитные генераторы имеют наилучшие массогабаритные показатели и наивысшие абсолютные значения выходной мощности. В качестве первичных накопителей энергии, используемых для запитки подобных генераторов, кроме известных емкостных и индуктивных накопителей энергии, необходимо отметить сверхпроводящие индуктивные накопители энергии, выполненные на высокотемпературных сверхпроводящих материалах, которые характеризуются сравнительно высоким значением критических магнитных полей (≈100 Тл) при токе 10^3-10^7 А и мощностью 10^{12} Вт, которая эквивалентна энергии 10^9 Дж.

Современный уровень развития СВЧ-генераторов обеспечивает выделение в нагрузке энергии 10^7-10^8 Дж, мощность которой эквивалентна мощности энергии, освобождающейся при взрыве заряда взрывчатого вещества массой 10 кг.

Наибольший эффект от использования СВЧ-оружия предполагается достигнуть за счет воздействия на радиоэлектронные системы противника критически важной военной и государственной инфра-

структуры. С его помощью можно нарушать работу любых электронных систем. Перспективные магнетроны и клистроны мощностью до 1 ГВт с использованием антенн с фазированной решеткой позволят фактически парализовать аэродромы, стартовые позиции ракет, центры и пункты управления, навигационные системы, вывести из строя системы государственного управления, системы управления войсками и оружием, а также блоки управления, установленные на управляемом оружии. Кроме того, в качестве целей для СВЧ-оружия рассматриваются системы ПВО, а также объекты, представляющие повышенную опасность для окружающей среды (химические заводы, атомные станции и др.), что позволит выводить их из строя без утечки опасных компонентов за пределы контролируемой зоны. Это выдвигает СВЧ-оружие в разряд наиболее приоритетных вооружений будущего [2, 300].

Начиная с 1995 г. за рубежом ведутся интенсивные исследования и разработки средств РЭБ функционального поражения, использующих энергию ЭМИ и СВЧ ЭМИ, с дальностью действия более 10 км, у которых мощность в импульсе достигает нескольких гигаватт, а длительность импульса составляет наносекунды. Такие средства функционального поражения используются для вывода из строя линий радиосвязи и систем управления [250].

Боевые комплексы СВЧ-оружия могут быть созданы в вариантах наземного, воздушного и космического базирования. По мнению разработчиков, возможны и другие модификации СВЧ-аппаратов, позволяющие оборудовать такими установками корабли, самолеты, вертолеты. Данное оружие может быть использовано для обнаружения и выведения из строя БПЛА-разведчиков, а также любых электронных устройств, которыми располагают войска противника [300].

Наиболее активными в области создания СВЧ-оружия сегодня являются США, Великобритания, Германия и Израиль [2].

В США работы по созданию СВЧ-оружия осуществляются всеми видами вооруженных сил, а также министерством энергетики.

Разрабатываемое в США СВЧ-оружие относится [14]:

- к тактическому (наземные, корабельные и авиационные комплексы);
- к стратегическому (наземный комплекс противокосмической обороны).

Основные направления НИОКР по СВЧ-оружию, проводимых в интересах ВС США, включают [14]:

- развитие компонентной базы;
- модельные и натурные оценки эффективности поражения (стойкости к СВЧ-излучению американских и зарубежных образцов ВВТ);
- реализацию целевых объектов создания комплексов СВЧ-оружия для вертолетов армейской авиации и беспилотных летательных аппаратов, защиты наземных объектов, а также ведения противоминной борьбы.

В США в течение нескольких десятилетий ведется разработка СВЧ-боеприпасов для установки вместо традиционных (на основе взрывчатых веществ) бетонобойных боевых частей управляемых и неуправляемых авиационных бомб, а также крылатых ракет. Такие боеприпасы планируется применять на фоне обычных огневых средств для подавления информационно-управляющей инфраструктуры противника, а также для поражения других объектов, насыщенных вычислительной и радиоэлектронной техникой [14].

Применение неразрушаемых СВЧ-генераторов в качестве основного или дополнительного вооружения носителя рассматривается американскими специалистами в следующих программах [14]:

- системы самозащиты самолетов и вертолетов;
- средства подавления ПВО на БПЛА;
- мобильные комплексы на боевых машинах и малых кораблях;
- стационарные или корабельные тактические комплексы.

В качестве типовых целей тактических комплексов СВЧ-оружия рассматриваются различные электронные компоненты ВВТ. При этом недопущение вывода из строя собственной аппаратуры носителя таких излучателей остается серьезной технической проблемой [14].

Более подробные сведения о функциональном поражении СВЧ-оружием представлены в работах [83, 128, 245, 248, 251, 462].

4.7.5.3. Средства и боеприпасы функционального поражения СВЧ-излучением (на примере средств ВС США)

Согласно сообщениям зарубежных СМИ американские военнослужащие в ходе боевых действий в Ираке в интересах натурных

испытаний применяли также экспериментальные образцы боеприпасов, создающие мощный электромагнитный импульс, в том числе СВЧ-диапазона. Принцип действия ЭМИ-боеприпаса основан на создании при взрыве мощного направленного электромагнитного излучения, способного выводить из строя радиоэлектронную аппаратуру и системы электроснабжения. По механизму воздействия это излучение подобно ЭМИ ядерного взрыва [338].

Современные средства функционального поражения условно можно разделить [250]:

- на мобильные;
- на одноразового действия;
- на малогабаритные.

Мобильные СВЧ-средства функционального поражения используют диапазон частот от 0,5 до 20 ГГц и работают с частотой повторения импульсов 10 Гц при длительности импульса 200-1000 нс; импульсная мощность излучения может достигать 1-5 ГВт, энергия в импульсе – 2-10 кДж; тип энергоустановки – газотурбинный генератор, тип генераторного прибора – гираторы, виркаторы, черенковский генератор; КПД генераторного прибора 36-40%, КПД установки в целом – 20-25 %; масса 6-10 т; размещение – автомобиль, бронетранспортер; диаметр антенны 2-5 м; дальность действия – в пределах прямой видимости [250].

СВЧ-средства функционального поражения одноразового действия используют диапазон частот 6-10 ГГц, развивают мощность в импульсе 3-5 ГВт при длительности импульса 150-1500 нс; тип генераторного прибора – взрывомагнитный генератор, резонансный магнетрон, виркатор; масса 500 кг, дальность действия 3-4 км [250].

Малогабаритные СВЧ-средства функционального поражения используют диапазон 0,5-100 ГГц, имеют импульсную мощность 1-5 ГВт; импульс длительностью 1-100 нс; тип генераторного прибора – взрывомагнитный генератор, ударно-волновой генератор; масса 40-50 кг; дальность действия 1-2 км [250].

В 1991 г. во время операции «Буря в пустыне» американское командование впервые применило в Ираке СВЧ-оружие. Так, с целью повышения эффективности информационной войны, ведущейся в интересах идеологической обработки гражданского населения, для подавления телевизионных передач в Багдаде в район расположения телецентра была сброшена так называемая «электронная бомба», являющаяся оружием функционального поражения радиоэлектронных систем. В результате взрыва специального заряда этой бомбы образовал-

ся мощный электромагнитный импульс, действие которого нарушило работу телецентра. Во время этой же операции ВМС США для подавления радиоэлектронных систем управления и связи Ирака использовали в нескольких из 116 запущенных ракет Tomahawk боевые части, создающие мощный электромагнитный импульс. Примененная в ракете БЧ при взрыве излучала СВЧ-импульс мощностью 5 МВт [245].

Интересным является то, что за несколько месяцев до начала иракской кампании многими экспертами давались оценки, согласно которым подобные СВЧ-боеприпасы могут появиться не ранее 2005 г. Это позволяет говорить о том, что по итогам кампании 1999 г. против Югославии, в которой впервые были применены средства вывода из строя систем энергоснабжения типа графитовых бомб, руководством Пентагона было принято решение об интенсификации работ по созданию эффективного электромагнитного оружия [2].

При этом командование коалиционных сил относилось к применению СВЧ-боеприпасов с особой осторожностью, так как крылатые ракеты достаточно эффективно сбиваются средствами ПВО, а это могло привести к попаданию отдельных узлов и деталей принципиально нового средства поражения к противнику, а от него – в третьи страны, что привело бы к утрате США приоритета в разработке этого вида оружия [2].

Следует также отметить, что ряд потерь авиационной техники коалиционных сил связан с отказом их электроники именно в результате применения США СВЧ-оружия. Это может свидетельствовать о том, что технология таких боеприпасов еще недостаточно отработана. Можно также констатировать то, что еще не найдено эффективной защиты собственных электронных систем от воздействия СВЧ излучения [2].

Одним из исследуемых в США вариантов электромагнитного оружия является СВЧ-боеприпас, выполненный на базе управляемой авиационной бомбы GBU-31 и оснащенный взрывомагнитным генератором, устанавливаемым в корпусе осколочно-фугасной БЧ Мк84 калибра 2000 фунтов. Для КРВБ и управляемых ракет класса «воздух-земля» разрабатываются специальные БЧ, создающие мощный электромагнитный импульс. В дальнейшем предполагается создание образцов СВЧ-боеприпасов, которые смогут обеспечить вывод из строя оборудования, расположенного в заглубленных объектах (расчетная глубина поражения СВЧ-излучением 40-50 м) [338].

В перспективе в США намечено разработать образцы СВЧ-боеприпасов, создающих излучение гигаваттного уровня мощно-

сти. При этом радиус зоны поражения таких боеприпасов может составлять сотни метров. В частности, предполагается создание СВЧ-боеприпасов в корпусах проникающих боевых частей, что, по оценкам специалистов США, обеспечит вывод из строя оборудования, расположенного в заглубленных объектах [14].

В 2009 г. ВВС США заключили с фирмой «Боинг» контракт, предусматривавший разработку в течение трех лет в рамках проекта CHAMP (Counter-electronic High Power Microwave Advanced Missile Project) демонстрационного образца нелетального СВЧ-оружия, размещаемого на борту крылатой ракеты либо другой воздушной платформе. Оно предназначено для подавления электронных устройств противника без нанесения повреждения корпусу или иным силовым структурам технических либо боевых средств противника. Основу этого оружия составляют перезаряжаемые емкостные накопители, а также генераторы с АФАР и электронным управлением лучом [119].

Фирма «Боинг» разрабатывает крылатую ракету воздушного базирования большой дальности и управляемые бомбы серии «Джейдам-ER» с перспективными СВЧ боевыми частями, а фирма «Рейтеон» – боеприпас «MALD-V» на базе малогабаритной автономной ложной воздушной цели ADM-160 MALD. В настоящее время предполагается провести серию полномасштабных наземных и воздушных испытаний этих демонстрационных образцов, созданных на основе компактных СВЧ-технологий. Так, в октябре 2012 г. экспериментальная крылатая ракета осуществила подлет к комплексной цели из семи зданий (полет продолжался около 1 ч) и мощным электромагнитным импульсом вывела из строя находившиеся в них компьютеры при минимальном их физическом повреждении, а затем вернулась в заранее указанное место и приземлилась. ВВС США ожидают, что вышеуказанная технология будет окончательно доработана и поступит на вооружение после 2016 г. Кроме того, планируется оснастить крылатую ракету AGM-86 ALCM СВЧ-генератором, способным за время полета произвести несколько «выстрелов», и протестировать ее [119].

Особое место среди СВЧ-систем занимает СВЧ-боеприпас, поражающее воздействие которого на радиоэлектронную аппаратуру противника осуществляется мощным электромагнитным излучением, генерируемым в результате взрыва. В 2009 г. в США проводились испытания нового образца такого боеприпаса. Его пиковая мощность составила 35 МВт при длительности импульсов 100-150 нс в диапазоне 2-6 ГГц. Длина устройства 1,5 м, диаметр около 0,15 м. В основу СВЧ-боеприпаса положены способы преобразования кинетической

энергии взрыва, горения и электрической энергии постоянного тока в энергию электромагнитного поля высокой мощности [119].

ВМС США также имеют на вооружении экспериментальные ракеты, неядерные головные части которых оснащены взрывомагнитными генераторами СВЧ-излучения. Часть таких ракет флот использовал на начальном этапе войны в 1991 г. в Персидском заливе для подавления/поражения электронных систем и средств ВС Ирака. Но определить эффективность применения таких ракет невозможно, так как для решения тех же задач одновременно применялись традиционные средства РЭБ [119].

Помимо разработки СВЧ боевых частей ведется разработка бортовых СВЧ-генераторов для оборудования БПЛА типа BQM-145A. СВЧ средствами поражения предположительно будут оснащаться и экспериментальный беспилотный самолет X-45 и его палубная модификация X-47. Разрабатывается также проект оснащения мощным микроволновым генератором и транспортного самолета C-130 Hercules для создания на его основе самолета подавления ПВО по образцу модели AC-130 Spectre огневой поддержки. Однако в рамках этого проекта разработчикам так и не удалось решить вопросы эффективной защиты бортовой радиоаппаратуры от СВЧ-излучения. Эксперты отмечают, что опасность повреждения собственной аппаратуры не позволит в ближайшее время в полной мере использовать СВЧ-генераторы на пилотируемых летательных аппаратах [2].

Кроме указанных разработок ведутся работы по созданию нескольких модификаций СВЧ-излучателей для корпуса морской пехоты и военно-морских сил США. Так, командование морской пехоты планирует устанавливать СВЧ-излучатели на транспортно-десантных средствах для их использования при ведении боевых действий в городских условиях, а также в качестве нелетального оружия для управления толпой. Военно-морские силы США планируют использовать СВЧ-генераторы в качестве одного из основных компонентов противоракетной обороны кораблей [2].

Большое внимание в США уделяется созданию бортовых авиационных систем СВЧ-оружия в виде как отдельных боевых подсистем, так и, например, путем интеграции бортовых СВЧ-средств с комплексом РЭБ самолета. В частности, ведутся работы по созданию авиационных многофункциональных РЛС с активными ФАР, предназначенных для радиоэлектронного подавления средств ПВО противника, а также индивидуальной защиты (постановки помех авиационным РЛС противника) самолета [14].

Американские вооруженные силы планируют оснастить АФАР тактические истребители, а также стратегические бомбардировщики. Ряд фирм в инициативном порядке ведут исследования по созданию систем индивидуальной защиты гражданских самолетов с применением СВЧ-оружия [14].

В США разрабатываются СВЧ-средства для защиты самолетов только в зоне аэропорта на наиболее критичных с точки зрения безопасности участках полета: взлете и посадке. Основу создаваемой зональной системы защиты «Виджилент игл» составит наземная стационарная СВЧ-установка, электромагнитное излучение которой должно вызывать временные сбои в работе или необратимые повреждения электронных элементов системы управления зенитных управляемых ракет переносных зенитно-ракетных комплексов. В ее состав войдут мощные импульсные генераторы, построенные по модульной схеме, и активная антенна из фазированных решеток с электронным управлением узконаправленным лучом. Предполагается, что дальность действия установки может составить единицы километров. По заявлению разработчиков, ее излучение не будет вызывать сбоев в работе бортовой аппаратуры самолетов, электронных компонентов инфраструктуры аэропортов и не причинит вреда здоровью людей [14, 119].

Когда датчики фиксируют стартующую зенитную ракету, приводится в действие СВЧ-установка, которая генерирует в направлении ракеты СВЧ-импульс, выводящий из строя систему управления ракетой. Для обнаружения ракет ПЗРК и их сопровождения в полете предполагается использовать несколько инфракрасных датчиков, которые планируется размещать на прилегающей к аэропорту территории (на мачтах, башнях и др.). Серийные образцы системы «Виджилент игл» предполагается разместить, в первую очередь, в наиболее крупных аэропортах США. По оценкам американских специалистов, применение системы будет эффективно только при значительном увеличении дальности действия СВЧ-установки или при размещении дополнительного числа таких установок на протяжении всего посадочного курса самолетов [14, 119].

Таким образом, развитие систем РЭБ становится наиболее эффективным, быстрореализуемым, экономически выгодным, а порой и единственно возможным средством, нейтрализующим техническое превосходство противостоящей стороны в информационной и технологической сферах. Основной прирост боевых потенциалов в ближайшей перспективе будет возможен за счет использования интеллектуальных систем управления войсками и оружием, а также применения

средств вооруженной борьбы, использующих нетрадиционные способы воздействия на противника. К таким средствам вооруженной борьбы, прежде всего, относится техника РЭБ, представляющая собой сложный объект, характеризуемый высокой наукоемкостью. Современные средства, комплексы и системы РЭБ на нынешнем этапе развития находятся в состоянии интенсивного совершенствования. В долгосрочной перспективе (2020-2025 гг.) объем задач, возлагаемый на средства РЭБ, не только не уменьшится, а увеличится за счет количественного увеличения объектов воздействий и увеличения способов воздействия по ним. Оснащение вооружения средствами и комплексами РЭБ способно многократно повысить их боевой потенциал и снизить возможные потери. При этом стоимость техники РЭБ составляет единицы процентов по отношению к стоимости основных видов вооружения [248].

4.8. Оружие массового поражения

4.8.1. Ядерное оружие

Официально ядерное оружие в достаточно больших количествах находится на вооружении пяти государств (США, Россия, Китай, Великобритания, Франция). Кроме того, оно имеется в Израиле, Индии, Пакистане и в Северной Корее [300].

Усилиями ученых убедительно показан разрушительный, губительный для человечества характер ядерной войны. Проведенными исследованиями определено, что предельно допустимым значением ядерного воздействия, т.е. «ядерным порогом», после которого могут начаться катастрофические изменения биосферы и климата на Земле, является энергия, выделяющаяся при взрыве ядерных боезарядов суммарной мощностью около 100 Мт. Несмотря на это, в сознании военных и политиков ядерных держав по-прежнему сохраняется представление о высокой значимости ядерного оружия в системе вооружения их ВС и планируется возможность его применения. В связи с этим ведущие ядерные державы продолжают работы по дальнейшему совершенствованию ядерного оружия [300].

К ядерному оружию третьего поколения специалисты относят средства, использующие энергию ядерного взрыва для генерации преимущественно какого-либо одного поражающего фактора. Иными словами, создаются боеприпасы, у которых выход неосновных поражающих факторов был бы незначителен и не оказывал существенного

влияния на окружающую среду, а также на технические и военные системы, не являющиеся объектами целенаправленного воздействия [95].

Появились образцы ядерно-нейтронного оружия, при взрыве боеголовки которого основное поражение живым организмам наносится потоком нейтронов [300].

Продолжается разработка оружия на основе гамма-излучения, в котором выделение энергии из ядер некоторых элементов происходит без деления или синтеза ядра. Так, например, взрыв на основе гафния, ядра которого могут существовать в высокоэнергетической форме или в виде ядерных изомеров, может быть очень мощным. Один грамм полностью заряженного изомера гафния может содержать больше энергии, чем 50 кг тринитротолуола, что позволяет изготовлять миниатюрные ракеты с боеголовками, заметно превышающими по мощности существующие обычные вооружения. В результате взрыва на основе ядерных изомеров происходит гамма-излучение, способное уничтожить любое живое существо, и выпадает сравнительно мало радиоактивных осадков в сравнении с взрывом на основе деления ядра [300].

Активно ведутся работы по созданию ядерно-кинетического оружия, ядерно-микроволнового оружия, рентгеновских лазеров с ядерной накачкой. Идет разработка ядерных боеприпасов с повышенным выходом электромагнитного импульса [300].

По данным зарубежной печати США в рассматриваемой перспективе сохранят в составе стратегических ядерных сил триаду, включающую МБР шахтного базирования, баллистические ракеты морского базирования, размещенные на атомных подводных лодках (БРПЛ на ПЛАРБ), крылатые ракеты воздушного базирования (КРВБ) с ядерной боевой частью (ЯБЧ), применяемые стратегической авиацией. [203]

Существуют планы замены к 2030 г. ядерных зарядов, размещенных на этих носителях, более совершенными образцами, создаваемыми без проведения испытаний. Основное внимание намечается уделить повышению таких характеристик боеприпасов, как надежность, способность противостоять старению и технологичность. В результате замены ожидается сокращение как общего количества ЯБЧ, так и числа боеголовок, устанавливаемых на одну МБР или БРПЛ. По некоторым сообщениям американской прессы уже к 2012 г. национальный ядерный арсенал по сравнению с настоящим временем может сократиться на 50%. Сегодня нельзя точно спрогнозировать, сколько

ядерных боезарядов и носителей в результате будут иметь вооруженные силы США к 2030 г., но подходы Вашингтона к ведению переговоров об ограничении стратегических наступательных потенциалов свидетельствуют о его стремлении удержать количественное превосходство по этому параметру над Россией и КНР [203].

На текущем этапе США отказались от планов применения в ядерном снаряжении такого тактического оружия, как торпеды, противолодочные и зенитные ракеты, артиллерийские снаряды, глубинные бомбы, управляемые фугасы, но сохраняют определенное количество ядерных БЧ крылатых ракет морского базирования и тактических ядерных авиационных бомб (по некоторым оценкам по нескольку сотен). С учетом технической совместимости таких ракет со стратегическими бомбардировщиками В-2, использующих технологии малой заметности, возросшего боевого радиуса собственно тактической авиации (более 1000 км с учетом дозаправки в воздухе), наличия специализированных хранилищ за пределами континентальной части США данный тип боеприпасов может быть использован против целей практически в любой точке Земли. Официальный Вашингтон почти не комментирует предназначение своего арсенала тактических авиабомб, но специалисты по проблемам разоружения считают, что таким образом США демонстрируют готовность перехода к ограниченному применению ядерного оружия против носителей угроз своим жизненно важным интересам. Кроме того, наличие американских ядерных складов в Европе призвано обеспечить солидарность в вопросах ядерного планирования в рамках НАТО [203].

В западной прессе неоднократно появлялась информация о якобы имеющихся у командования ВС США планах принятия на вооружение так называемых сверхмалых боеприпасов (мощность измеряется десятками тонн в тротиловом эквиваленте), предназначенных для ограниченного применения в ходе региональных войн, локальных конфликтов и антитеррористических операций. Считается, что они могли бы использоваться для поражения заглубленных объектов или создания мощного электромагнитного импульса, выводящего из строя радиоэлектронную аппаратуру противника на обширной территории. Особенностью «сверхмалых» боеприпасов должно стать сочетание собственно ядерной БЧ минимально достаточной мощности с высокоточными средствами доставки, что позволяет обеспечить необходимый поражающий эффект при снижении радиационного загрязнения местности. Однако многие зарубежные эксперты полагают, что реализация такого проекта сдерживается по политическим соображениям.

В рамках новой ядерной стратегии программами создания новых комплексов МБР (оснащенных в том числе неядерными боеголовками) и модернизации ракет Minuteman-3 предусматривается создание высокоточных систем, способных решать боевые задачи по поражению высокозащищенных заглубленных, малоразмерных и стратегических мобильных объектов и нанесению «молниеносных глобальных ударов», ранее возлагавшиеся только на МБР МХ. В силах наземного базирования реализуется программа модернизации ракетной системы Minuteman-3 в целях повышения оперативности ее перенацеливания и продления срока службы [95].

В современных условиях основные усилия США в области развития стратегического ракетного вооружения наземного базирования направлены на сохранение ракетных комплексов Minuteman-3 в боевом составе стратегических наступательных сил до 2030 г. При этом программа модернизации МБР включает не только смену головных частей, но и замену электронных блоков бортовой системы управления, зарядов твердотопливных ракетных двигателей первой и второй ступеней, установку нового двигателя третьей ступени, доработку жидкостного двигателя ступени разведения и др. По мнению специалистов, эти мероприятия проводятся в целях обеспечения высокой эффективности и требуемых эксплуатационных характеристик ракетных комплексов [95].

Наряду с реализацией программы по модернизации МБР Minuteman-3 в США проводятся исследования по разработке новой межконтинентальной баллистической ракеты. По сообщениям в открытой печати глава Командования глобальных ударов заявил, что его структура приступила к определению требований к перспективной МБР, которая придет на смену Minuteman-3 [95].

Таким образом, МБР по-прежнему могут эффективно использоваться при нанесении упреждающих и ответно-встречных ракетно-ядерных ударов.

4.8.2. Химическое оружие

Химическое оружие – оружие массового поражения, действие которого основано на токсичных свойствах химических веществ. Главными компонентами химического оружия являются боевые отравляющие вещества (ОВ) и средства их применения (химические боеприпасы: снаряды, ракеты, мины, авиационные бомбы, выливные авиационные приборы). Химическое оружие может быть использовано

для уничтожения, подавления и изнурения войск и населения, заражения местности (акватории), военной техники, материальных средств, продуктов питания, уничтожения животных, лесов, посевов [300].

Применение химического оружия было запрещено сначала Женевским протоколом 1925 г., который ратифицировали около 100 государств, затем «Конвенцией о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении» 1993 г. В 1993 г. Россия подписала, а в 1997 г. ратифицировала конвенцию о запрещении химического оружия. В связи с этим была принята программа уничтожения запасов химического оружия, накопленного за многие годы его производства. Согласно принятой в апреле 2012 г. программы химическое оружие в России, а также в США должно быть полностью уничтожено [300].

Но, несмотря на запрещение, по различным данным арсенал химического оружия постоянно совершенствуется по двум основным направлениям[300].

1. Разработка и совершенствование бинарного оружия – разновидности химических боеприпасов, снаряжаемых раздельно обычно двумя нетоксичными или малотоксичными компонентами, образующими боевое отравляющее вещество при их смешивании во время полета боеприпаса к цели или непосредственно перед его применением. Наличие бинарного оружия трудно проконтролировать, так как его составными частями, хранящимися порознь, являются нетоксичные вещества.
2. Развитие оружия нелетального действия. Среди возможных видов этого оружия специалисты на одно из первых мест ставят новые химические средства, приводящие к временному выводу личного состава из строя. В частности, перспективным является создание высокоэффективных психотропных препаратов с особыми свойствами и обратимостью воздействия – обездвижителей, нейроингибиторов и т.п.

Рассматривая более подробно разработку химических нелетальных средств поражения, следует отметить, что она ведется по двум направлениям [300].

1. Разработка и создание так называемых инкапаситантов – физиологически активных веществ с различным характером токсического действия, в том числе – дисрегуляторов и веществ калечащего действия.

2. Создание более совершенных раздражающих веществ (ирритантов).

К инкапаситантам относится большая группа физиологически активных веществ с различным характером токсического действия. В отличие от веществ смертельного действия токсины инкапаситантов выводят из строя людей при дозах ниже летальных. Поэтому при применении инкапаситантов, как правило, не бывает случаев смертельных поражений [300].

Ирританты – вещества, вызывающие раздражение глаз (лакрипаторы) и верхних дыхательных путей (стерниты). При прямом попадании ирритантов на слизистые оболочки их действие развивается за время, измеряемое секундами. Они вызывают обильное слезотечение, жжение в носоглотке, сильный кашель, чихание и загрудинные боли. При повышенных концентрациях ирританта в воздухе возможен ожог легких и носовое кровотечение, покраснение кожи с нетерпимой болью. Поражение средней тяжести за счет воздействия ирритантов, неопасное для жизни, вызывает потерю способности человека к активным действиям не более чем на шестьдесят минут [300].

Весьма важным является обстоятельство, состоящее в том, что на многие вещества, относящиеся к инкапаситантам, не распространяется запрет химической конвенции 1993 г. В частности, это касается следующих ирритантов: стернитов – отравляющих веществ, раздражающих верхние дыхательные пути; лакритаторов – слезоточивых отравляющих веществ; наркотических анальгетиков, обладающих способностью сковывать двигательные функции человека; эметиков – синтетических и природных веществ, обладающих сильным рвотным действием [300].

Ирританты по комплексу свойств могут представлять интерес в качестве веществ для изнурения живой силы противника и сковывания его действий. Эффект применения наркотических анальгетиков и эметиков в случае достижения внезапности может оказаться ошеломляющим. Действие анальгетиков является нокаутирующим, пораженные утрачивают способность держаться на ногах и тем более передвигаться. В тяжелых случаях люди впадают в бессознательное состояние. При поражении эметиками у пострадавших скоротечно начинается неукротимая рвота, сопровождаемая диареей. Из-за выделения рвотных масс пораженные эметиками вынуждены сбрасывать противогаз даже при нахождении в зараженной атмосфере [300].

Как отмечается в документах министерства обороны США, имеются данные о том, что специалистами уже разработаны основы

технологий для создания химического оружия нелетального действия. Разработаны вещества (порошок тетрафторэтилена), при обработке которыми участка дороги, взлетно-посадочной полосы или площадки поверхность становится скользкой, как лед, что значительно затрудняет движение транспорта и людей. Специалисты считают, что с помощью тетрафторэтилена можно эффективно заблокировать критически важные объекты и транспортные узлы противника [300].

4.8.3. Биологическое (бактериологическое) оружие

Биологическое оружие – это специальные боеприпасы и боевые приборы со средствами доставки, снаряженные биологическими средствами. Оно предназначено для поражения живой силы противника, животных, посевов сельскохозяйственных культур, а также порчи некоторых видов снаряжения и материалов [300].

Поражающее действие биологического оружия основано на использовании, в первую очередь, болезнетворных свойств патогенных микробов и токсичных продуктов их жизнедеятельности. Основу поражающего действия биологического оружия составляют биологические средства – специально отобранные для боевого применения биологические агенты. Для поражения людей используются агенты, отобранные в группу биологических средств, возбудители тяжелых инфекционных заболеваний человека. Для поражения сельскохозяйственных животных в качестве биологического оружия могут использоваться возбудители заболеваний, опасные в равной степени для животных и человека или поражающие только животных. Для поражения сельскохозяйственных культур возможно использование возбудителей бактериальных, вирусных и грибковых болезней культурных растений [300].

Несмотря на существование «Конвенции о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении» (1972 г.), которую ратифицировали 148 государств, в настоящее время имеются многочисленные факты, свидетельствующие о том, что в ряде стран продолжают расти ассигнования и осуществляться обширные программы военно-биологической направленности по совершенствованию имевшихся и созданию новых бактериальных (биологических) рецептур, способов и средств их боевого применения, осуществляется активное обучение личного состава вооруженных сил действиям в

условиях применения химического и бактериологического (биологического) оружия [300].

В настоящее время особое внимание в этой области уделяется разработке так называемого оружия нелетального (несмертельного) действия [300].

К биологическому оружию нелетального действия нового поколения зарубежные исследователи относят средства генной инженерии, на основе которых могут быть созданы принципиально новые возбудители инфекционных заболеваний и токсины, отвечающие требованиям, предъявляемым к оружию нелетального действия. В развитых странах основное внимание уделяется качественно новым разработкам с целью выведения бактерий и вирусов, поражающих людей, животных и растения с определенным генотипом [300].

По сообщениям зарубежных средств массовой информации в настоящее время ведутся исследования по созданию таких микроорганизмов и насекомых, которые смогут оказывать воздействие на элементы электронных и электротехнических устройств, разрушать изоляцию, материалы печатных плат, смазок и приводов механических устройств. В частности, в последнее время активизировались исследования в области конструирования микроорганизмов, временно лишающих противника работоспособности, уничтожающих запасы продовольствия и даже горюче-смазочных материалов. Предполагается, что по итогам таких исследований будут производиться специальные биотехногенные боеприпасы нелетального воздействия [300].

4.8.4. Генетическое оружие

Под генетическим оружием понимают вещества химического или биологического происхождения, которые могут вызывать в организме людей мутации (изменение структуры) генов, сопровождающиеся нарушением здоровья или запрограммированным поведением людей. В настоящее время данный вид оружия еще находится в стадии проработки, поэтому ряд экспертов относит его к биологическому оружию на новых принципах [300].

Специалисты в области безопасности считают, что генетическое оружие – это искусственно созданные штаммы бактерий и вирусов, измененные с помощью технологий генной инженерии таким образом, чтобы они могли вызывать негативные изменения в организме человека. Генетическое оружие действует в зависимости от пола, возраста и различных антропологических признаков, которые можно вы-

явить путем анализа структуры ДНК, хранящей генетический код (различия между отдельными людьми и популяциями связаны с неравномерным распределением белков в их отличительных генах). Генетически обусловлены (закодированы в ДНК) внешний вид человека, манера поведения, длительность жизни и множество других характеристик. Генная инженерия позволяет также создавать копии ДНК – на этом принципе строятся все эксперименты по клонированию, вызывающие наибольшие споры и неприятие со стороны общественности и церкви [300].

В последние годы в области биотехнологии уже удалось разработать методики получения обширного спектра физиологически активных белков, влияющих на болевую чувствительность и психосоматические реакции млекопитающих. Исследования таких биорегуляторов находятся на различных стадиях, вплоть до клинических испытаний на человеке [300].

Особым видом генного оружия является так называемое этническое оружие – оружие с избирательным генетическим фактором. Оно рассчитано на поражение, прежде всего, определенных этнических и расовых групп населения. Возможность разработки и последующего применения такого оружия исходит из генетических различий разных рас и этнических групп людей. Объектами воздействия этнического оружия могут стать также животные, растения, микрофлора почвы, специфичные для данного района Земли и составляющие важное условие существования человека в этом районе [300].

В организмах определенных групп людей присутствуют генетически обусловленные биохимические особенности, зависящие от факторов внешней среды и, прежде всего, пищи и инфекционных агентов. Под влиянием таких региональных факторов внешней среды складывались различные биологические структуры, которые закреплялись наследственно и передавались последующим поколениям людей. Такие внутривидовые отличия могут быть непосредственным объектом целенаправленного химического или биологического воздействия этнического оружия на клетки, ткани, органы, системы людей. Это может явиться одним из средств геноцида и оружием стерилизации (лишения способности к деторождению) [300].

Ученые предполагают, что к 2020 г. генная инженерия достигнет еще более значительных результатов, что позволит в том числе обеспечить производство токсичных продуктов, которые можно будет применять в качестве оружия. Это может создать принципиально новую стратегическую ситуацию, когда главной целью «генетической

войны» со стороны некоторых стран становится не разгром вооруженных сил противника, а уничтожение значительной части его населения, которое объявляется «избыточным» на фоне убывающего плодородия Земли [300].

4.9. Оружие на новых физических и других принципах

В настоящее время к оружию на новых физических и других принципах относятся [300]:

- лазерное;
- ускорительное (пучковое);
- акустическое (инфразвуковое);
- электромагнитное;
- радиочастотное и СВЧ;
- геофизическое;
- генное (генетическое).

Данные виды оружия имеют, как правило, различную степень проработанности и реализации, а также принципы поражения противника, однако их всех объединяет высокая степень перспективности при использовании в вооруженных конфликтах. Кроме того, любой из этих видов оружия может стать основой новой революции в военном деле, связанной с принципиальным изменением принципов ведения войны.

4.9.1. Лазерное оружие

Лазерное оружие – вид оружия направленной энергии, основанный на использовании электромагнитного излучения высокоэнергетических лазеров (средняя выходная мощность лазера более 20 кВт) [300].

Поражающее действие лазерного оружия определяется в основном термомеханическим и ударно-импульсным воздействием лазерного луча на цель и достигается за счет нагревания до высоких температур материалов объекта. Это вызывает расплавление или даже испарение материалов, повреждение чувствительных элементов вооружения, ослепление органов зрения человека вплоть до необратимых последствий и нанесение ему тяжелых поражений в виде термических ожогов кожи. Для противника действие лазерного излучения отличается внезапностью, скрытностью, отсутствием внешних при-

знаков в виде огня, дыма, звука, высокой точностью, прямолинейностью распространения и практически мгновенным действием [300].

Среди преимуществ лазерного оружия специалисты отмечают огромную концентрацию энергии на единице площади, практически мгновенное поражение объекта на недостижимых для других видов оружия дальностях, высокую избирательность поражения [95].

Из всего многообразия лазеров наиболее приемлемыми для лазерного оружия считаются твердотельные, химические со свободными электронами, рентгеновские лазеры с ядерной накачкой и др. Лазерные боевые комплексы могут быть наземного, морского, воздушного и космического базирования с различной мощностью, дальностью действия, скорострельностью и боезапасом [300].

Объектами поражения таких комплексов могут быть живая сила противника, его оптические системы, летательные аппараты и ракеты различных типов [300].

В США активно ведутся работы по совершенствованию комплексов лазерного оружия стратегического назначения. Они же ближе всего к постановке на вооружение систем, способных поражать цели при помощи лазерного луча. Идея использования лазерного оружия для перехвата ракет рассматривалась еще в рамках широко известной программы «Звездных войн». Один из самых известных достижений в этой области – это химический лазер системы ПРО Nautilus, также известный как THEL (Tactical High-Energy Laser), предназначенный для перехвата ракет.

В США с 1996 г. дочерней фирмой «Boeing» – Boeing Defense and Space Group велись разработки лазерного оружия авиационного базирования с целью создания воздушного лазера ПРО, способного поражать баллистические ракеты на дальности 400-460 км. В результате проекта был разработан химический лазер COIL (Chemical Oxygen Iodine Laser), генерирующий волну 1,3 мкм, на основе переохлажденного жидкого кислорода и металлического йода. Лазер этого типа способен вырабатывать очень узкий, хорошо сфокусированный луч мощностью 1 МВт с низким затуханием в атмосфере. В качестве носителя лазера ПРО выбрали самый большой на то время транспортный самолет Боинг-747-400F со стартовой массой 340 т, из которых 72 т могли быть заняты лазерным оборудованием. В фюзеляж удалось втиснуть только 6 химических модулей COIL общей мощностью 6 МВт вместо запланированных 14. Это сразу снизило проектную дальность действия лазера до 250 км. Запаса жидкого переохлажденного кислорода и мелкодисперсного порошкообразного йода на борту

хватало для осуществления 20-40 лазерных «выстрелов». В 2005 г. лазерную ПРО должны были испытать в полете, после чего Пентагон собирался заказать 7 таких машин. Однако вскоре обнаружились два непреодолимых технологических препятствия. Во-первых, на каждый 1 Вт электроэнергии вырабатывается 4 Вт тепловой энергии, которую всю невозможно отвести. Она идет на нагрев самого оборудования и самолета-носителя. При мощности в 6 МВт перегрев самолета приобретает катастрофические размеры. Тем более что на борту находятся еще и емкости с жидким кислородом. Второй барьер – плавление линз с расфокусировкой луча лазера. Температура излучения такова, что кварцевое стекло не выдерживает. В результате в июне 2009 г. Пентагон прекратил финансирование проекта Airbome Laser, сокращенно ABL, в связи с его бесперспективностью [316].

В дальнейшем компании Boeing, Northrop Grumman и Lockheed Martin продолжили доработку проекта в инициативном порядке. Для целей ПРО на борту самолета Boeing B-747-400F установили 3 лазера: лазер TILL (Track IllumiHATOr Laser), который предназначен для обнаружения и сопровождения (подсветки) цели, а также корректировки параметров оптической системы, с помощью которого будет осуществляться поражение цели; второй – лазер BILL (Beacon IllumiHATOr), используемый для компенсации атмосферных искажений, и третий – шестимодульный боевой лазер [300].

В феврале 2010 г. были проведены испытания боевого лазера воздушного базирования, в ходе которого, как было заявлено, были сбиты две баллистические мишени – имитаторы жидкостной и твердотопливной ракет средней дальности. В дальнейшем во время летных испытаний 20 октября 2010 г. планировалось сбить в полете баллистическую ракету на разгонном участке, однако аппаратура сопровождения цели не смогла дать ее координаты. При этом обнаружение ракеты по факелу двигателя прошло успешно. Предыдущее испытание также закончилось неудачей. Так, 1 сентября 2010 г. во время полета лазер должен был поразить баллистическую ракету на расстоянии 100 миль, но программный сбой привел к расфокусировке луча и его смещению с центра мишени. В результате ракету уничтожить не удалось [316].

Таким образом, результаты испытания мощного лазерного оружия весьма неоднозначны, а при его создании и эксплуатации возникают сложности, непреодолимые при современном технологическом уровне. Таким образом, в ближайшие 20-30 лет мощные боевые лазеры, способные сбивать ракеты, не будут созданы, при этом основ-

ные усилия по созданию лазерного оружия были сосредоточены на создании лазерного оружия киловаттной мощности.

Разработкой лазерного оружия для ВМС США занимается компания Northrop Grumman Corporation. Эта компания сумела создать самый мощный и надежный боевой твердотельный лазер. В 2009 г. ее инженерам удалось первыми в мире достичь на лазере подобной конструкции мощности луча в 105,5 кВт. Работы ведутся в рамках военной программы JHPSSL (Joint High Power Solid-State Laser – «Модульный высокомощный твердотельный лазер»). В 2010 г. удалось добиться непрерывной работы твердотельного лазера на этой мощности в течение 6 ч. Это произошло во время тестовых испытаний в процессе интеграции системы наведения и слежения перед полевыми испытаниями. По габаритам установка-демонстратор JHPSSL сопоставима с автобусом и состоит из 7 лазерных усилителей мощностью каждого порядка 15 кВт, что в сумме дает 105,5 кВт. В одном из пресс-релизов Northrop Grumman за 2009 г. сообщалось, что было проведено успешное испытание системы из 8 лазерных усилителей общей мощностью 120 кВт [316].

6 апреля 2011 г. прошли испытания «Морского лазера-демонстратора» MLD (Maritime Laser Demonstrator), созданного Northrop Grumman Corporation. В испытаниях участвовал твердотельный лазер, разрабатываемый в рамках военной программы JHPSSL и состоящий из нескольких модулей мощностью по 15 кВт, который был установлен на борту выведенного из боевого состава эсминца типа Spruance Paul Foster. В пресс-релизе по итогам тестирования сообщалось, что впервые боевая лазерная система для корабля была интегрирована с его радиолокационной системой обнаружения и его навигационной системой, а также впервые лазерное оружие производило «выстрелы» в море с движущейся платформы. Ранее аналогичные системы проходили тестирование только на наземных полигонах. Было проведено 35 «стрельб» в открытом море лучом высокой мощности. Лазер MLD показал, что способен отслеживать и повреждать малое судно, перемещающееся на «репрезентативных» скорости и дальности. В ходе испытаний с помощью лазерного луча удалось поджечь подвесной двигатель и взорвать небольшую надувную лодку. По мнению конструкторов, прототип в ходе испытаний показал, что способен преодолевать сложные условия моря – волнение, влажность воздуха и т.д. [316].

В ВМС США отдают предпочтение лазерам на свободных электронах (Free Electron Laser, FEL). Считается, что они лишены не-

достатков химического лазера – в первую очередь, не выделяют так много тепла, поскольку энергетический луч получают за счет колебаний электронов в магнитном поле. Этот принцип позволяет варьировать частоту и мощность лазера в широком диапазоне. По мнению американских экспертов, этот тип лазера идеально подходит для корабельных систем ПВО и ПРО по следующим причинам. Во-первых, на кораблях стоят мощные энергетические установки, зачастую избыточной мощности. Во-вторых, над морем воздух чище, чем над сушей, а в условиях повышенной влажности, осадков и облачности луч лазера на свободных электронах можно быстро корректировать для преодоления помех [316].

На портале YouTube было выложено официальное видео испытаний созданного исследовательской лабораторией Командования морских систем ВМС лазера LaWS (Laser Weapon System), проходивших 30 июля 2012 г. в Сан-Диего на борту USS Dewey (DDG-105) [132]. В апреле 2013 г. ВМС США заявили о планах оснащения в 2014 г. боевых кораблей лазерами, способными поражать беспилотные летательные аппараты и мелкие суда [133]. В конце 2014 г. первая боевая лазерная установка была развернута на корабле ВМС США в Персидском заливе [134].

В настоящее время исследования по разработке лазеров на свободных электронах в интересах ВМС США продолжаются, при этом высказываются прогнозы о возможности создания мегаваттного лазера к 2018-2020 г. [316].

Изменение акцента разработчиков с мегаваттной мощности в сторону киловаттной скорректировало применение лазерных средств в сторону их использования для поражения БПЛА в составе систем ПВО, а также в сторону создания гибридных систем ПВО-ПРО.

Американская корпорация Boeing в 2009 г. объявила об успешном проведении опыта по применению боевого лазера против малогабаритного БПЛА. Лазер был установлен на платформе бронемашины Avenger (модифицированной HMMWV), которая обычно используется армией и морской пехотой США для выполнения задач ПВО. Laser Avenger способен применять против БПЛА свое вооружение, не раскрывая при этом позиции войск, т.е. можно уничтожать БПЛА противника, не подвергая при этом опасности другие подразделения, находящиеся вблизи бронемашины [300].

В 2012 г. компания Lockheed Martin официально представила прототип компактной наземной системы лазерной ПВО-ПРО ADAM (Area Defense Anti-Munitions) [135]. Система испытывалась в 2012 и

2013 г. для борьбы с небольшими БПЛА и ракетами на расстоянии в 1,5-2 км и в 2014 г. – против моторных лодок [136].

Корпорация Boeing в кооперации с британским подразделением европейского консорциума BAE System создало гибрид лазера и малокалиберной автоматической пушки Mk-38. Автоматом Mk-38 на турели вооружаются десантные и вспомогательные суда ВМС США. Эффективный огонь может вестись на дальность 2,5 км. Исполнители в июле 2011 г. объявили о создании прототипа тактической лазерной системы TLS (Tactical Laser System) для поражения БПЛА и малых судов [316].

Годом раньше подобную систему ПВО-ПРО на авиакосмическом салоне Farnborough-2010 в Великобритании показала американская компания Raytheon. Шесть волоконных лазеров LaWS (Laser Weapon System) общей мощностью 50 кВт были объединены с корабельной 20-мм шестиствольной автоматической артиллерийской установкой Mark 15 Phalanx CIWS (Close-In Weapon System – «орудийная система ближнего боя»). Подразумевается, что комбинированная установка сможет поражать цель 6 лазерами, чьи лучи сведены в одну точку. В первую очередь она предназначена для борьбы с противокорабельными ракетами. Если же это не удастся, то на более близком расстоянии в дело вступит шестиствольная пушка, выпускающая 4500 снарядов в минуту (дальность эффективной стрельбы Mark 15 Phalanx – 1,5 км). На испытаниях в мае 2010 г. система обнаружила, захватила, взяла на сопровождение и поразила четыре БПЛА, летевших на разных высотах и дальностях. Представители Raytheon дали понять, что условия испытаний были близки к реальным боевым. При этом в британских СМИ появилось неподтвержденное сообщение, что один из БПЛА был поражен на дальности 3,2 км при скорости 480 км/ч [316].

В декабре 2013 г. в США прошли испытания боевого мобильного лазера HEL MD (High Energy Laser Mobile Demonstrator) мощностью 10 кВт для подразделений тактического звена. Во время испытаний установка уничтожила более 90 минометных снарядов и несколько БПЛА. Разработку программы HEL MD ведет корпорация Boeing. В 2014 г. были проведены успешные его испытания в сложных погодных условиях. Идут работы по установке с мощностью лазера 50 кВт, а в дальнейшем – 100 КВт. Это позволит уничтожать цели с более высокой скоростью движения [117, 317].

Американское военное агентство DARPA испытало в начале 2014 г. установку Excalibur. Она включает в себя 28 волоконных лазеров, объединенных в систему, которая способна фокусировать луч на

расстоянии, превышающем 7 км. Каждый элемент обладает излучающей мощностью в 10 Вт. Лазеры объединены в блоки по 7 шт., при этом диаметр такого блока составляет 10 см, а их общее количество и мощность можно наращивать простым соединением. Эксперименты DARPA показали эффективность масштабируемого лазера с набором излучателей. Excalibur использует особый алгоритм оптимизации лазерного излучения и в течение считанных миллисекунд корректирует параметры лазерного луча, компенсируя турбулентность атмосферы. В течение трех лет планируется довести мощность до 100 кВт. Данной мощности достаточно для уничтожения ракет, снарядов, БПЛА и поражения живой силы. Кроме того, такую систему можно будет совместить с существующими платформами: вертолетами, самолетами, кораблями и бронетехникой. Разработчики ожидают, что волоконно-оптический лазер будет в 10 раз легче и компактнее текущих опытных твердотельных лазерных систем [142].

Отдельные лазерные системы планируется применять на самолетах, вертолетах, БПЛА и бронетехнике в составе системы обороны от ракет.

Так, компания General Atomics проводила лабораторные испытания «лазерной системы третьего поколения», которая будет способна выполнить десять импульсов мощностью по 150 кВт между перезаряжанием, которое займет всего 3 мин. Компания проектирует контейнер массой 1360 кг, в котором разместится лазерная установка и который будет встроен в отсек вооружения БПЛА Avenger. При условии финансирования Министерства обороны США этот контейнер может быть готов к испытаниям на борту воздушного судна к 2018 г. [118].

Под руководством управления DARPA Министерства обороны США разрабатывается лазерная система перехвата и уничтожения в полете снарядов противника. Проект HELLADS (High-Energy Liquid Laser Area Defense System) разрабатывает компания General Atomics Aeronautical Systems, получившая в январе 2011 г. контракт на 40 млн долл. В основе лежит лазер с жидкой активной средой. Циркуляция жидкости позволяет отводить больше тепла, в результате можно увеличить мощность луча. На сегодняшний день лазер HELLADS достигает мощности 150 кВт. Установка создается для защиты самолетов от ракет ПЗРК и класса «воздух–воздух», поэтому к ней предъявляются жесткие требования по габаритам: вес – не более 750 кг, объем – не более 2 кв. м. Изначально предполагалось, что HELLADS будет монтироваться в комплекс вооружения стратегического бомбардировщика

B-1B. Пока неизвестно, когда начнутся авиационные испытания, но уже сейчас есть основания полагать, что эту систему гораздо раньше попытаются применить для защиты от реактивных, артиллерийских и минометных снарядов [316].

Ведутся работы по созданию лазерного оружия космического базирования, рассматриваемого военным ведомством США в качестве неотъемлемой части перспективных систем противоракетной обороны и противоспутниковой борьбы [300].

Проекты по созданию лазерного оружия ведутся не только в США, но также и в других технологически развитых странах.

Французская кораблестроительная компания DCNS реализует программу Advansea, в ходе которой планируется создать к 2025 г. полностью электрифицированный боевой надводный корабль с лазерным и электромагнитным вооружением [221].

В ноябре 2011 г. в Швейцарии немецкая компания Rheinmetall продемонстрировала перехват беспилотного самолета размещенной на бронетранспортере лазерной системой, разработанной ее подразделением Rheinmetall Defence [143].

В рамках отдельных программ идет совершенствование лазерного оружия тактического назначения, которое позволяет выводить из строя оптико-электронные приборы и поражать незащищенные органы зрения выбранных, особо важных целей среди личного состава противника (командиры, наводчики, снайперы и т.п.) [300].

В таких военных целях могут быть использованы «зеленые» лазеры серии Spyder, к продаже которых приступил Китай. Это самые мощные лазеры данного спектрального диапазона, производимые сегодня серийно, предлагаются 3 модели мощностью 200, 250 и 300 мВт. Лазер Spyder 300 мВт имеет пиковую мощность 450 мВт, заявленный радиус действия около 200 км, работает от источника питания напряжением 3 В, потребляемый ток не превышает 1,2 А, длина волны излучения – 532 нм (зеленый свет). Лазер выполнен в цилиндрическом корпусе диаметром 20 мм и длиной 198 мм, продолжительность работы диода – не менее 80 тыс. часов, продолжительность непрерывной работы от одного комплекта батарей – 2 ч. По заверениям производителей и первых пользователей, мощности лазера достаточно, чтобы прожечь лист бумаги, прожечь воздушный шар с большого расстояния, зажечь сигарету или спичку [300].

Для создания эффективных систем лазерного оружия оптимальным вариантом является использование лазеров, генерирующих излучение в тех областях электромагнитного спектра, в которых рабо-

тают разведывательные оптико-электронные приборы и головки самонаведения управляемых ракет, а глаз человека обладает максимальной спектральной чувствительностью. Поражение органов зрения рассматривается специалистами как наиболее перспективное направление вывода личного состава из строя при ведении боевых действий. Это объясняется, прежде всего, тем, что человек является конечным и главным звеном в системе «машина – человек» [300].

Ведутся разработки лазерного оружия, устанавливаемого как на наземных, так и на воздушных носителях (вертолетах). При этом источник ослепляющей вспышки можно разместить, например, в артиллерийских боеприпасах (на основе взрывного нагревания инертных газов). Смонтированные на бронемашинах пехоты лазерные «пушки» могут ослеплять прицелы противника и его личный состав [300].

4.9.2. Ускорительное (пучковое) оружие

Ускорительное (пучковое) оружие – это оружие, в котором передача энергии поражающим элементам обеспечивается ускорителем того или иного типа. Ускоритель разгоняет пучок элементарных частиц или плазмы, впоследствии выстреливаемых по цели. Это оружие может быть использовано как в атмосфере, так и вне ее, то есть в космическом пространстве [300].

Поражающим фактором пучкового оружия является остронаправленный пучок заряженных или нейтральных частиц высокой энергии – электронов, протонов и нейтральных атомов водорода. Мощный поток энергии, переносимый частицами, может создать в материале цели интенсивное тепловое воздействие, ударные механические нагрузки, способен разрушать молекулярную структуру организма человека и инициировать рентгеновское излучение [300].

Основным элементом такого оружия должны стать ускорители нейтральных и заряженных частиц. Устройства ускорителей электронов и атомов водорода и возможные области их применения в оружии существенно отличаются [14].

Электронный пучок может распространяться только в специально созданном в атмосфере канале сильно разреженного и ионизированного воздуха, который его ослабляет, нейтрализуя при этом объемный заряд, который приводит к рассыпанию пучка. Магнитное поле Земли сильно искривляет траекторию электронного пучка в вакууме, что исключает возможность создания ускорительного оружия большой дальности и, прежде всего, космического. Прямолинейно распро-

страняться может только пучок нейтральных атомов водорода, причем в ускорителе разгоняются отрицательные ионы, которые на выходе нейтрализуются в специальной газовой ячейке. Однако даже небольшие остатки атмосферы (на высотах до 200 км) легко ионизуют нейтральные атомы, а образующиеся при этом протоны сильно отклоняются магнитным полем Земли [14].

Воздействие на цель ускорительного оружия носит как поверхностный, так и объемный характер в силу большой глубины проникновения частиц, причем основные планы создания ускорительного оружия связывались, в первую очередь, именно с его уникальными свойствами.

Объемный характер воздействия на цель, обусловленный большой глубиной проникновения ускоренных до околосветовых скоростей частиц, приводит к наблюдаемым внешним вторичным эффектам, пропорциональным массе цели, что позволяет выделить боевой блок в составе сложной баллистической цели. Именно эта задача и ставилась американцами в программе создания космического ускорительного оружия для национальной системы ПРО [14].

Другим механизмом воздействия пучка частиц является радиационное повреждение полупроводниковых элементов электроники, наступающее, как правило, при уровнях воздействия, существенно меньших, чем необходимо для иных механизмов поражения цели. Такой механизм рассматривается для поражения космических аппаратов и электроники ракет, а также боевых блоков в космосе [14].

Третий механизм воздействия основан на радиационных эффектах и обусловлен разложением под действием частиц химических соединений с образованием активных радикалов или свободных электронов, что инициирует в веществе химические реакции. При воздействии на взрывчатое вещество или твердое топливо начинается процесс горения. Этот механизм, по-видимому, предполагался при разработке концепции ускорительного оружия для систем ПВО-ПРО кораблей, а также в рассматриваемой сейчас в США системе ускорительного оружия для разминирования [14].

Применение пучкового оружия отличается мгновенностью и внезапностью поражающего действия. Ограничивающим фактором по дальности действия этого оружия являются частицы газов, находящиеся в атмосфере, с атомами которых взаимодействуют разогнанные частицы, постепенно теряя свою энергию. Наиболее вероятными объектами поражения пучкового оружия может быть живая сила, элек-

тронное оборудование, а также различные системы вооружения и военной техники [300].

Работы по ускорительному оружию на пучках заряженных частиц (электронов) ведутся в интересах создания комплексов ПВО кораблей, а также для мобильных тактических сухопутных установок. Установки имеют большие массогабаритные характеристики и поэтому могут создаваться либо как стационарные, либо на специальной подвижной технике большой грузоподъемности [300].

Таким образом, для создания реально действующего ускорительного оружия необходимо наличие очень мощных источников энергии.

Пока космическое ускорительное оружие с традиционными источниками питания находится на стадии разработки концепции, возможное принятие его на вооружение относят к периоду не ранее 2018 г. Оно может найти применение для нарушения устойчивости орбитальной космической группировки, поражения одиночных баллистических ракет на заатмосферном участке без срабатывания аппаратуры ядерного подрыва и уничтожения других средств воздушно-космического нападения и разведки [300].

4.9.3. Акустическое (инфразвуковое) оружие

Акустическое (инфразвуковое) оружие основано на использовании направленного излучения инфразвуковых колебаний с частотой несколько герц, которые могут оказать сильное воздействие на человеческий организм. Способность инфразвуковых колебаний проникать через бетонные и металлические преграды повышает интерес военных специалистов к этому оружию. Дальность его действия определяется излучаемой мощностью, значением несущей частоты, шириной диаграммы направленности и условиями распространения акустических колебаний в реальной среде [300].

При рассмотрении поражающего действия акустического оружия следует учитывать, что оно охватывает три характерных диапазона частот [300]:

- инфразвуковую область – ниже 20 Гц;
- слышимую область – от 20 Гц до 20 кГц;
- ультразвуковую область – свыше 20 кГц.

Такая градация определяется особенностями воздействия звука на организм человека. Установлено, что пороги слышимости, уровни

боли и другие негативные воздействия на организм человека увеличиваются с уменьшением частоты звука.

Инфразвуковые колебания способны вызвать у людей состояние тревоги и даже ужаса. По утверждению некоторых ученых, при значительной мощности излучения в результате резкого нарушения функций отдельных органов человека и поражения его сердечно-сосудистой системы может наступить летальный исход. Согласно результатам проводившихся исследований инфразвуковые колебания могут воздействовать на центральную нервную систему и пищеварительные органы, вызывая паралич, рвоту и спазмы, приводить к общему недомоганию и болевым ощущениям во внутренних органах, а при более высоких уровнях на частотах в единицы герц – к головокружению, тошноте, потере сознания, а иногда к слепоте и даже смерти. Инфразвуковое оружие может также вызывать у людей паническое состояние, потерю контроля над собой и непреодолимое желание укрыться от источника поражения. Определенные частоты могут воздействовать на среднее ухо, вызывая вибрации, которые, в свою очередь, становятся причиной ощущений, сродни тем, какие бывают при укачивании и морской болезни. Подбором определенной частоты излучения можно, например, спровоцировать массовые инфаркты миокарда у личного состава войск и населения противника [300].

В США разработано несколько типов инфразвукового оружия, которое было испытано в ноябре 1999 г. Два из них предназначены для вооружения одиночного бойца, другие монтируются на стандартных армейских транспортерах. Все типы этих боевых генераторов вырабатывают инфразвук мощностью от 120 до 130 дБ. В настоящее время в США, Германии и Великобритании разрабатывается ряд принципиально новых акустических источников нелетального воздействия, таких, например, как генераторы вихревых структур (Vortex-технологии). Появились сообщения о разработке новых видов акустического оружия на основе фазированных акустических колебаний или мощных источников непрерывных акустических колебаний. По имеющимся оценкам такие средства могут поражать людей на сравнительно больших расстояниях (до 1-2 км) [300].

По сообщениям печати в США продолжаются работы по совершенствованию инфразвукового оружия. Преобразование электрической энергии в звуковую низкой частоты происходит при помощи пьезоэлектрических кристаллов, форма которых изменяется под воздействием электрического тока [300].

Опытные образцы инфразвукового оружия уже применялись ранее в вооруженном конфликте в Югославии, когда так называемая «акустическая бомба» производила звуковые колебания очень низкой частоты [300].

В США также ведутся исследования по созданию инфразвуковых систем на основе использования больших громкоговорителей и мощных усилителей звука. В Великобритании разработаны излучатели инфразвука, не только оказывающие воздействие на слуховой аппарат человека, но и вызывающие резонанс внутренних органов, нарушающий работу сердца, вплоть до смертельного исхода. Для поражения людей, находящихся в бункерах, убежищах и боевых машинах, испытываются акустические «пули» очень низких частот, образующиеся при наложении ультразвуковых колебаний, излучаемых большими антеннами [300].

4.9.4. Электромагнитные пушки (рельсотроны)

Электромагнитные пушки – оружие, в котором для придания начальной скорости снаряду используется магнитное поле либо энергия электромагнитного излучения используется непосредственно для поражения цели. В этом случае магнитное поле применяются как альтернатива взрывчатым веществам в огнестрельном оружии [300].

Одним из видов электромагнитного оружия является рельсовая пушка (англ. Railgun) – форма оружия, основанная на превращении электрической энергии в кинетическую энергию снаряда. Другие названия: рельсовый ускоритель масс, рельсотрон, «Рейлган» (Railgun) [300].

Западные специалисты в своих планах переоснащения вооруженных сил немаловажное значение среди исследуемых систем оружия на новых физических принципах придают созданию средств вооруженной борьбы на базе электродинамических ускорителей массы или электромагнитных орудий (пушек), основной привлекательной особенностью которых является достижение гиперзвуковых скоростей поражения [300].

Считается, что главным преимуществом электромагнитных орудий по сравнению с традиционными артустановками станет увеличенная до 64 МДж дульная энергия (для сравнения: дульная энергия корабельных артустановок: Мк45 мод. – 4-18 МДж, AGS – 33 МДж) и, как следствие, высокая начальная скорость полета снаряда. Например, при стрельбе на максимальную дальность около 500 км для снаряда

массой 20 кг расчетная начальная скорость полета оценивается в 2,5 км/с, а скорость встречи с целью – не менее чем в 1,5 км/с [14].

По замыслу американских разработчиков, сравнительно низкий уровень энергетических потерь снарядов при стрельбе на большие дальности достигается прохождением значительной части их баллистической траектории вне плотных слоев атмосферы с максимальной высотой полета до 160 км. Высокие начальные скорости снарядов электромагнитных орудий позволят добиться существенных боевых преимуществ над современными образцами артиллерийского вооружения, важнейшими из которых являются [14]:

- малое подлетное время до цели, значительно снижающее время устаревания данных целеуказания и не позволяющее противнику принять меры эффективного противодействия;
- высокая поражающая способность бронебойных подкалиберных снарядов благодаря их значительной кинетической энергии;
- расширенные возможности уничтожения критичных по времени мобильных целей, а также высокозащищенных стационарных объектов.

Кроме того, ожидается, что отказ от применения взрывчатых веществ обеспечит при стрельбе тысячекратное снижение показателей заметности ЭМО в видимом и инфракрасном диапазонах длин волн и десятикратное – в акустическом, а также позволит снизить на 30% силу отдачи и повысить взрывопожаробезопасность боевых кораблей и бронированных машин [14].

Основной и наиболее трудной технологической задачей при создании электромагнитных орудий в интересах вооруженных сил является разработка компактного мощного и энергоемкого электрооборудования [14].

В 2005 г. ВМС США запустили программу по разработке электромагнитных рельсовых орудий под названием Velocitas Eradico. В программе участвуют корпорации General Atomics и BAE Systems.

Компания General Atomics разработала орудие, способное доставлять снаряд весом в 10 кг на расстояние более 200 км со средней скоростью около 2 000 м/с. По мнению экспертов, такое орудие имеет настильную траекторию на расстоянии до 30 км.

В феврале 2008 г. ВМС США продемонстрировали рельсотрон с энергией 10 МДж, снаряд которого развил дульную скорость 2520 м/с (9000 км/ч) [300]. В декабре 2010 г. в Центре разработки надводного вооружения ВМС США было проведено успешное испы-

тание рельсотрона с дульной энергией 33 МДж. Масса используемых в тестах снарядов варьировалась от 2 до 3,2 кг. В феврале 2012 г. близкий к серийному образцу прототип промышленного рельсотрона от BAE Systems был испытан на 32 МДж [226]. Серийный образец этой системы должен иметь дальность стрельбы до 180 км, а в перспективе – до 400 км. В настоящее время инженеры разрабатывают системы автоматической подачи снарядов, охлаждения и питания установки.

ВМС США планирует установку рельсотронов на свои боевые корабли к 2020 г. Ожидается, что такое оружие будет способно поражать цель на расстоянии 400 км с точностью до 5 м при начальной скорости полета 5800 м/с [300].

В перспективных разработках со сроком завершения разработок в 2020 г фигурирует уже установка мощностью в 64 МДж, что примерно в 7 раз выше, чем у нынешних опытных образцов. Эти орудия должны поступить на вооружение строящихся в США эсминцев серии DDG1000 Zumwalt, чья модульная конструкция и электрическая трансмиссия рассчитывались с прицелом на перспективные рельсотроны [300].

4.9.5. Радиочастотное и сверхвысокочастотное оружие

Радиочастотным оружием называют средства, поражающее действие которых основано на использовании электромагнитных излучений на человеческий организм сверхвысокой (СВЧ) или чрезвычайно низкой частоты (ЧНЧ). Диапазон сверхвысоких частот находится в пределах от 300 МГц до 30 ГГц. К чрезвычайно низким относятся частоты менее 100 Гц [300].

Объектом поражения радиочастотным оружием является человек, при этом используется известная способность радиоизлучений сверхвысокой и чрезвычайно низкой частоты вызывать повреждения (нарушение функций) жизненно важных органов и систем человека, таких как мозг, сердце, центральная нервная система, эндокринная система и система кровообращения. При этом отмечаются два вида воздействия: тепловое и нетепловое [300].

Тепловое – вызывает перегрев тканей и органов и при достаточно длительном излучении приводит к патологическим изменениям [300].

Нетепловое – в основном приводит к функциональным нарушениям в различных органах человеческого организма, особенно в

сердечно-сосудистой и нервной системах. На использовании электромагнитного излучения основана работа СВЧ-устройств [300].

Не так давно в США был испытан один из СВЧ-приборов, получивший название «Бесшумный страж». По заявлению американских военных, дальность действия нового оружия достигает 500 м. Излучаемый антенной пучок волн создает на теле противника тепловое пятно температурой до 50° С, вызывающее сильный болевой эффект, хотя отмечено, что такие волны могут проникать в кожу лишь на глубину 0,04 мм и не могут вызвать настоящего ожога. Волны не проникают сквозь стену или стекло, но обычная одежда не представляет для них препятствия. Наблюдавшие за ходом испытаний эксперты отметили, что никто из тех, кто подвергся действию излучения, не смог оставаться на месте более 5 с, а шоковое состояние наступало уже через 3 с [300].

Отмечается, что если воздействовать на биотоки организма человека, которые имеют частоту от 1 до 35 Гц, СВЧ-излучением, то у человека возникают: нарушение восприятия реальности; подъем или снижение тонуса; возбуждение или впадение в апатию; усталость, сильное переутомление; тошнота и головная боль; возможные полная стерилизация инстинктивной сферы, а также повреждения сердца, начиная от аритмии до полной его остановки; поражение мозга и центральной нервной системы. Кроме того, человек начинает слышать несуществующие шумы и свист, наблюдаются резь в глазах, боль в ушах (как при перепадах атмосферного давления), онемение рук, гул в голове, подергивание ног и жжение в подошвах. Это оружие может поражать и внутренние органы человека, причем с вероятностью летального исхода [300].

С помощью СВЧ-генератора на определенных частотах можно также воздействовать на психику человека, нарушать восприятие окружающей действительности, подавлять одновременно сознание людей и внушать им определенное поведение [300].

Первый боевой СВЧ-генератор – установка ADS для дистанционного нелетального воздействия на людей прошла сертификацию ВВС США для применения в Ираке. Она излучает направленную энергию в диапазоне миллиметровых радиоволн (частота 94 ГГц), которая оказывает кратковременное шоковое воздействие на людей на расстоянии до 500 м. Прошедший испытания экспериментальный комплекс ADS, получивший наименование System 1, устанавливается на шасси джипа Hummer и оснащен антенной системой, способной формировать луч диаметром 2 м. Пентагон провел сертификационные

испытания установки ADS на добровольцах (военнослужащих и резервистах), которые при облучении испытывали болевой шок и рефлекторное стремление немедленно скрыться из зоны поражения. Около 10 тыс. проведенных испытаний показали, что болевой порог достигался в течение секунды облучения, а после 5 с боль становилась невыносимой [300].

4.9.6. Геофизическое оружие

Поражающее действие геофизического оружия основано на использовании в военных целях природных явлений и процессов, вызываемых искусственным путем. В зависимости от среды, в которой происходят эти процессы, оно подразделяется [300]:

- на атмосферное;
- на литосферное;
- на гидросферное;
- на биосферное;
- на озонное.

Средства, с помощью которых стимулируются геофизические факторы, могут быть различными, но энергия, затрачиваемая этими средствами, всегда значительно меньше энергии, выделяемой силами природы в результате вызванного геофизического процесса [300].

Атмосферное (погодное) оружие – наиболее исследованный на сегодня вид геофизического оружия. Его поражающими факторами являются различного рода атмосферные процессы и связанные с ними погодные и климатические условия, от которых может зависеть жизнь как в отдельных регионах, так и на всей планете. На сегодня установлено, что многие активные реагенты, например йодистое серебро, твердая углекислота и другие вещества, будучи рассеяны в облаках, способны вызывать проливные дожди на больших площадях. С другой стороны, такие реагенты, как пропан, углекислота, йодистый свинец, обеспечивают рассеяние туманов. Распыление этих веществ может осуществляться с помощью наземных генераторов и бортовых устройств, устанавливаемых на самолетах и ракетах [300].

В районах, где влагосодержание воздуха велико, указанным выше методом можно вызывать ливневые дожди и тем самым изменять водный режим рек, озер, болот и соответственно значительно ухудшить проходимость дорог и местности, а в низменных районах вызывать наводнения или, наоборот, засуху [300].

Литосферное оружие основано на использовании энергии литосферы, то есть внешней сферы «твердой» Земли, включающей земную кору и верхний слой мантии. При этом поражающее действие проявляется в виде таких катастрофических явлений, как землетрясение, извержение вулкана, перемещение геологических образований. Источником выделяющейся при этом энергии является высвобождаемая напряженность в тектонически опасных зонах [300].

Гидросферное оружие основано на использовании в военных целях энергии гидросферы – прерывистой водной оболочки Земли, располагающейся между атмосферой и твердой земной корой (литосферой) [300].

Использование энергии гидросферы в военных целях возможно при воздействии на гидроресурсы (океаны, моря, реки, озера) и гидросооружения не только ядерных взрывов, но и крупных зарядов обычного взрывчатого вещества. Поражающими факторами гидросферного оружия будут высокие волны и затопления [300].

Биосферное (экологическое) оружие основано на катастрофическом изменении биосферы. Биосфера охватывает часть атмосферы, гидросферу и верхнюю часть литосферы, которые взаимосвязаны сложными биохимическими циклами миграции веществ и энергии. В настоящее время имеются химические и биологические средства, применение которых на обширных территориях может уничтожить растительный покров, поверхностный плодородный слой почвы и тем самым истощить запасы продовольствия и др. [300].

Искусственно вызванные эрозия почвы, гибель растительности, непоправимый ущерб флоре и фауне вследствие применения различного рода химических средств, зажигательного оружия могут привести к катастрофическому изменению биосферы и, как следствие, массовому поражению людей [300].

Озонное оружие основывается на использовании энергии ультрафиолетового излучения (УФ-излучение), излучаемого Солнцем. Экранирующий озонный слой простирается на высоте от 10 до 50 км с максимумом концентрации на высоте 20-25 км и резким убыванием вверх и вниз. В нормальных условиях поверхности Земли достигает незначительная часть УФИ с длиной волны 0,01-0,2 мкм. Основная ее часть, проходя через атмосферу, поглощается озоном, рассеивается молекулами воздуха и частицами пыли. Озон – один из наиболее сильных окислителей, убивает микроорганизмы, ядовит. Его разрушение ускоряется в присутствии ряда газообразных примесей, в особенности брома, хлора, фтора и их соединений, которые могут быть до-

ставлены в озонный слой с помощью ракет, самолетов и других средств [300].

Частичное разрушение озонного слоя над территорией противника, искусственное создание временных «окон» в защитном озонном слое могут привести к поражению населения, животного и растительного мира в запланированном районе земного шара за счет воздействия больших доз жесткого ультрафиолетового излучения и других излучений космического происхождения [300].

Примерный перечень геофизических эффектов и последствий от активных воздействий на различные геосферы, а также возможные методы и средства воздействий, исходя из общих физических соображений, представлены в табл. 4.13 по данным из работы [300].

Таблица 4.10. Перечень эффектов и последствий при активных воздействиях на различные геосферы [300]

Геосферы	**Методы и средства воздействия**	**Эффекты и последствия**
Литосфера, включая земную кору и почву	- подземные и подводные ядерные взрывы или взрывы химических ВВ; - взрывы на шельфе или в прибрежных водах; - сейсмовибраторы или вибраторы в подземных выработках или скважинах, заполненных водой.	- инициирование землетрясений; - возможно усиление вулканических извержений и возникновение эффектов «цунами»; изменение химического и вещественного состава почвы, в том числе радиоактивное и химическое загрязнение.
Гидросфера (океаны, моря)	- выброс в приземные слои атмосферы различных химически активных веществ или пылевых компонентов, влияющих на солнечное излучение; - создание регионального парникового эффекта, способного привести к образованию атмосферных явлений, возникающих, например, при развитии процесса Эль-Ниньо.	- развитие тайфунов, ураганов и штормов; возникновение волн цунами и нагонных волн; изменение погоды и возможно кратковременные изменения климата.

Продолжение табл. 4.10

Геосферы	Методы и средства воздействия	Эффекты и последствия
Приземные слои атмосферы	- выброс в атмосферу различных химически активных и аэрозольных (пылевых) компонентов; - воздействие электромагнитным СВЧ-излучением и тепловым потоком.	- увеличение осадков, приводящих к наводнениям; ускорение таяния снегов и ледников; - уменьшение осадков, приводящих к засухам; - возникновение разрушительных ураганов в различных широтах; - изменения прозрачности атмосферы и, как следствие, погоды в локальном или региональном масштабах.
Озоносфера	- выброс в озоносферу различных химических и выше веществ; - создание на высотах озоносферы искусственных образований, влияющих на распространение солнечного излучения; - воздействие УФ и СВЧ-излучений.	- создание новых и расширение существующих озоновых дыр и соответствующее увеличение интенсивности жесткого ультрафиолетового излучения, падающего на землю; - рост концентрации озона; - изменение радиационного баланса атмосферы.
Ионосфера	- инжекция различных химических веществ (газообразных, дисперсных); - инжекция электронов, ионов; - воздействие мощного ОНЧ, КВ и СВЧ-излучений, а также источников УФ-излучения; взрывы химических ВВ.	- изменения в ионном и нейтральном составе среды с последующим значительным влиянием на функционирование различных радиотехнических и оптических средств; - инициирование высыпания заряженных частиц из различных слоев ионосферы; - вариации геомагнитного и электрического полей Земли локального и другого масштабов; - возникновение искусственных молний.

Окончание табл. 4.10

Геосферы	Методы и средства воздействия	Эффекты и последствия
Магнитосфера и околоземное космическое пространство	- инжекция электронов и плазмы; воздействие мощным ОНЧ-излучением; выброс мелкодисперсных веществ (типа «иголок»); взрывы химических ВВ.	- изменение магнитного поля Земли; изменение электрического поля приземных слоев атмосферы; - возникновение искусственных или изменение параметров естественных радиационных поясов Земли; возможность увеличения «космического мусора».

Несмотря на подписание большинством стран – членов ООН Конвенции 1978 г. «О запрещении военного и любого иного враждебного использования средств воздействия на природную среду» и наличие возможности ведущих индустриальных государств осуществлять глобальный мониторинг физических параметров окружающей среды, ряд крупных корпораций и фирм промышленно развитых стран (в первую очередь, США, Японии и Великобритании) в последние годы значительно расширили тематику исследований по активному воздействию на среду обитания человека, а также на атмосферные процессы, способные оказывать существенное влияние на космические системы (разведка, связь, навигация) [300].

Много внимания уделяется исследованиям свойств ионосферы и развивающихся в ней динамических процессов. Ионосфера расположена в верхних слоях атмосферы на высотах более 50-80 км и характеризуется значительным содержанием свободных электронов и ионов. Она оказывает большое влияние на распространение радиоволн, поэтому это одна из важнейших геосфер для использования радиосвязи КВ-диапазона, а также для спутниковой связи [300].

Для изучения состояния и свойств ионосферы используются, в частности, так называемые нагревные стенды – источники радиоволн высокой мощности для диагностики ионосферы. Такие стенды сооружены во многих странах: «Сура» в России, EISCAT в Норвегии, HAARP в США на Аляске и др. По мере роста мощности этих стендов в обществе возникла тревога по поводу последствий от их воздействия на ионосферу [300].

Экспериментальные и теоретические исследования по воздействию на ионосферу мощным КВ-излучением американской установки HAARP показывают, что из-за увеличения излучаемой мощности

нельзя ожидать возникновения новых геофизических эффектов, принципиально отличающихся от уже обнаруженных и изученных явлений. Говорить же о каких-либо глобальных возмущениях окружающей среды, отмеченных ранее, пока оснований нет. Тем не менее при дальнейшем увеличении мощности излучения последствия от такого воздействия на ионосферу заслуживают специального изучения [300].

Учитывая результаты проведенного анализа, геофизическое оружие в данный момент следует пока рассматривать в качестве гипотетического. Однако не исключена возможность, что из-за бурного развития науки и техники в недалеком будущем исследования по проблеме примут реальные практические очертания, появятся принципиально новые подходы к технологии создания некоторых видов геофизического оружия [300].

4.9.7. Оружие на основе нанотехнологий

Важное место в ряду новейших технологий, отвечающих потребностям создания как высокотехнологичных образцов ВВТ, так и техники гражданского назначения нового поколения, занимают нанотехнологии, позволяющие видоизменять вещество на уровне молекул и атомов.

В общем случае под нанотехнологиями следует понимать совокупность знаний и документированных данных о методах, приемах и способах, обеспечивающих возможность контролируемым образом создавать и модифицировать объекты, включающие компоненты с размерами менее 100 нм (1 нм=10^{-9}м) хотя бы в одном измерении [13, 201, 202].

Развитию нанотехнологий – научно-технологического направления, сформировавшегося на стыке физики, химии, биологии, медицины и материаловедения, придается огромное значение во всех развитых в техническом отношении странах мира. Во многих странах программы развития нанотехнологий отнесены к высшим национальным приоритетам.

В ряду приоритетных направлений развития наноиндустрии в мире можно выделить следующие [13]:

- создание наноматериалов двойного назначения со специфическими эксплуатационными свойствами (прежде всего прочностными характеристиками);
- материалы и технологии для наноэлектроники и нанофотоники;

- углеродные наноматериалы и наноструктуры (углеродные нанотрубки, фуллерены и др.);
- медицинские препараты и биоматериалы.

При этом существует два различных концептуальных подхода к обработке вещества и созданию планируемых изделий на наноуровне. Эти подходы условно названы технологиями «сверху-вниз» и «снизу-вверх» [13, 217].

Подход «сверху-вниз» основан на уменьшении размеров физических тел механической или иной обработкой, вплоть до получения объектов с ультрамикроскопическими, нанометровыми параметрами. В качестве простого примера можно привести некоторые полупроводниковые устройства, структура которых создается фотолитографической обработкой. При фотолитографии полупроводниковая заготовка подвергается обработке лазерным лучом, что позволяет получить в ней заранее спланированную конфигурацию схемы. Разрешающая способность (т.е. минимальный размер элементов изготавливаемой схемы) определяется при этом длиной волны лазерного излучения. В настоящее время самые короткие длины волн такого излучения позволяют осуществлять микрообработку с точностью до 100 нм. Следует, однако, отметить, что эта технология является сложной и требует дорогостоящего оборудования, вследствие чего она малопригодна для организации эффективного крупномасштабного производства [13, 217].

Идея технологии «снизу-вверх» заключается в том, что сборка создаваемой «конструкции» осуществляется непосредственно из элементов «низшего порядка» (атомов, молекул, структурных фрагментов биологических клеток и др.), располагаемых в требуемом порядке. Этот подход можно считать «обратным» по отношению к изложенному выше методу миниатюризации «сверху-вниз», который заключается в простом уменьшении размеров деталей. Типичным примером подхода «снизу-вверх» может служить поштучная укладка атомов на кристаллической поверхности при помощи сканирующего туннельного микроскопа или других устройств подобного типа. Этот метод позволяет наносить друг на друга не только отдельные атомы, но и целые их слои. Несмотря на то, что в настоящее время описываемый подход характеризуется весьма низкой эффективностью и производительностью, по оценкам специалистов, ему принадлежит будущее [13, 217].

Военное применение нанотехнологий, прежде всего, направлено [13]:

- на снижение заметности вооружения и военной техники;
- на обнаружение «невидимых» ВВТ противника;
- на снижение энергопотребления;
- на создание самовосстанавливающихся систем (например, позволяющих автоматически восстанавливать поврежденную поверхность танка или самолета);
- на создание вычислительных и связных систем;
- на создание устройств обнаружения химических и биологических загрязнений.

Конечной целью использования нанотехнологий в интересах развития вооружения и военной техники может считаться создание идеального элемента ВВТ, масса, габариты и энергоемкость которого стремятся, как ни парадоксально это звучит, к нулю, а его способность выполнять требуемые функции не уменьшается. Предельный случай идеализации элементов ВВТ заключается в уменьшении их размеров при одновременном увеличении выполняемых функций [13].

В ведущих в военно-техническом отношении зарубежных странах (США, Германия, Великобритания, Франция, Швеция) проводится широкий спектр НИОКР, связанных с чисто военными приложениями нанотехнологий. Ведущая роль в этих исследованиях и разработках принадлежит США, которые в последние годы резко увеличили объем военных НИОКР в данной области.

Министерство обороны США проявило интерес к нанотехнологическим исследованиям более 20 лет назад, а в 1996 г. «нанонаука» была внесена в список шести стратегических направлений научно-технических исследований в области обороны. После принятия в 2000 г. «Национальной нанотехнологической инициативы» американское военное ведомство стало получать значительную долю выделяемых на нее ассигнований. Доля Министерства обороны составляет около четверти всех ассигнований, выделяемых в рамках «Национальной нанотехнологической инициативы», вследствие чего оно занимает второе место в списке финансирования развития нанотехнологий по министерствам и агентствам, уступая лишь национальному научному фонду США [202].

Основными направлениями нанотехнологических исследований и разработок, осуществляемыми в интересах ВС и разведывательных ведомств США, являются следующие [13]:

- фундаментальные нанотехнологические исследования в интересах решения общих задач национальной безопасности;
- создание наноструктурных материалов с заданными свойствами;
- создание наноструктур в интересах разработки прототипов функциональных наноустройств;
- создание новых типов детекторов химических, биологических, радиологических и взрывчатых веществ;
- создание приборов и инструментов для нанотехнологических исследований, в том числе метрологического оборудования;
- развитие наноэлектроники, нанофотоники и наномагнетиков в интересах создания перспективных радиоэлектронных средств и систем связи;
- создание новых типов систем аккумулирования и преобразования энергии;
- создание нанороботов;
- использование нанотехнологий для защиты окружающей среды.

Среди западноевропейских стран наиболее серьезных успехов в военных приложениях нанотехнологий добилась Франция, Министерство обороны которой было одним из организаторов Второй международной конференции по микро- и нанотехнологиям, состоявшейся в Гренобле в 2001 г. [13].

Военные эксперты уверены, что использование нанотехнологий в военной сфере в корне изменит характер боевых действий – война станет более быстрой и разрушительной. При этом нанотехнологии планируется применять как для создания оружия, так и для создания оборонительных систем. Главная особенность нанооружия состоит в том, что против него нет другой защиты, кроме нанозащиты. При этом масштаб исследований и рост числа полуфантастических проектов сдерживаются лишь гипотетической опасностью – пока неизвестна токсичность наноматериалов [89].

Есть, безусловно, и геополитическая сторона гонки нанотехнологий – страна, первая освоившая и выпускающая вооружения во всем нанодиапазоне, приобретет огромную военную силу, которой мало кто сможет противостоять. Мощность нанофабрик в отличие от ядерного комплекса может расти не по дням, а по часам. Миллионы боевых устройств можно будет выпускать за считанные часы. Эвентуальный

противник не сможет узнать об этом даже с помощью изощренной разведки. Как следствие, баланс сил может измениться [89].

Пока еще не до конца понятно, как нанотехнологии повлияют на развитие человеческой цивилизации, и пока не предусматривается надежных мер контроля исследований в области молекулярного производства. Однако уже сейчас можно сказать, что дальнейшее развитие нанотехнологий опасно [89].

Кроме опасности неконтролируемой гонки нановооружений возникает опасность бесконтрольного использования нанотехнологий отдельными организациями и группами людей. Особенно опасно, если эта группа людей или организация использует молекулярное производство монопольно. Такой нанодеспотизм является второй угрозой использования нанотехнологий в обществе [89].

Еще одной угрозой является потенциальная техногенная катастрофа, возникшая из-за того, что при нанотехнологических исследованиях не побеспокоились о безопасности их проведения. Это может случиться как в любой стране, так и в любой исследовательской группе или организации [89].

Благодаря потенциалу наносборки и молекулярного конструирования станет возможным создание невидимых видов вооружения, которое станет опаснее химического и биологического видов оружия. Нанотехнологичное оружие может стать одним из новейших видов «грязного» оружия массового поражения. Ведь нанороботы могут полностью уничтожить биосферу Земли, используя ее как строительный материал [89].

Нанотехнологии фундаментально изменят природу войны. Благодаря возможностям наносборки и молекулярного конструирования станет возможным создание невидимых видов вооружений, настолько же опасных и массовых, как биологическое или химическое оружие. Однако нанотехнологическое оружие благодаря способу его производства будет более избирательным. Наноружие будет создаваться с атомарной точностью, что позволит создавать роботов, по размеру меньших, чем бактерии в биологическом оружии. Кроме того, таких нанороботов, в отличие от бактерий, можно будет программировать. Это означает, что наноружие сможет обойти оборону противника и нанести удар по целям, действуя по принципу высокоточного оружия, но в наномасштабе.

Развитие радикально новых видов оружия всегда сопровождается нарушением установленных международным сообществом правил. Так как технология молекулярного производства позволит созда-

вать гораздо более опасные виды оружия, чем существуют сегодня, мы можем ожидать попыток введения контроля за ними и их распространением. Наиболее очевидной является попытка их полного запрещения, однако вряд ли она сработает. В прошлом ни одна попытка о полном запрете вооружений не работала, и нет никаких оснований надеяться, что нанотехнологии в этом плане будут отличаться от своих предшественников [89].

Таким образом, нанотехнологии могут стать причиной серьезных конфликтов, в том числе вооруженных. Данное утверждение базируется на том, что сложившаяся в мире геополитическая ситуация в значительной степени опирается на созданную систему глобального контроля уровня вооружений и военной техники технологически развитых стран. В случае же нанотехнологий контроль практически невозможен, в крайнем случае, весьма проблематичен [89].

Нанотехнологии позволяют создавать принципиально новые виды оружия в виде миниатюрных (наноразмерных) автономных роботов, которые могут быть изготовлены в огромных количествах и способны осуществлять разведывательные, диверсионные и военные операции, в том числе вывод из строя ракетно-ядерного оружия [89].

Наличие нанотехнологического оружия принципиально изменит военную стратегию и потребует учета следующих факторов, таких как [89]:

- минимум необходимого числа военнослужащих;
- скрытый характер собственной военной мощи;
- возможность первого сокрушительного удара по противнику с минимальной или нулевой возможностью ответа.

Военные специалисты полагают, что нация, имеющая решающее преимущество в нанотехнологии, сможет уничтожить любого противника. При этом нанотехнологическая война будет беспрецедентно быстрой и глобально разрушительной.

Новое нанооружие может принять вид легко размножаемых нанобиороботов, способных внедряться в генетическую структуру человека. Испытания такого оружия могут быть проведены скрытно, вне рамок общественного сознания. Важно и другое: его не нужно создавать и хранить как обычное вооружение. Достаточно отладить и иметь в действии производственные комплексы в виде самовоспроизводящихся систем с коротким временем генерации оружия. Такие системы могут размещаться не обязательно на собственной территории. Они могут находиться в океанах и в космосе. Их назначение, как и назначение самого оружия, нельзя определить обычными методами [89].

В связи с развитием нанотехнологий следует особо выделить направления возникновения новых военно-технических угроз, таких как [89]:

- новые типы обычного оружия повышенной точности и поражающей силы;
- боевые автономные миниатюрные системы наземного, воздушного и космического базирования, в том числе распределенные (типа «рой»);
- сверхскоростные информационные распределенные системы;
- ультрасверхвысокочастотные радиоэлектронные средства обнаружения и связи;
- распределенные сенсорные сети (типа «умная пыль») специального назначения;
- имплантируемые микро- и наносистемы, предназначенные для управления человеком, изменения его потенциальных возможностей и «манипулирования» человеческим организмом;
- биологическое и химическое оружие триггерного и генетически избирательного действия.

Примеры технологий, используемых при создании наноружия, приведены ниже.

Покрытия из нанокерамики уже сейчас применяются в 150 областях, их, к примеру, используют при изготовлении валов пропеллеров, телескопических перископов и т. д. Нанокерамика используется везде, где необходимы водонепроницаемость и защита от коррозии. К тому же новый материал гораздо прочнее обычной керамики и не столь ломок [89].

В США военные машины предполагается оснастить специальной «электромеханической нанокраской», которая позволит менять цвет, наподобие хамелеона, а также предотвратит коррозию и сможет «затягивать» мелкие повреждения на корпусе машины. «Краска» будет состоять из большого количества наномеханизмов, которые позволят выполнять все вышеперечисленные функции. На исследования «нанокраски» министерство обороны США выделяет около двух миллиардов долларов в год. Также с помощью системы оптических матриц, которые будут отдельными наномашинами в «краске», исследователи хотят добиться эффекта невидимости машины или самолета [89].

Для защиты от спор Bacillus anthracis, т.е. бактерий, наиболее распространенных в качестве военного бактериологического агента,

компания Nanomaterials Research Corp. предложила использовать фуллерены, соединенные с антителами. Результаты клинических испытаний препарата показали, что он убивает саму бактерию и ее споры до того, как концентрация патогенов в организме приведет к его смерти. При этом с момента заражения организма антраксом проходит 24 ч [89].

Другим проектом является создание чипа для определения биологической опасности размером с почтовую марку. Устройство может определить присутствие нескольких видов различного бактериологического оружия. На его базе выпущен детектор HANAA, который можно использовать в полевых условиях. Прибор питается от батареек и весит около 1 кг. Его принцип действия основан на репликации ДНК-образца с помощью полимеразной цепной реакции. Когда же искомой ДНК становится достаточно для определения, прибор ее обрабатывает с помощью флуоресцентных меток и соотносит с одним из запрограммированных типов патогенной ДНК. Весь процесс обработки четырех различных образцов занимает 30 мин [89].

С помощью нанотехнологий была создана кремниевая микрокамера, в которой происходит процесс нагрева-охлаждения ДНК. Как говорят разработчики прибора, он может опознать патоген при концентрации 10 бактерий в 1 пробе, которая представляет собой капсулу диаметром 5 мм и 2 см длиной. Так как такие токсины, как рицин, не содержат ДНК и соответственно не могут быть опознаны детектором Handheld Advanced Nucleic Acid Analyzer HANAA, компания также выпустила устройство на основе иммунохимического чипа, которое может опознавать 5 токсинов типа рицина. Эти устройства были успешно испытаны на специальном танке FOX в ходе войны в Ираке. Танк обнаружил следы рицина, зарина, споры антракса и другие токсины [89].

Разработаны воздушные фильтры на основе нановолокон, которые первоначально предназначались для астронавтов NASA. Благодаря ультрамалым порам (около 50 нм) фильтр не пропускает отдельные вирусы и бактерии. Сферой использования и детекторов, и средств защиты будет охрана аэропортов, многоэтажных зданий, больниц, правительственных учреждений и пр. [89].

Ученые, которые занимаются созданием нанооружия, утверждают, что благодаря потенциалу наносборки и молекулярного конструирования станет возможным создание невидимых перспективных видов вооружения, которое будет в десятки раз мощнее обычного оружия. Оно будет напоминать облако пыли, способное взорвать лю-

бой объект, в том числе и подземный. По мнению ряда зарубежных военных специалистов, разведка местности с помощью «умных молекул» станет возможной уже через 7-10 лет [89].

Облако «умной пыли» будет состоять из пылинок, представляющих собой часть системы наблюдения и анализа. Среди них будут видеокамеры с возможностью передачи информации, узлы обработки разведданных. Такой разведцентр, напоминающий небольшое дымное облако, должен самостоятельно перемещаться и обладать высокой степенью живучести и защищенности. Сценарий разведки местности такой «умной пылью» будет следующим. Распыленное в окрестностях важного объекта облако незаметно перемещается в его сторону. Попутно выбираются оптимальные места для размещения «субоблаков». Облако видеонаблюдения, каждая пылинка которого представляет собой отдельный пиксель матрицы с интерфейсом связи с соседями, стремится занять лучшую позицию для большего обзора пространства. Жучки или, возможно, «мошки» устанавливают «контроль за звуками». Самая сложная часть – передача информации в штаб разведки в ближайшее время вряд ли сможет обойтись без засылки агента с устройством, считывающим ее [89].

По данным «Национальной нанотехнологической инициативы» США в 2006 г. в Афганистане были испытаны системы слежения за передвижением войск союзников НАТО, чтобы координировать их действия. Встроенные компьютеры позволят активировать на расстоянии любой вид оружия, а более компактные источники энергии позволят сильно улучшить возможности боевых роботов. При этом в ходе военных действий армии будут уничтожать людей, а не военную технику или промышленные предприятия [89].

Самая очевидная и простая в исполнении задача, которую можно будет поручить уже самым первым, сравнительно большим стайным нанороботам, состоит в физическом уничтожении сил противника с помощью микрозарядов взрывчатки. Будучи сброшенным с самолета, БПЛА облако само автоматически ищет цели, разделяется на кластеры необходимого для их поражения размера, облепляет их, проникая в незащищенные места, и синхронно подрывается. Получившийся объемный взрыв сжигает системы управления техникой и опустошает самые защищенные бомбоубежища с максимальной эффективностью, недоступной обычным видам вооружения [89].

Аналитик Т. Маккарти утверждает, что нанотехнологии будут способствовать снижению уровня экономического влияния отдельных государств. В ходе военных действий армии будут предпочитать уни-

чтожать людей, а не военную технику или промышленные предприятия. Нанотехнологии позволят организовать промышленное производство даже в регионах, где нет минеральных ресурсов. Они сделают небольшие группы вполне самодостаточными, что может способствовать распаду государств [89].

В США уже создан Институт военных нанотехнологий – для разработки вооружения и экипировки «солдата будущего». Это будет, собственно, уже не солдат в привычном сегодня понимании, а отдельный самостоятельный механизм. Например, форма одежды у него будет толщиной всего несколько миллиметров. Ее планируют создать на основе нановолокна из нанополиуретана. Последний по структуре очень напоминает паутину. Это, по сути дела, мягкая броня, защищающая солдата от неограниченного количества пуль – в отличие от современных бронежилетов, где количество принятых пуль ограничено. Пульс, давление и температуру солдата считывают микроскопические датчики, размещенные в костюме, данные передаются врачу, который находится в сотнях километров от места боевых действий. Врач дает «костюму» команду сделать необходимые инъекции. «Костюм» же предупредит солдата о химической или биологической атаке. Приказы универсальному солдату будут приходить, отображаясь на защитном стекле его шлема. Шлем заменит ему и бинокль, и прибор ночного видения. В рюкзаке за спиной солдата разместится аппаратура глобальной системы позиционирования, которая не позволит ему заблудиться даже в самой сложной местности [89].

Помимо США над несколькими военными проектами, в которых предполагается использование нанотехнологий, работают специалисты Израиля, Великобритании, Франции и других технологически развитых стран.

Например в Великобритании одним из наиболее интересных нанопроектов является проект механического летающего насекомого MFI (Micromechanical Flying Insect). В рамках этой программы в Центре исследований в области наноэлектроники в Глазго, уже создана математическую модель процесса собирания микроустройств в стаи и обмена информацией между ними для совместных действий. Ведутся разработки моделей боевого применения групп MFI в различных видах боя. Планируется, что себестоимость таких насекомых составит около 10 центов, а производить их будут так называемые «нанофабрики» прямо на поле боя [89].

В Китае в настоящее время насчитывается около 800 компаний, занимающихся внедрением нанотехнологий и более 100 научно-

исследовательских лабораторий. Характер их работы традиционно остается закрытым. Однако не исключено, что большинство из них ориентировано на удовлетворение нужд оборонно-промышленного комплекса. Так, известно, что наибольший интерес у китайских военных вызывают микрочипы, способные повышать живучесть личного состава при применении противником оружия массового поражения [89].

Таким образом, нанотехнологии в перспективе можно отнести к тем видам оружия, которые могут в ближайшем будущем принципиально изменить ведение войн за счет создания принципиально новых наступательных и оборонительных систем.

4.10. Перспективные исследования в интересах дальнейшего совершенствования вооружения и военной техники (на примере исследований агентства DARPA)

4.10.1. Общая характеристика агентства DARPA и проводимых ею проектов

Разработка новых вооружений и систем военного назначения требует существенного научно-технического задела во многих областях фундаментальной и прикладной науки. Ниже представлены основные тенденции по перспективным исследованиям, проводимым в интересах совершенствования вооружения и военной техники на примере Агентства передовых оборонных исследовательских проектов Министерства обороны США – DARPA.

DARPA – агентство передовых оборонных исследовательских проектов в структуре министерства обороны США, целью которого является сохранение технологического превосходства вооруженных сил США, предотвращение внезапного для США появления новых технических средств вооруженной борьбы, поддержка прорывных исследований, преодоление разрыва между фундаментальными исследованиями и их внедрением в военную сферу [234].

Несмотря на то, что деятельность DARPA концентрируется преимущественно на военной проблематике, заметная часть его программ посвящена разработке технологий, имеющих двойное назначе-

ние. Интернет, производство полупроводников и интегральных схем – в основе всех этих направлений, широко использующихся в настоящее время гражданским сектором, лежат разработки, осуществленные при непосредственном участии DARPA.

Существование DARPA в развитой системе поддержки оборонных НИОКР США может показаться избыточным – ведь военные ведомства (Армия, ВМС и ВВС) имеют в своем подчинении собственные научно-исследовательские подразделения, деятельность которых направлена на решение текущих технологических задач этих ведомств и специализированные лаборатории оборонных исследований. Однако DARPA в США было создано именно для того, чтобы устранить узкие места ведомственных НИОКР, оказать финансовую поддержку тем проектам, которые не могут быть поддержаны и профинансированы в рамках исследовательских программ других военных ведомств [234].

Основная задача DARPA – приведение в соответствие военным задачам технологических возможностей, включая новые боевые концепции, которые открываются с помощью этих технологий. Сложность состоит в том что, во-первых, некоторые военные задачи не имеют простого и очевидного технического решения, а во-вторых, многие возникающие технологии могут иметь значение для вооруженных сил только в долгосрочной перспективе. При этом риск неуспеха может быть достаточно высоким.

Структуру DARPA составляют 6 основных отделов, которые ведут исследования по следующим направлениям, такие как [234]:

- адаптивное управление AEO (Adaptive Execution Office) – исследования в области построения адаптивных платформ и архитектур, включая универсальные программные платформы, модульные аппаратные средства, многофункциональные информационные системы и средства разработки и проектирования;
- оборонные исследования DSO (Defense Sciences Office) – исследования в области фундаментальной физики, новых технологий и приборов на новых физических принципах, энергетики, новых материалов и биотехнологий, прикладной и вычислительной математики, медико-биологических средств защиты, а также биомедицинских технологий;
- инновации в информационных технологиях I2O (Information Innovation Office) – информационные системы мониторинга и управления, технологии высокопроизводительных вычислений, интеллектуальный анализ данных,

системы распознавания образов, когнитивные системы машинного перевода;

- микросистемные технологии MTO (Microsystems Technology Office) – технологии электроники, фотоники, микромеханических систем, перспективной архитектуры интегрированных микросхем и алгоритмов распределенного хранения данных;
- стратегические технологии STO (Srtategic Technology Office) – системы связи, средства защиты информационных сетей, средства РЭБ, системы устойчивые к кибератакам, системы обнаружения замаскированных целей на новых физических принципах, энергосбережение и альтернативные источники энергии;
- тактические технологии TTO (Tactical Technology Office) – современные высокоточные системы вооружения, лазерное оружие, беспилотные средства вооружений на базе воздушных, космических, наземных и морских платформ, перспективные космические системы мониторинга и управления;
- биологические технологии BTO (Biological Technologies Office) – исследования в области инженерной биологии, включая омиксные технологии, синтетическую биологию, метаболическую инженерию, генную терапию (включая искусственную хромосому человека), прикладные аспекты нейронаук.

Большинство технологических новшеств, сформировавших облик современных вооруженных сил США, было разработано и внедрены при непосредственной поддержке DARPA – рис. 4.56. К ним относятся: технология Stealth, различное высокоточное оружие, новейшие средства разведки и наблюдения.

Для выполнения поставленных задач в рамках своей деятельности DARPA реализует собственный управленческий поход к руководству процессами разработки проектов новых технологий и продуктов военного назначения, который сводится к «привлечению к работе эксперта и предпринимательски настроенного менеджера программы, поощрению этих специалистов, предоставлению им максимальной свободы действий, а также быстрому принятию решений относительно тех проектов, которые следует начинать, и тех, которые следует признать тупиковыми и прекратить дальнейшую работу над ними» [234].

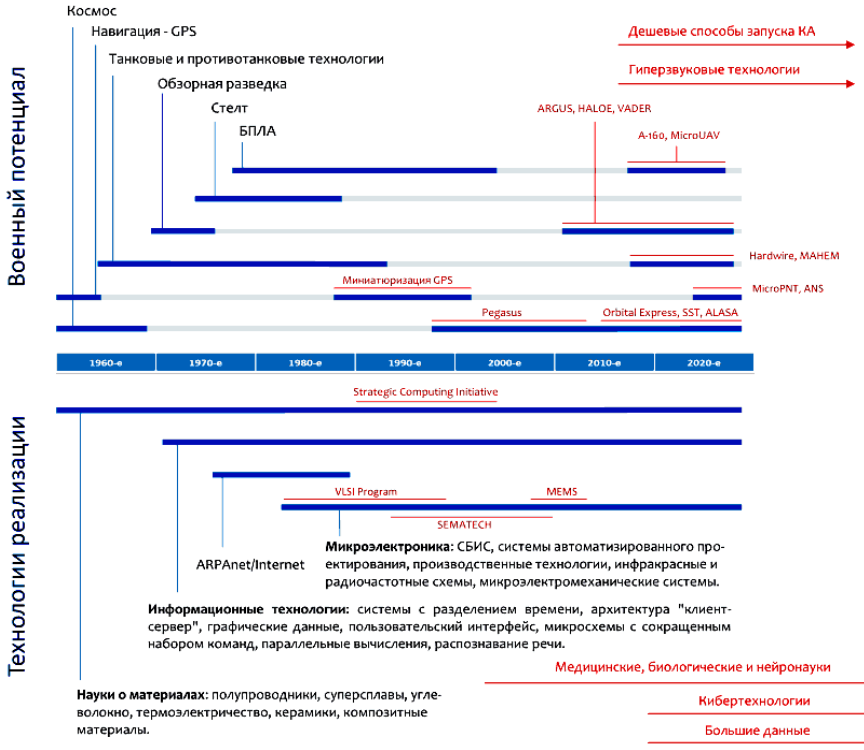


Рис. 4.56. Современные и перспективные программы DARPA [234]

Анализируя программы DARPA можно отметить реализацию создаваемых технологий в нескольких конкретных приложениях – расширение возможностей человека в реальном мире за счет робототехнических средств, использование человеком виртуального мира как части «дополненной реальности». Как результат – разработка комбинации методов управления и преобразования объектов из живого, неживого и виртуального миров на пути достижения военного технологического превосходства. Таким образом, разрабатываемые новые передовые исследовательские программы условно можно разделить на три технологии [234]:

- технологии человека;
- технологии робототехники;
- сетевые технологии.

Технологии человека – возможность инженерного оперирования клетками, словно деталями большого механизма, для излечения

безнадежных больных, восполнения потери частей тела, создания еще более существенных технологий здоровья, а также использования биологических механизмов для производства и сервиса. Научные области технологий человека [234]:

- регенеративная медицина;
- клеточные технологии;
- генетика;
- вирусология;
- синтетическая биология;
- морская биология;
- пилотируемая космонавтика и космические исследования.

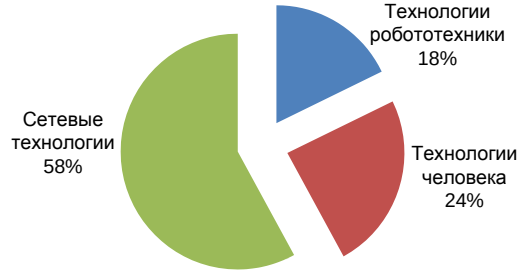
Технологии робототехники – возможность механических операций, наблюдения и доставки грузов в любое время и в любое место, включая миниатюрные манипуляции, скоростные и высотные перемещения, наземный автоматический транспорт и подводные операции. Научные области технологий робототехники [234]:

- аэромеханика;
- адаптивные системы управления;
- распознавание образов;
- спецхимия;
- материаловедение (сверхпрочные материалы, управление формой и механическими напряжениями);
- радиоэлектроника (миниатюризация, компонентная база);
- фотоэнергетика;
- источники питания;
- космическое приборостроение;
- инерциальная навигация.

Сетевые технологии – оперирование совокупностью объектов, средств и систем как единым управляемым пространством, в частности развитием технических средств связи, разведки и обработки информации, а также средств научно-технической разведки, социокультурного анализа и интернет-технологий. Научные области сетевых технологий [234]:

- волновая электроника;
- информационные технологии;
- математика и алгоритмы;
- визуализация данных;
- связь;
- кибертехнологии и защита информации;
- машинные средства языкового перевода.

Анализ финансирования отдельных технологических направлений (рис. 4.57), а также программ, работа по которым продолжится как минимум до 2020 г. (табл. 4.11), позволяет сделать вывод, что ядро исследований DARPA составляют технологии совершенствования сетевых и вычислительных возможностей. При этом безусловное лидерство принадлежит сетевым технологиям [234].



№ п/п	Направление	Количество программ	Расходы, тыс. долл.
1	Технологии робототехники	8	60 210
2	Технологии человека	9	82 000
3	Сетевые технологии	21	196 220

Рис. 4.63. Распределение затрат по программам DARPA в 2015 г. [234]

Таблица 4.11. Существующие в настоящее время в DARPA направления создания технологий, работа по которым, по всей видимости, продолжится как минимум до 2020 г. [234]

Сфера исследований	Разрабатываемые технологии
Сетевые технологии	- обработка структурированных и неструктурированных данных больших объемов и значительного многообразия для получения человекочитаемых результатов; - программные реализации концепции «системы систем»; - игрофикация управления операциями на боевом пространстве.
Технологии автоматической коммутации событий реального и виртуального миров	- групповое управление «роем» роботов. - «Интернет вещи»; - адаптивные производственные линии и «микрофабрики»; - системы дополненной реальности и электростимуляции ЦНС.

Окончание табл. 4.11

Сфера исследований	Разрабатываемые технологии
Технологии человека	- биологическая защита от неизвестных ранее патогенов; - терапия нейротравм центральной нервной системы; - фундаментальные механизмы старения организма; - системы автоматизированного проектирования живых существ.
Технологии робототехники	- высокоэффективные транспортные средства доставки персонала и грузов; - автономные операции роботов (подводные, наземные, воздушные); - энергообеспечение длительных автономных действий; - навигация в условиях радиоэлектронного противодействия; - робототехнический транспорт для воздушного и водного пространства, пересеченной местности и дорог общего пользования.
Технологии интеграции возможностей человека и робота для действий в реальном мире	- роботы для снижения физической нагрузки на человека; - автоматические средства мониторинга и коррекции здоровья; - расширение возможностей органов чувств за счет использования электронных сенсорных систем.
Технологии интеграции и взаимного усиления возможностей человека и компьютерных сетей	- системы ускоренного обучения человека; - системы поддержки принятия решений в науке и медицине; - системы искусственного интеллекта в проведении кибероперациий; - нестандартные аппаратные средства (нейроморфные чипы, и др.) обработки сложноструктурированных данных.
Интегрированные сетевые технологии преобразования реального мира за счет взаимодействия человека и роботов	- управление конфигурацией когнектома мозга человека и животных; - единое боевое пространство (объединяющее как виртуальную, так и реальную составляющие) с универсальным протоколом проведения операций; - автономная ресурсо-независимая робототехника и обеспечивающая инфраструктура.

Ниже представлен обзор некоторых научных программ DARPA, выполнявшихся в 2015 г. и по тематике исследований, относящихся к прорывным военным исследованиям, которые в самом ближайшем будущем могут существенно повлиять на принципы ведения войны и обеспечить для США технологическое доминирование в военной сфере.

Обзор программ исследований DARPA основан на материалах работы [234] и классифицирован не в соответствии с принадлежностью к конкретному направлению DARPA (как это сделано в первоисточнике), а в соответствии с принадлежностью к одной из предметных областей развития вооружений, рассмотренных в вышестоящих подразделах:

- базовые технологии в радиотехнике, электронике и оптике;
- вычислительные системы и системы обработки информации;
- системы связи и инфокоммуникаций;
- технологии разведки, наблюдения и целеуказания;
- авиационные и космические технологии;
- технологии робототехники;
- технологии кибербезопасности и информационного противоборства;
- оружие на новых физических принципах;
- технологии транспортировки и транспорта;
- технологии новых материалов и биотехнологии.

4.10.2. Базовые технологии в радиотехнике, электронике и оптике

4.10.2.1. Технологии радиотехники

Разработка адаптивных радиочастотных технологий – *программа ART* (*Adaptive Radio Frequency Technology*). Программа ART предусматривает удовлетворение потребности вооруженных сил в доступных, компактных, энергоэффективных, коммутационных и сенсорных интерфейсах в радиочастотном диапазоне. Эти интерфейсы способны автоматически адаптироваться к условиям внешней среды в режиме реального времени, а также выбирать оптимальные параметры приема, передачи и обработки сигналов с возможностью самостоятельной модификации и перестройки архитектуры аппаратной части в зависимости от внешних условий. Реализация программы позволит

обеспечить бойцов (наряду с малогабаритными автономными роботизированными транспортными платформами, включая БПЛА) компактными и эффективными системами структурно-параметрической идентификации сигналов для создания когнитивных технологий управления следующего поколения для перспективных радиоэлектронных систем, связи, безопасности и разведки [234].

Создание адаптивной масштабируемой фазированной антенной решетки *– программа APAA* (*Adaptive Phased Antenna Array*). Программа APAA предусматривает создание единых принципов построения базовой АФАР для различных видов военной техники. В рамках программы разрабатывается единый блок радиочастотных решеток и изменяемый электромагнитный интерфейс. Технология должна позволить объединять несколько пространственно-распределенных небольших АФАР решеток в одну [234].

Разработка цифрового приемника широкого диапазона *– программа DISARMER* (*Direct SAMpling Digital ReceivER*). Программа предназначена для производства гибридных фотонно-электронных аналого-цифровых преобразователей (АЦП), способных работать во всем X-диапазоне (8-12 ГГц). Использование высокостабильной оптической синхронизации позволит улучшить динамический диапазон в 100 раз. Такая широкая полоса пропускания вкупе с высокой надежностью приемника найдет применение в системах РЭБ и радиотехнической разведке, так как потенциально позволяет существенно сократить расходы, размер и вес таких систем. В ходе программы DISARMER будет разработан, изготовлен и протестирован гибридный фотонно-электронный АЦП [234].

Формирование облика перспективных приемопередающих устройства миллиметрового диапазона *– программа MWFT* (*Millimeter-wave Frequencies Transceiver*). Программа MWFT предусматривает развитие систем связи, радиолокации и радиоразведки на основе приемопередающих средств в миллиметровом диапазоне длин волн. Это позволит обеспечить как уменьшение загруженности приемопередающих трактов при заданной пропускной способности системы, так и снижение вероятности обнаружения и перехвата радиосигнала вероятным противником. Реализация программы будет основана на использовании набора широкополосных приемопередающих устройств с высоким динамическим диапазоном и фотонных компонентов, обладающих высокими характеристиками скорости обработки данных мониторинга в миллиметровом диапазоне длин волн. Разрабо-

танные в рамках этой программы технологии будут использованы в средствах ВМС и ВВС [234].

Разработка технологий повторного использования электромагнитного спектра *– программа Spectrum Efficiency and Access.* В настоящее время в связи с широким распространением радиосредств гражданского и военного назначения остро стоит вопрос нехватки имеющейся полосы частот. Минобороны необходимы технологии, нуждающиеся в меньшей ширине спектра. Программа предусматривает разработку принципов повторного использования спектра, например, совместное использование частот и координации между сенсорными/радиолокационными системами [234].

4.10.2.2. Технологии электроники

Создание кортикального процессора *– программа Cortical Processor.* Выделение закономерностей и сигналов, имеющих сложную пространственную форму и временное распределение в больших потоках зашумленных и неоднозначных данных, является серьезной проблемой даже для самых современных систем анализа сигналов и изображений. Существующие вычислительные подходы в подавляющем большинстве ресурсоемки и способны извлечь лишь ограниченную часть полезной информации из больших объемов данных. Современный машинный интеллект плохо распознает аномальные сигналы, требуя распознавания всех аспектов нормального сигнала для того, чтобы определить аномальные части. Поэтому должны быть разработаны новые подходы для решения этих задач, основанные на низком энергопотреблении. Программа Cortical Processor предусматривает создание аппаратной имитации неокортекса. Неокортекс в живой природе используется для выполнения высших мозговых функций, таких как чувственное восприятие, моторные команды, пространственное мышление, сознательное мышление и язык. В рамках программы должен быть разработан «кортикальный процессор» на основе иерархической временной памяти. По аналогии с нейронными моделями, в частности коры головного мозга, процессор должен распознавать сложные пространственные и временные закономерности, а также адаптироваться к меняющимся условиям [234].

Формирование задела по терагерцовой радиоэлектронике *– программа Terahertz Electronics.* Переход в терагерцовый диапазон позволит в будущем создавать радиолокационные системы высокого разрешения, близкого к разрешению оптико-электронных систем,

надежные системы связи с миниатюрными антеннами, а также высокоэффективные спектроскопы для обнаружения взрывчатых веществ. Программа предусматривает разработку и демонстрацию материалов и технологий производства транзисторов, микросхем приемников и генераторов терагерцовых частот, а также малогабаритных мощных усилителей с масштабируемыми вакуумными приборами [234].

Разработка методов интеграции разнородных электронных систем *– программа DAHI* (*Diverse & Accessible Heterogeneous Integration*). Характеристики электронных микросистем играют жизненно важную роль в широком перечне боевых и обеспечивающих систем, стоящих на вооружении. Именно они обеспечивают технологические преимущества над противником в таких сферах, как радиолокация, радионавигация, радиосвязь и РЭБ. Существующие производственные технологии ограничиваются конечной совокупностью материалов и систем, которые могут быть взаимно интегрированы, заставляя разработчиков идти на компромиссы при выборе комплектующих для создания электронных микросистем. В рамках этой программы проводятся исследования по поиску новых технологий, позволяющих комплексировать электронные микросистемы различного назначения и материалов изготовления на основе единой микросхемы [234].

Формирование научно-технического задела по переходу на новые технологии создания микроэлектронных компонентов *– программа FAB* (*Fast and Big Mixed-Signal Designs*). Основным преимуществом кремниево-германиевой технологии (SiGe) производства компонентов микроэлектроники является возможность создания приборов для работы на высоких частотах (до 110 ГГц). Программа FAB предполагает разработать технологический процесс создания SiGe-компонентов, способных к интеграции с CMOS-компонентами, созданными с использованием 14 нм технологического процесса [234].

4.10.2.3. Технологии оптики

Формирование научно-технического задела в области фотоники *– программа BPS* (*Basic Photon Science*). В программе рассматриваются основы генерации, управления и обнаружения фотонов, их взаимодействия в интегрированных устройствах, начиная от присущей им способности переноса информации (в традиционном и квантовом смысле) до новейших методов оптической модуляции, использующей не только амплитудную и частотную модуляцию, но и дополнительную модуляцию по орбитальному угловому моменту. Результа-

ты программы BPS позволят Минобороны разработать новые методы связи, обработки сигналов и визуализации в дополнение к лучшему пониманию физических пределов совершенствования технических параметров оптических систем. Созданные технологии могут быть использованы для миниатюризации систем разведки, наблюдения и рекогносцировки, в том числе на основе новых подходов к генерации оптических сигналов и оптического деления частоты, а также для применения в системах синхронизации времени от ультрастабильных оптических часов, СВЧ-приборах со сверхнизким уровнем фазового шума, эталонных генераторах частоты и настольных источниках когерентного рентгеновского излучения, а также изолированных источниках нейтронов для медицинской и иных сфер применения [234].

Разработка фотонных коррелляторов для задач обработки критически значимых данных *– программа Gargoyle.* Датчики, процессорные устройства и пользователи массово передают данные, но развитие вычислительных возможностей их обработки существенно запаздывает, не справляясь с все возрастающими потоками информации. Например, совокупный мировой поток данных через оптоволоконные кабели в настоящее время составляет более 100 ТБ/с и, как ожидается, превысит 1 ПБ/с к 2020 г. Программа Gargoyle предполагает разработку фотонных коррелляторов для задач обработки критически значимых данных, обеспечивая почти нулевое время ожидания и обработку как цифровых, так и аналоговых данных в оптической форме с высокой пропускной способностью. Требования к этой технологии включают широкополосную модуляцию методом прямого расширения спектра с полосой пропускания более 10 ГГц и обеспечение киберзащиты в волоконно-оптических сетях с возможностью расширения скоростей передачи данных до значений более 10 ТБ/с [234].

Разработка технологий автоматизированного синтеза цифровых оптических систем на чипе *– программа DODOS* (*Direct On-Chip Digital Optical Synthesis*)**.** Развитие методов точного управления частотой радиоволн в 1940 г. революционно изменило военные исследования. Регулирование частоты радиоволн является технологией, используемой в радиолокации, спутниковой и наземной связи, а также в технологиях зондирования и навигации. Однако на сегодняшний день синтез оптических частот ограничен лабораторными условиями из-за большого размера, относительной хрупкости и высокой стоимости оптических синтезаторов. Программа DODOS предусматривает решение задачи автоматизированного синтеза цифровых оптических систем на одной микросхеме. Планируется объединение несколь-

ких разработок для создания универсальной микросхемы с интегрированным синтезатором оптических частот, что позволит обеспечить возможность построения на его основе широкополосных когерентных систем оптических коммуникаций, портативных высокоточных атомных часов, а также высокоточных систем обнаружения сверхмалых концентраций опасных газов или токсичных веществ [234].

4.10.3. Вычислительные системы и системы обработки информации

4.10.3.1. Вычислительные системы

Формирование научно-технического задела в области нечеткой обработки сигналов и интеллектуального использования данных *– программа UPSIDE* (*Unconventional Processing of Signals for Intelligent Data Exploitation*). Суть проекта заключается в создании новых микросхем, которые будут работать на принципах вероятностных аналоговых вычислений. Построенный на их основе компьютер станет оперировать не значениями бит, а вероятностями принятия ими конкретных значений. Ожидаемым результатом программы должна стать вычислительная машина, реализующая «мягкие» вычисления, с более низким энергопотреблением, чем сравнимые с ней по вычислительной мощности традиционные компьютеры [234].

Разработка технологии вероятностного программирования для самообучающихся машин *– программа PPAML* (*Probabilistic Programming for Advancing Machine Learning*). Эта программа ставит целью разработать интеллектуальные машины, которые будут учиться с помощью алгоритмов вероятностного программирования обрабатывать базы данных большого объема и выбирать наилучшие варианты решения задач. Разработанный в ходе этой программы искусственный интеллект будет учиться и спустя некоторое время сможет легко решать простые задачи. Технология PPAML поможет Минобороны более эффективно решать множество аналитических задач, которые сегодня требуют существенных людских ресурсов, таких как: разведка, наблюдение, распознавание речи, вождение автомобиля, просеивание информации в поисках ценных данных и т.д. При этом предполагается использование самых различных аппаратных платформ – суперкомпьютеров на базе многоядерных процессоров, кластеров обычных ПК и облачных сети [234].

Создание высокоэффективных встраиваемых вычислительных систем *– программа PERFECT* (*Power Efficiency Revolution for Embedded Computing Technologies*). Программа PERFECT разрабатывает средства решения проблемы нехватки вычислительных ресурсов для создания встраиваемых цифровых систем нового поколения. В рамках программы должны быть созданы новые компьютерные системы производительностью 75 Гфл/Вт., при этом действующие системы показывают пока в 75 раз худшие результаты. Согласно результатам предварительных экспериментов нижняя граница энергоэффективности для масштабных гетерогенных многозадачных систем оценивается в 50 Гфлопс/Вт. Предполагается, что аппаратными средствами для таких систем будут являться чипы, производимые по техпроцессу с нормами 7 нм. Разработка PERFECT подразумевает синхронизацию работ по пяти направлениям: программно-аппаратная архитектура; параллельная обработка множества потоков; устойчивость системного и прикладного софта по отношению к программным ошибкам и воздействиям; оптимизация трафика обрабатываемых данных; новые алгоритмы, обеспечивающие высокую устойчивость работы и низкое потребление энергии [234].

Разработка защищенной облачной инфраструктуры, обеспечивающей сетевую поддержку военных операций *– программа MRC* (*Mission-oriented Resilient Clouds*). Создаваемые по программе MRC системы должны обеспечить индивидуальную безопасность серверных узлов в облаке и обеспечить их способность продолжать устойчивую работу в ситуации, когда составные части подвержены кибер- или физическим атакам и выведены из строя, а ключевые узлы вследствие побочных эффектов функционируют со сбоями [234].

Создание технологии быстрой разработки программного обеспечения за счет использования двоичных логических элементов *– программа RAPID* (*Rapid Software Development using Binary Components*). В рамках программы RAPID разрабатывается система идентификации и извлечения компоненты программного обеспечения для повторного использования в новых приложениях. У Минобороны есть критически важные компьютерные приложения, которые должны быть перенесены в будущие операционные системы. Во многих случаях исходный код приложения недоступен для редактирования, что вынуждает продолжать использование программного обеспечения на устаревших и более не поддерживаемых разработчиком операционных системах. Технологические разработки по программе выполняются в

рамках направления «С3: системы навигации, управления и связи» [234].

Разработка технологии интеграции системных архитектур *– программа System of Systems Architecture, Technology Development, and Demonstration*. Программа SSATDD нацелена на поиск путей интеграции системных архитектур и различных программных сред в единую аппаратно-программную универсальную среду для ее эффективного использования в многокомпонентных коммуникационных системах [234].

4.10.3.2. Обработка информации и анализ данных

Формирование научно-технического задела в области обработки «Больших данных» *– программа Big Mechanism.* Эта программа предусматривает создание новых подходов к автоматизации вычислительного интеллекта применительно к таким областям как биология, виртуальное пространство, экономика, социальные науки и разведка. Освоение этих областей требует технологии создания абстрактных, прогнозных, а в идеале – причинно-следственных моделей из массивных объемов разнородных данных, генерируемых человеком, сенсорами и сетевыми устройствами. В качестве модели для исследований рассматриваются научные данные в области лечения рака. В рамках программы Big Mechanism уже в 2015 г. стало возможным определить мишени для терапии, основанные на выводах анализа разнородных данных [234].

Разработка человеко-машинных интерфейсов экспертных систем – *программа HCS* (*Human and Computer Symbiosis*). Программа направлена на разработку компьютерной технологии для поиска и использования источников информации. Технология HCS позволит компьютерам определять, в какой момент им будет необходима информация, составлять и отправлять тексты с вопросами к экспертам, взаимодействовать с ними и извлекать знания из их ответов. Приобретая знания и встраивая их в современные экспертные системы, компьютеры будут специализироваться и станут сами экспертами в предметной области. Когда достаточное количество компьютеров соберет необходимый объем знаний, люди начнут использовать их через интерфейс экспертных систем. Главная техническая проблема касается формулировки, в которой излагаются вопросы и ответы. Некоторым вопросам будет достаточно естественных языков, но в некоторых слу-

чаях потребуются математическая формализация, рисунки или другая формулировка [234].

Создание виртуального вычислительного интеллекта – *программа CCI* (*Cyber Computational Intelligence*). Данная программа направлена на создание новых подходов к вычислительному интеллекту, функционирующему в виртуальном пространстве. В корпоративных сетях и в Интернете размещены огромные массивы данных, сгенерированные разнообразными сетевыми элементами, узлами и конечными пользователями. Эти данные, как правило, не имеют никакого стандартного формата, и большинство из них предназначено для оператора-человека. Технологии CCI облегчат использование неформализованных данных, позволят контролировать события в сети, в том числе и обнаруживать нападения с использованием уязвимостей нулевого уровня, оптимизировать производительность сетей, обеспечивать производительности сетей в условиях кибератак, а также восстанавливать их работоспособность после нападения [234].

Разработка технологии глубокого анализа и фильтрации текстовых материалов – *программа DEFT* (*Deep Exploration and Filtering of Text*). Программа разработана для помощи военнослужащим, работа которых связана с принятием решений на основе выводов, полученных из информации, содержащейся в текстах. Создаваемые в рамках DEFT технологии автоматизированного глубокого понимания естественного языка смогут обеспечить разработку решений для более эффективной обработки текстовой информации, исключая возможность ее двусмысленного понимания со стороны человека-оператора [234].

Разработка технологии формальная верификация математических решений в игровой форме *– программа CSFV* (*Crowd Sourced Formal Verification*). Сложные математические проблемы можно представить в виде интересных и увлекательных игр, в которые люди будут с удовольствием играть онлайн. Привлечение в эти игры множества игроков потенциально позволит разгрузить аналитиков в сфере безопасности. Программа CSFV направлена на представление серьезных математических задач в виде интересных головоломок, которые игроки могут решать для собственного удовольствия. С помощью интеллекта и изобретательности игроков планируется сократить нагрузку на аналитиков силовых ведомств и коренным образом улучшить доступность формальной верификации математических решений [234].

Разработка технологии глобальной аналитики – *программа QGA* (*Quantitative Global Analytics*). Программа QGA предусматривает разработку и интеграцию технологий анализа большого объема данных в целях превентивного обнаружения опасных тенденций и глобального прогнозирования. Входными данными для работы алгоритмов прогнозирования служит социально-экономическая информация – рыночные цены, уровни производства, показатели международной торговли и уровни экспорта. Программа будет использовать сочетание количественного анализа глобальных и региональных экономических и финансовых данных с использованием математических методов, анализа социальных сетей, количественной социологии и климатических исследований. Разработанные в рамках программы технологии позволят повысить ситуационную осведомленность и формировать прогнозы о новых классах экономико-социальных и экологических угроз [234].

Совершенствование технологий поиска в сети Интернет – *программа Memex*. В рамках этой программы разрабатываются информационные технологии, способные быстро и тщательно найти и структурировать множество интересующих сведений в сети Интернет. В рамках этой работы будут рассмотрены недостатки централизованного поиска для предметно-ориентированной индексации веб-контента, а разработка нового алгоритма поиска обеспечит быстрый, гибкий и эффективный доступ к предметно-ориентированному содержанию. В результате реализации программы планируется создать сверхмощную поисковую систему на основе усовершенствованных поисковых программ, которая будет способна вести поиск в самых отдаленных уголках сети, которые недостижимы для современных интернет-поисковиков, обеспечивая своим пользователям технологическое превосходство в области индексации контента и веб-поиска [234].

Разработка технологий обработки «Больших Данных» – *программа XDATA*. В рамках этой программы разрабатываются вычислительные методы и программные инструменты анализа больших объемов данных, как «полу-структурированных», так и неструктурированных. Планируется решить следующие основные задачи: создать масштабируемые алгоритмы обработки «сырых» данных в распределенных хранилищах и создать эффективные средства взаимодействия человека с компьютером, помогающие с помощью настраиваемой визуализации делать логические выводы из данных, полученных из различных источников. В рамках программы будет дан толчок развитию инструментария с открытым кодом в интересах гибкого создания про-

граммного обеспечения для обработки больших объемов данных в сроки, заданные требованиями оборонных проектов [234].

Создание системы автоматизированного контент-анализа изображений и мультимедиа *– программа VMR* (*Visual Media Reasoning*). Сегодня объем визуальных данных необычайно быстро растет и уже сейчас опережает возможности ручного анализа, не говоря уже о том, чтобы анализировать каждое изображение в отдельности. В рамках программы VMR будет разработано программное обеспечение, позволяющее визуально исследовать миллионы цифровых фотографий и каталогизировать их по тому или иному признаку [234].

Разработка системы информационного обеспечения для бойцов сухопутных сил – *программа IS2* (*Infantry Squad Systems*). Программа IS2 предусматривает создание технических систем, позволяющих отдельному бойцу получать многократное информационное преимущество при выполнении специальных операций. Применение систем многоспектрального зрения, датчиков, информационных интерфейсов в составе экипировки военнослужащего позволяет ему многократно увеличить свои боевые возможности, превратив его в «универсального солдата» [234].

Создание интегрированной системы сбора распределенной информации и планирования нанесения комплексного удара – *программа IPSIS* (*Integrated Planning for Strike, ISR, and Spectrum*). Программа IPSIS предусматривает:

- создание единой интегрированной системы сбора информации с распределенных датчиков на борту пилотируемых и беспилотных транспортных средств (наземных, подводных, аэрокосмических);
- автоматизации процесса поддержки принятия решений оператором при планировании и нанесении комплексного удара с использованием тактических и стратегических систем ракетного вооружения;
- интеллектуальное определение оптимальных средств и параметров нанесения такого удара.

При создании интегрированной системы будут предусмотрены различные режимы работы в зависимости от функций оператора (от системы мониторинга до полуавтоматической активной системы), а также подсистема планирования и оптимизации ракетного удара в зависимости от окружающей обстановки и задач специальных операций. Разработанные в рамках программы технологии будут переданы ВМС и ВВС [234].

Разработка технологии «доказательства агрессии» – *программа Battlefield Evidence.* На сегодняшний день основной объем работы по судебно-криминалистической экспертизе приходится на долю аналитиков и следователей, осуществляющих кропотливый поиск всей доступной информации с последующим представлением полученных данных в виде логичной цепочки событий. Программа Battlefield Evidence предусматривает создание технологий для поиска и сопоставления разнообразных типов неструктурированной информации, включая медиаматериалы для получения необходимых доказательств действий злоумышленников. Планируется развить, объединить и расширить технологии поиска текста, речи и видеоинформации для представления в виде соответствующей пространственно-временной информации. Программа также разовьет и применит методы, позволяющие аналитикам эффективно и на уровне интуиции искать подозрительные действия, неочевидные отношения и другие зацепки для последующих оперативных мероприятий [234].

4.10.4. Технологии связи и инфокоммуникаций

Разработка концепции адаптивной распределенной мобильной сети *– программа CBMANET* (*Control-Based Mobile Ad Hoc Networking*). Проект предусматривает разработку радиосети, которая будет обладать значительно большими гибкостью и устойчивостью по сравнению с существующими беспроводными сетями. Частной целью является создание комплексного аппаратно-программного решения со специальным стеком протоколов и набором унифицированных служб, которое бы позволяло развертывать беспроводную сеть с возможностью динамического конфигурирования ее характеристик. Основное внимание будет уделяться эффективности управления сетевыми ресурсами, организации взаимодействия между элементами стека протоколов и гибкости конфигурирования сети, а также применяемым методам коллективного доступа, маршрутизации и администрирования. Согласно требованиям к перспективной радиосети ее узлы планируется оснащать ненаправленными антеннами и приемопередатчиками с мощностью излучения не более 5 Вт [107].

Создание мобильных адаптивных сетей нового поколения *– программа WNaN* (*Wireless Network after Next*). Основная цель данной программы заключается в разработке беспроводной сети, обеспечивающей быструю настройку сетевой конфигурации и ее функций при минимальной стоимости сетевого оборудования. Предполагается, что

с уменьшением себестоимости оборудования станет возможным формирование крупных сетей, которые состоят из множества размещенных с высокой плотностью узлов с передатчиками относительно небольшого радиуса действия. Это позволит значительно увеличить устойчивость и целостность сети, поскольку при высокой плотности увеличивается количество резервных маршрутов для передачи данных из одной точки сети в другую, а также обеспечить доступ к сети максимального числа участников боевых действий. Разрабатываемые решения будут представлять собой оснащенные серийными четырехканальными радиостанциями беспроводные узлы, в которых должна быть реализована поддержка технологий многоканальной обработки MIMO (Multiple Inpit Multiple Output), а также значительно расширена функциональность сетевого уровня. Этот шаг позволит обеспечить интеграцию на основе данной платформы разрабатываемых в рамках программы CBMANET методов адаптивной маршрутизации и сетевого управления, алгоритмов динамического использования спектра, технологий пространственного разделения каналов, а также ряд других процедур коммутации и маршрутизации [107].

Разработка устойчивой системы авиационной поддержки – *программа PCAS* (*Persistent Close Air Support*). Сегодня чтобы вызвать авиационную поддержку, приходится вести долгие переговоры с летчиком, соотносить ориентиры на карте и задавать направления голосом, на что может потребоваться более часа. Разрабатываемая по программе PCAS цифровая система позволит сухопутным войскам автоматизировано выбирать тип авиационной поддержки из числа возможных (вертолет, истребитель, бомбардировщик, БПЛА), а также подбирать необходимое вооружение [234].

Создание транспортных беспроводных сетей – *программа Fixed Wireless at a Distance.* Вооруженные силы заинтересованы в системе, способной оперативно обеспечить широкополосную связь без развертывания статичной инфраструктуры и без использования космических каналов связи. Программа FWD предусматривает преодоление ограничений нынешних MANET-сетей, которые масштабируются, в лучшем случае, на сотни пользователей, после чего начинается резкое падение скорости передачи данных в таких сетях. Новые технологии, основывающиеся на коммерческих протоколах, от WiFi до LTE обеспечат гигабитные линии связи за счет использования БПЛА в качестве магистральных узлов [234].

Разработка стандарта радиосвязи с пропускной способностью 100 Гбит/с – *программа 100 Gb/s RF Backbone.* В настоящее

время в ВС США для осуществления коммуникаций различного рода применяется безопасный беспроводной протокол передачи данных Common Data Link (CDL). Он обеспечивает максимальную скорость передачи данных на уровне 250 Мб/с, однако этой скорости уже недостаточно для полноценного управления БПЛА, а также отправления и получения разведывательных данных. Целью программы является создание нового беспроводного стандарта связи, который способен обеспечить скорость передачи данных 100 Гб/с при радиусе покрытия 200 км. При этом требования к массе конечного оборудования и уровню его энергопотребления предъявляются такие же, как и к оборудованию CDL [234].

Разработка новых принципов организации передачи информации на поле боя *– программа CLASS* (*Computational Leverage Against Surveillance Systems*). Программа CLASS предусматривает создание набора модульных информационно-коммуникационных блоков с использованием новейших принципов передачи, приема и обработки радиосигналов для предотвращения возможного перехвата и снижения вероятности обнаружения передаваемых данных на поле боя средствами мониторинга и подавления вероятного противника. Реализация программы будет сосредоточена на трех основных исследовательских направлениях [234]:

- разработка сигналов сложной формы, не поддающихся анализу и дешифровке без знания их исходных свойств и параметров модуляции;
- пространственное распределение приемопередающих систем, позволяющее динамически и адаптивно изменять кажущееся положение источника полезного сигнала для средств мониторинга и подавления вероятного противника;
- управляемая интерференция для многопозиционных систем передачи, которая учитывает естественный рельеф местности и позволяет создавать зоны «гашения» сигнала в местах дислокации противника.

Создание гибкой архитектуры сложных многокомпонентных информационно-коммуникационных систем в «запретных зонах» *– программа CCE* (*Communication in Contested Environments*). В настоящее время наблюдается тенденция постоянного роста объема и скорости обработки данных в распределенных информационно-коммуникационных системах, в том числе в задачах интеграции данных систем мониторинга обстановки и управления человеко-машинными системами в единое информационное пространство. Реа-

лизация программы CCE предусматривает концентрацию на трех основных направлениях [234]:

- совершенствование бортовых систем связи транспортных средств и комплексов вооружений для снижения времени задержки и повышения пропускной способности протоколов обмена информацией;
- выработка требований к информационным системам с учетом возможности интеграции коммерческой коммуникационной архитектуры с аппаратно-программными решениями с учетом специфики оборонной отрасли;
- обеспечение гибкости создаваемой архитектуры для обеспечения высокого резерва по модернизации и возможности замены функциональных компонентов.

Обеспечение гарантированного функционирования систем связи за пределами прямой видимости *– программа ABLSC* (*Assured Beyond Line-of-Sight Communications*). Программа ABLSC предусматривает разработку технологий обеспечения разведзащищенности систем связи мобильных комплексов вооружений в зонах электромагнитной доступности средств радиомониторинга и РЭБ противника. Таким образом, мобильные комплексы вооружений смогут оставаться незамеченными (с точки зрения пеленгования источника радиоизлучений) на территориях, контролируемых противником, при этом сохраняя стабильную связь с другими средствами и системами [234].

4.10.5. Технологии навигации и систем единого времени

Разработка технологий совместного взаимодействия средств в навигационной среде при отсутствии доступа к GPS *– программа CODE* (*Collaborative Operations in Denied Environment*). Программа CODE предусматривает разработку концепции развития коммуникационных технологий и осуществления коллективного взаимодействия подразделений и систем в зонах с отсутствием возможности использования систем глобального позиционирования GPS для снижения зависимости от космических средств навигации и связи. Программа ориентирована на распределение критических навигационных функций (системы зондирования, обеспечения связи и точности навигации) на отдельных относительно небольших БПЛА, повышающих уровень автономности каждой системы [234].

Разработка микротехнологий для местроопределенния, навигации и хранения точного времени *– программа Micro PN&T* (*Micro-Technology for Positioning, Navigation, and Timing*). Средства РЭБ и зоны затрудненного приема могут помешать работать вооружению, которое требует непрерывного контакта с системой GPS. Программа Micro PN&T предусматривает создание высокоточных инерциальных навигационных систем, позволяющих обходиться без приема сигналов GPS. В рамках программы планируется разработка компактных высокостабильных гироскопов, датчиков пространственной ориентации на новейших физических принципах и систем единого времени (СЕВ) на основе технологий холодных атомов со сверхэкономичным потреблением энергии. Планируется создание микроядерного магнитно-резонансного гироскопа, использующего гироскопическое вращение микрочастиц в магнитном поле для определения местоположения. При этом отсутствие у гироскопа движущихся частей делает его не подверженным воздействию таких факторов, как ускорение и вибрация [234].

Создание адаптивной навигационной системы *– программа ANS* (*Adaptable Navigation Systems*). Программа ANS предназначена для обеспечения военнослужащего возможностью эффективно ориентироваться в любой ситуации, включая моменты, когда сигнал GPS недоступен в результате действий средств РЭБ противника, особенностей ландшафта или природных явлений (например, в условиях Арктики или Антарктики). Программа ANS основана на разработке трех основных технологических решений [234]:

- разработка инерциального измерительного блока нового типа, которому требуется меньше фиксаций координат от системы GPS. Например, за счет использования сверхкомпактных атомных часов, использующих холодные атомы;
- создание методов использования эфирных сигналов (SoOp) от различных источников – наземного, воздушного и космического базирования, а также природных сигналов SoOp (навигация по геофизическим полям) в целях уменьшения потребностей коррекции положения по данным GPS;
- разработка методов сочетания данных от SoOp-источников с данными от инерциальных и иных датчиков, то есть многоцелевых навигационных систем, которые могут изменять конфигурацию для обеспечения действий произвольного оборудования при любых условиях.

Разработка перспективных систем независимого точного времени *– программа PTECE (Precision Timing Enabling Cooperative Effects)*. Программа PTECE предусматривает разработку универсальной платформы (независимой от GPS и не уступающей ей по точности) регистрации, синхронизации и передачи информации о времени в пространстве удаленных распределенных взаимодействующих между собой человеко-машинных систем. Научный акцент программы будет направлен на новейшие достижения в области создания компактных атомных часов на основе технологии холодных атомов и оптической сверхскоростной передачи данных для обеспечения возможности глобального доступа, создания недорогостоящей инфраструктуры и повышения уровня помехоустойчивости и защищенности в сложных задачах навигации и пространственного позиционирования [234].

4.10.6. Технологии разведки, наблюдения и целеуказания

Создание адаптивных низкобюджетных сенсоров *– программа ADAPT* (*Adaptable Low Cost Sensors*). Эта программа нацелена на разработку дистанционных датчиков военного назначения с использованием промышленных технологий гражданской индустрии «гаджетостроения». Ожидается, что такой подход позволит быстро и с высокой экономической эффективностью внедрить в производство сенсоры для проведения разведывательных операций, сбора данных и рекогносцировки с быстро обновляемым циклом производства и возможностью регулярного совершенствования выпускаемых устройств [234].

Разработка многофункциональных оптических сенсоров *– программа MFOS* (*Multi-Function Optical Sensing*). Программа MFOS ставит своей целью разработку многофункционального оптического сенсорного датчика, позволяющего реализовать альтернативный подход к обнаружению, слежению и идентификации целей, а также контролю и управлению огнем боевых самолетов (истребителей) с дальним радиусом действия. При реализации программы планируется использование передовых достижений в области создания высокочувствительных матриц фокальной плоскости и технологии компактных многополосных, сканирующих, лазерных систем, работающих в ближайшем, среднем и дальнем инфракрасном диапазонах [234].

Разработка концепции открытой архитектуры для радиоэлектронных систем наблюдения и разведки *– программа SDISR*

(*Software-Defined ISR*). Программа SDISR предусматривает моделирование и создание единой открытой архитектуры радиоэлектронных систем (преимущественно для РЛС) для объединения и интеграции процессов разработки аппаратной и программной составляющих (обычно выполняются независимо) таких систем, а также для повышения эффективности и согласованности их функционирования. Реализация такой единой открытой архитектуры сделает возможным использование унифицированной аппаратно-программной платформы, позволяющей значительно ускорить и повысить эффективность модернизации и отладки проектируемых систем наряду с определением оптимальных путей проектирования новых радиотехнических систем, которая будет востребована при разработке перспективных средств радио-, радиотехнической и радиолокационной разведки [234].

Формирование научно-технического задела по технологиям визуализации и регистрации видеоизображений – *программа MIST* (*Military Imaging and Surveillance Technology*). Программа MIST предусматривает разработку принципиально новых физических принципов решения задач наблюдения и разведки, обеспечивающих получение высококонтрастных пространственных изображений целей высокого разрешения на расстояниях, существенно превышающих возможности существующих оптических систем. Планируются создание и полевые испытания серии опытных образцов, позволяющих надежно регистрировать и распознавать объекты на значительном расстоянии с компенсацией возможных помех из-за турбулентности атмосферных потоков. Научный акцент программы сделан на исследования в области разработки и интеграции компонентов высокоимпульсных лазеров, а также телескопических приемных устройств, исключающих необходимость механической и синтетической апертурной фокусировки, а также на создание вычислительных алгоритмов интеллектуальной обработки изображений для повышения пространственного разрешения изображений и качества распознавания целей [234].

Разработка многофункциональных радиотехнических систем – *программа Multifunction RF.* Эта программа предусматривает достижение существенного повышения функциональных возможностей человеко-машинных систем в области регистрации и восприятия информации об окружающей среде и объектах, а также обеспечение автоматизированной навигации, управления и поддержки принятия решений для перспективных летательных комплексов (включая БПЛА). Реализация программы также позволит обеспечить выполнение автономного взлета и посадки, совершения основных функцио-

нальных маневров во время полета в условиях полного отсутствия видимости [234].

Создание видео локатора с синтезированной апертурой – *программа ViSAR* (*Video-rate Synthetic Aperture Radar*). Цель программы ViSAR – разработка и демонстрация возможностей информационного датчика EHF-диапазона (Extremely High Frequency), который в условиях плотной облачности (естественной, вроде песчаной бури или искусственной дымовой завесы) сможет обеспечивать столь же эффективную работу систем обнаружения, прицеливания и наведения, как и современные ИК-системы в безоблачную погоду [234].

Разработка технологии автоматического распознавания целей – *программа ATR* (*Automatic Target Recognition Technology*). Технологии ATR обеспечивают обнаружение, идентификацию и сопровождение особо важных целей множеством датчиков, объединенных в единый массив. Современные системы такого класса, как правило, разрабатываются для конкретных типов датчиков и нединамичны из-за программных ограничений, таких как заранее определенный перечень целей и рабочих режимов, что ограничивает гибкость выполнения миссии. Программа ATR предусматривает разработку технологий, которые уменьшают эти операционные ограничения, одновременно обеспечивая значительное повышение эффективности систем целеуказания и существенно сокращая время их разработки [234].

Создание автоматизированной системы поддержки принятия решений для аналитиков за счет комплексирования датчиков различных разведывательных платформ – *программа Insight.* Сегодня аналитики разведывательных служб перегружены информацией. Поступающий непрерывный поток данных от датчиков космических, воздушных и наземных средств разведки обеспечивает непревзойденное представление о поле боя. Однако на этапе обработки этой информации многие из программных средств комплексирования не могут легко обмениваться или сопоставлять такую информацию, как, например, видео- и радиолокационные данные. Недостатки современных систем разведки проявляются и в отсутствии автоматизированных средств для интерпретации, редактирования и представления потоков данных в удобной для восприятия форме. Важная информация часто теряется или вовсе не учитывается из-за большого потока входящих данных. Отсутствие комплексных инструментов человеко-машинного интерфейса ограничивает возможности операторов, а также затрудняет разбор и понимание сложных данных. Программа Insight предусматривает создание автоматизированной системы помощи аналити-

кам путем комплексирования датчиков различных платформ в частности, за счет разработки системы эксплуатации и управления ресурсами (E&RM) разведывательной службы нового поколения [234].

Создание глобальной системы сбора информации, наблюдения и разведки *– программа WISR* (*Worldwide Intelligence Surveillance and Reconnaissance*). Данная система обеспечит выполнение разведывательных задач в недоступных ранее районах. Американские войска ограничены в использовании традиционных средств разведки и наблюдения во многих критически значимых местах в мире. В то же время миллионы отправляемых по всему миру видеороликов, число которых только увеличивается, отражают интересные для национальной безопасности, а также важные события в мире. В рамках программы WISR будет произведена интеграция видео- и изображений в 3D- и 4D-реконструкциях событий. Методы WISR также могут быть использованы для отслеживания культурных и социальных изменений при подготовке к вводу на территорию экспедиционных войск [234].

4.10.7. Авиационные и космические технологии

Разработка концепции гиперзвукового воздушно-реактивного оружия *– программа HAWC (Hypersonic Air-breathing Weapon Concept)*. Программа HAWK предусматривает разработку и внедрение технологий, позволяющих существенно повысить эффективность глобального стратегического удара по защищенным целям вероятного противника. В рамках этой программы запланированы демонстрационные испытания новых образцов гиперзвукового реактивного оружия, базирующихся на воздушных платформах. Направления исследования по программе включают в себя [234]:

- оптимизацию конфигурации перспективных воздушных транспортных платформ;
- оптимизацию конфигурации воздушного транспортного средства, влияющую на эффективность гиперзвукового полета;
- разработку новейшей системы углеводородного питания двигателей для обеспечения стабильности гиперзвукового полета;
- разработку методов температурного контроля для выполнения тактических задач в экстремальных средах с высокотемпературными характеристиками;

- адаптацию концепции для гиперзвуковых воздушных платформ многоразового использования в таких проектах, как «Глобальное присутствие» и «Космический лифт».

Формирование предложений по снижению аэродинамического сопротивления для гиперзвуковых систем – *программа TBG* (*Tactical Boost Glide*). Программа TBG предусматривает снижение аэродинамического сопротивления гиперзвуковых систем, в том числе для перспективных БПЛА, крылатых ракет и новых видов вооружения. Реализация программы будет вестись по следующим основным направлениям, таких как [234]:

- концептуальный дизайн и моделирование перспективных гиперзвуковых средств с адаптивными аэродинамическими и аэротермическими характеристиками для широкого спектра практических приложений и тактических задач;
- повышение надежности систем и подсистем наряду с увеличением их показателей живучести при эксплуатации в экстремальных и внешних условиях;
- поиск путей снижения стоимости разработки и испытаний перспективных гиперзвуковых летательных средств с системами адаптивного контроля профиля аэродинамического сопротивления.

Создание летательного аппарата вертикального взлета и посадки – *программа VTOL* (*Vertical Take-Off and Landing Technology Demonstrator*). Программа VTOL предусматривает создание пилотируемого или беспилотного летательного аппарата вертикального взлета и посадки, предназначенного для разведывательно-спасательных операций, наблюдения, транспортировки живой силы, военной техники и участия в специальных операциях. При этом масса аппарата должна составить 4,5-5,5 т, крейсерская скорость полета летательного аппарата – 555 км/ч, при посадке и зависании – не ниже 75% от эффективности при горизонтальном полете, отношение подъемной силы к весу летательного аппарата с полезным грузом – не ниже 10, вес полезного груза – не менее 40% от полного веса [234].

Разработка перспективных технологий воздухоплавания – *программа AAT* (*Advanced Aeronautics Technologies*). Программа AAT предусматривает проверку и оценку новых авиационных технологий с помощью инструментария прикладных исследований. Такие исследования могут включать: анализ пригодности использования в аэронавтике новых материалов, авиационных устройств, анализ тактики применения винтокрылых воздушных транспортных средств и летатель-

ных аппаратов с неподвижным крылом, а также способы их внедрения в производство. Прикладные области варьируются от методов управления движением до техники пилотирования. В результате этих исследований должны быть спроектированы, разработаны или улучшены образцы ЛА [234].

Создание системы автоматизации оборудования кабины экипажа летательных аппаратов *– программа ALIAS* (*Aircrew Labor In-cockpit Automation System*). Программа ALIAS предусматривает разработку аппаратных средств и программного обеспечения для унификации функций экипажа на любых аппаратах, сокращая время на переучивание и освоение новой авиационной техники летчиками [234].

Разработка технологии «воздушного старта» *– программа ALASA* (*Airborne Launch Assist Space Access*). В рамках программы планируется разработать отделяемую космическую ступень для обычных транспортных самолетов, которая могла бы выводить на низкую околоземную орбиту различное оборудование массой до 45 кг. Стоимость вывода оборудования в космос при помощи ALASA, включая стоимость самой ступени и топливные расходы, не должна превышать одного миллиона долларов [234].

Создание системы наблюдения за состоянием космического пространства *– программа SDA* (*Space Domain Awareness*). Программа SDA предусматривает разработку и интеграцию технологий наблюдения за состоянием объектов космического пространства (включая сверхмалые объекты на орбитах дальних планет) для обеспечения высокой осведомленности, которую не в состоянии обеспечить существующие системы разведки и контроля космического пространства. Основными направлениями исследований станут:

- разработка системы миниатюрных датчиков для мониторинга безопасности космического пространства, включая орбиты дальних планет;
- интеграция нетрадиционных методов сбора данных (включая сведения от астрономов- любителей);
- разработка методов анализа больших данных о состоянии всех потенциально опасных объектов и создание синергетической базы данных.

В результате реализации программы станет возможным существенное увеличение наблюдаемого пространства при выполнении дальних космических миссий [234].

Разработка технологий для спутников-инспекторов *– программа Phoenix*. В рамках программы Phoenix разрабатываются техно-

логии, позволяющие демонтировать и использовать повторно ценные компоненты и узлы от вышедших из строя или отработавших свой срок космических аппаратов, находящихся на ГСО. Одним из результатов программы будет специально разработанный спутник-инспектор, способный заниматься выполнением демонтажных, монтажных и ремонтных работ в космосе [234].

Разработка экспериментального воздушно-космического самолета – *программа Experimental Spaceplane One* (*XS-1*). В рамках программы XS-1 разрабатывается средство, которое можно использовать для выведения полезных грузов на низкую орбиту, а также проведения экспериментов на гиперзвуковой скорости, способное работать в условиях чрезвычайно высоких перегрузок, летать в широком диапазоне высот, выдерживать высокую температуру и обеспечивать высокую маневренность на орбите. Создаваемый по программе автоматический аппарат должен [234]:

- развивать скорость 10 М;
- совершать до 10 полетов в течение 10 дней;
- доставлять полезный груз на низкую орбиту;
- взлетать горизонтально с обычного аэродрома.

Разработка телескопа для наблюдения за космическими объектами в околоземном пространстве – *программа SST* (*Space Surveillance Telescope*). На сегодняшний день зарегистрировано порядка 22 тыс. искусственных объектов, которые вращаются вокруг Земли, при этом их число может утроиться в ближайшие 20 лет. Целью программы SST-является разработка технических средств обнаружения небольших объектов и предупреждения их столкновения со спутниками на высотах вплоть до геостационарной орбиты. Создаваемый по программе SST телескоп использует CCD-технологию (Curved Charge Coupled Device) захвата изображения и широкоугольную оптическую систему, благодаря чему он имеет высокую чувствительность, разрешающую способность и большой угол обзора. Небольшие габариты нового телескопа позволили сделать его мобильным, способным к быстрому перемещению в любую точку, оптимальную для наблюдения за выбранным участком неба [234].

Разработка технологий самосборки оптических систем в космосе – *программа OASIS* (*Optical Aperture Self-Assembly In Space*). Программа OASIS предусматривает разработку технологий строительства больших оптических диафрагм на орбите Земли из множества небольших модульных компонентов, самоорганизующихся в оптическую систему в космосе. Программа OASIS должна продемонстриро-

вать способность технологий собирать большие (более 5 м) оптические диафрагмы из модульных компонентов, которые выведены на орбиту как отдельные полезные грузы. При этом должна быть обеспечена расходимость, близкая к дифракционной. Программа OASIS должна на практике продемонстрировать реализацию сборки сложных и прецизионных объектов в космосе, размеры которых в собранной форме больше, чем параметры полезной нагрузки любой существующей или планируемой к разработке ракеты-носителя. Эта возможность позволит собирать орбитальные системы наблюдения и связи, которые невозможно реализовать сегодня, а также в ближайшем будущем в рамках однократно выводимого на орбиту груза [234].

4.10.8. Технологии робототехники

4.10.8.1. Базовые технологии

Проведение «соревнований военных роботов» *– программа Robotics Challenge.* Программа предусматривает создание робототехнических средств для операций по ликвидации чрезвычайных ситуаций. Создаваемые средства должны свободно передвигаться по неровной поверхности и обломкам, использовать обычный и электрический инструмент, управлять транспортными средствами, а также перемещать небольшие грузы. Дистанционно управляемый робот должен обладать определенной степенью автономности на случай помех и обрывов связи, а также быть адаптивным к управлению им неподготовленным оператором [234].

Формирование концепции «кратчайшего пути» в робототехнике *– программа Robotics Fast Track.* Программа RFT стремится коренным образом изменить технологии робототехники, способствуя развитию нестандартных технических решений. Программа предусматривает создание недорогих, крайне практичных составных робототехнических решений. Нестандартность и практичность этих решений предполагается обеспечить за счет вовлечения новых сообществ разработчиков (профессионалов робототехники и энтузиастов) в научно-исследовательские работы. Результатом должны стать опытные образцы и новые концепции, разрабатываемые в короткие сроки, с минимальными затратами по сравнению с традиционными циклами проектирования [234].

Разработка технологий объединения робототехнических систем в «стаи» *– программа Swarm Challenge.* Программа преду-

сматривает разработку алгоритмов управления стаей (роем) для беспилотных транспортных средств (UxVs), задействованных при выполнении боевых операций [234].

Разработка технологий распределенного управления боевым применением сил и средств – *программа DBM* (*Distributed Battle Management*). В настоящее время для управления БПЛА или дистанционным роботом требуется отдельный, прошедший специальную подготовку оператор. Программа DBM ставит задачу дать оператору возможность раздавать задачи и управлять действиями целой группы роботов [234].

Разработка технологий группового управления мобильными объектами – *программа Mobile Hotspots.* По мнению военных специалистов Пентагона, потенциал технических возможностей в ВС используется сегодня далеко не полным образом из-за отсутствия соответствующего программного обеспечения. Так, БПЛА, незаменимые для разведки, наблюдения и рекогносцировки, могли бы быть гораздо более эффективны на поле боя, если бы существовало приложение, позволяющее управлять ими всеми сразу, без необходимости управлять каждым аппаратом отдельно. Разработке такого приложения и посвящена эта программа [234].

4.10.8.2. Технологии для БПЛА

Разработка БПЛА с низкими требованиями к взлетно-посадочному пространству – *программа TERN* (*Tactically Exploited Reconnaissance Node*). Использование БПЛА в интересах ВМС требует наличия авианосцев или больших наземных баз с взлетно-посадочными полосами длиной более 1,6 км. Программа TERN предусматривает использование малых судов в качестве мобильных площадок для запуска и обслуживания БПЛА со средней (до 3000 км) и большой дальностью полета [234].

Создание реконфигурируемой воздушной системы – *программа ARES* (*Aerial Reconfigurable Embedded System*). Программа ARES предусматривает создание компактной высокоскоростной беспилотной системы доставки грузов в опасные и труднодоступные районы, с возможностью вертикального взлета и посадки [234].

4.10.8.3. Технологии для морских необитаемых аппаратов

Создание распределенной адаптивной системы обнаружения подводных лодок противника – *программа DASH* (*Distributed Agile Submarine Hunting*). Программа DASH предусматривает разработку прототипа компактного необитаемого подводного аппарата (без боевой нагрузки, но обладающего системой высокочувствительных надежных глубоководных сонаров) и создание адаптивной системы быстрого обнаружения и определения местоположения судов. Акцент в программе будет сделан на реализацию сети компактных необитаемых подводных аппаратов для мониторинга в контролируемой акватории тихоходных субмарин вероятного противника на основе анализа распределенных гидроакустических данных [234].

Создание распределенных разведывательно-ударных комплексов на основе необитаемых подводных аппаратов – *программа Hydra.* Целью программы является создание комплекса средствмониторинга Мирового океана. Результатом программы должно стать создание и развертывание сети универсальных необитаемых подводных аппаратов с различной полезной нагрузкой. Эта система, как ожидается, позволит контролировать важные акватории. Предполагается, что аппараты, созданные в ходе программы Hydra, смогут взять на себя часть функций кораблей ВМС. Это позволит не только обеспечить военное присутствие ВМС США во всех необходимых регионах, но и сократить затраты на эксплуатацию кораблей и их многочисленные походы. Кроме того, предполагается, что необитаемые аппараты могут нести вооружение [234].

Разработка открытой архитектуры для инфраструктуры подводного обеспечения – *программа UAAI* (*Undersea Architecture: Adaptive Infrastructure*). Программа предусматривает разработку универсальной адаптивной инфраструктуры для обеспечения длительных автономных миссий необитаемых подводных аппаратов и оптимизации их взаимодействия. Реализация в рамках программы единой гибкой распределенной архитектуры обмена информацией и согласования процессов ремонта, возобновления ресурсов и источников питания позволит обеспечить тактические и стратегические преимущетсва от использования мобильных комплексов на основе необитаемых подводных аппаратов (включая малые аппараты) за счет существенного повышения эффективности и согласованности их коллективных действий во время боя и при планировании специальных операций [234].

Разработка прототипа адаптивного многоцелевого подводного аппарата *– программа Blue Wolf.* Программа Blue Wolf предусматривает разработку и испытания прототипа уникального подводного транспортного средства с недостижимыми для обычных субмарин тактико-техническими (скрытность и фактор внезапности) и гидродинамическими характеристиками. Реализация программы направлена на устранение противоречия в эксплуатационном гидродинамическом профиле для необитаемых подводных аппаратов (низкая скорость движения, средняя маневренность, относительно большая продольная протяженность) и систем подводного вооружения (высокая скорость движения, высокая маневренность, относительно малая продольная протяженность), что позволит рассчитать и спроектировать универсальное адаптивное решение [234].

Создание средства автоматического сопровождения противолодочных операций *– программа ASW* (*Anti-Submarine Warfare*) *Continuous Trail Unmanned Vessel* (*ACTUV*). Основной задачей программы является создание необитаемого подводного аппарата ACTUV для обнаружения, отслеживания и сопровождения неопознанных подводных лодок. Ожидается, что судно ACTUV сможет автономно функционировать в море в течение 60-90 суток. Периодически ACTUV будет нуждаться в возвращении в порт для проведения дозаправки, ремонта и технического обслуживания его систем [234].

4.10.9. Технологии кибербезопасности и информационного противоборства

4.10.9.1. Технологии кибербезопасности

Формирование научного задела по транспарентным вычислениям *– программа Transparent Computing.* В рамках программы разрабатываются технологии, позволяющие осуществлять более эффективную политику безопасности в распределенных системах. Масштаб и сложность современных информационных систем скрывает связи между событиями, связанными с безопасностью, в результате чего работа по обнаружению атак и аномалий приходится на контекстную информацию, а не на конкретные события. Этот недостаток существующих систем, основанных на обработке событий, позволяет выполнять такие атаки, как подмена (на уровне пользователя) и мимикрия (на уровне машинного кода). Результат программы особенно важен для обеспечения безопасности крупных информационных систем

с разнородными компонентами, такими как распределенные системы видеонаблюдения, автономные системы и корпоративные информационные системы [234].

Разработка технологий автоматического поиска уязвимостей программного обеспечения – *программа MUSE* (*Mining and Understanding Software Enclaves*). Программа MUSE разрабатывает инструменты для повышения устойчивости и надежности сложных программных систем. Методы MUSE будут применять алгоритмы машинного обучения на основе анализа крупных программных комплексов для исправления ошибок и поиска уязвимостей в существующих программах, а также разрабатывать программы, которые будут удовлетворять предъявляемым спецификациям и требованиям. MUSE должна повысить безопасность программных систем, а также повысить вычислительные возможности в таких областях, как обработка графов, лечение компьютерных вирусов, анализ ссылок, анализ больших данных [234].

Разработка технологии втоматического программного анализа в интересах обеспечения кибербезопасности – *программа APAC* (*Automated Program Analysis for Cybersecurity*). Программа разрабатывает автоматические методы программного анализа для того, чтобы оценивать свойства информационной безопасности мобильных приложений. Программа включает создание новых и улучшение известных методов типизированного анализа, абстрактной интерпретации. Технологии APAC позволят разработчикам и аналитикам идентифицировать мобильные приложения, которые содержат скрытые функционально-деструктивные модули, с последующим их запретом на использование [234].

Разработка технологий гарантированной защиты военной техники от кибератак – *программа HACMS* (*High Assurance Cyber Military Systems*). Как отмечают эксперты, программа HACMS создавалась с целью обеспечения информационной безопасности всей движущейся техники и ориентирована, прежде всего, на БПЛА, но отдельные разработки смогут впоследствии использоваться и для защиты других систем. Результатом проекта HACMS должен стать пакет программных средств, интегрированных в системное ПО и распространяемых как в оборонном ведомстве, так и в коммерческой среде [234].

Создание «чистого» сетевого компьютера – *программа CRASH* (*Clean-slate design of Resilient, Adaptive, Secure Hosts*). Программа CRASH направлена на реализацию компьютерных систем, ко-

торые были бы менее уязвимы для информационно-технических воздействий и более эффективно восстанавливались после того, как их безопасность оказывалась нарушена. Среди базовых основ CRASH в первую очередь называют принципы компартментализации и наименьших привилегии. В соответствии с этим проектом создаваемая компьютерная архитектура должна реализовывать условия, в которых каждый отдельный фрагмент программы должен работать только с теми правами, которые требуются ему для выполнения кода, по сути, динамически изменяя привилегии элементов архитектуры системы [234].

Разработка технологии активной проверки прав доступа – *программа Active Authentication*. Создание для нужд ВС технологии информационной безопасности, основанной на принципе программной биометрии. При этом сканироваться будут не физические характеристики человека, а сочетание поведенческих особенностей, которые присущи пользователю во время его работы на ПК. Метод может включать в себя: анализ закономерностей нажатия клавиш, «узора» движения глаз при чтении, семантический анализ, который оценивает способ поиска, отбора, ввода информации и др. Программа будет фокусироваться на этих особенностях, так как они могут быть столь же уникальны, как, например, отпечатки пальцев. Результат программы может быть установлен на любом компьютере в виде программного обеспечения Active Authentication для проверки «подлинности» сотрудника [234].

Разработка интегрированных систем киберанализа – *программа ICAS* (*Integrated Cyber Analysis System*). Программа ICAS разрабатывает методы автоматического обнаружения зондирования, вторжения и деструктивных действий в корпоративных сетях. В настоящее время обнаружение подобных действий требует кропотливого анализа многочисленных системных журналов высококвалифицированными аналитиками по вопросам безопасности и системными администраторами. Программа ICAS разрабатывает технологии, принимающие во внимание взаимосвязи между обменом данных и характером поведения объектов из всех доступных источников системных данных [234].

Разработка технологии подтверждения аутентичности электронных компонентов – *программа SHIELD* (*Supply Chain Hardware Intercepts for Electronics Defense*). В последние два года на оборудовании, использующемся ВС, было выявлено более миллиона электронных деталей и компонентов сомнительного качества и под-

линности. Программа SHIELD предполагает разработать миниатюрный (100×100 мкм) и недорогой (меньше одного цента за штуку) чип, который будет подтверждать аутентичность электронных компонентов. Чип будет находиться внутри корпуса микросхемы, но никак не будет электрически связан с ее функциональной начинкой и не должен требовать существенных изменений в процессе производства [234].

Разработка концепции защиты кибер-физических систем – *программа PCPS* (*Protecting Cyber Physical Systems*). В последнее время получили развитие кибер-физические системы – специализированные вычислительные системы, имеющие физические средства взаимодействия с объектом контроля и управления (электрические, химические, оптические, механические, биологические и т.п.) и выполняющие единственную функцию. Широкое использование встроенных вычислительных систем в торговле, промышленности и здравоохранении, появление программно-конфигурируемых сетей, а также использование систем автоматического управления военными и гражданскими объектами жизнеобеспечения населения делают их защиту вопросом национальной безопасности. Программа PCPS предусматривает создание технологий для мониторинга распределенных гетерогенных сетей промышленных систем управления, включая обнаружение аномалий, которые требуют быстрой оценки, противодействия атакам типа «имитация соединения» (спуфинг) и «отказ в обслуживании» [234].

Создание активно-реактивных кибернетических систем – *программа ARCS* (*Active-Reactive Cyber Systems*). Программа ARCS предусматривает создание технологий, позволяющих узлам, системам и сетям активно распознавать угрозы и динамически реагировать на кибератаки. Современные технологии киберзащиты, как правило, статически сконфигурированы для удовлетворения целого комплекса инженерных компромиссов и редко бывают оптимизированы под динамические среды, в которых они действуют. Программа ARCS предусматривает создание технологий, которые будут использовать штатные датчики, удаленные контрольно-измерительные приборы и другие источники информации о ситуации в киберпространстве для постоянной оптимизации кибероборонь [234].

Разработка технологий адаптивного информационного доступа и контроля – *программа AIAC* (*Adaptable Information Access and Control*). Программа AIAC предполагает создание способов динамичного, гибкого и надежного обмена тщательно отобранной информацией за пределами защищаемого периметра компьютерной сети организации. В гражданской сфере есть осознанная потребность в техно-

логиях, которые ограничивают обмен информацией между коммерческими предприятиями и правительственными учреждениями. Программа AIAC ориентирована на создание технологий многоуровневой безопасности, избирательного управления доступом и подсистемами обработки политик, чтобы обеспечить специально настроенный доступ к определенным данным, но не ко всей базе данных или к файловой системе. Технологии AIAC будут разработаны для работы с виртуализацией, облачными вычислениями и программно-конфигурируемыми сетевыми технологиями, которые в настоящее время получили широкое распространение в гражданской и военной сферах [234].

Организация соревнований автоматических систем в обнаружении и исправлении уязвимостей нулевого уровня – *программа CGC* (*Cyber Grand Challenge*). В рамках соревнований участники должны разработать принципы усовершенствования систем тестирования программного обеспечения, выявления уязвимостей, генерации патчей и установки их на компьютеры в сети. Все эти задачи должны выполняться полностью в автоматическом режиме. Цель программы CGC – создание автоматической системы, способной находить уязвимости в программах, анализировать их, генерировать патчи и устанавливать их, закрывая, таким образом, обнаруженные «дыры». Если сегодня выпуск патча – дело десятков часов, то предполагается, что программы-победители CGC должны иметь возможность латать «уязвимости нулевого уровня» в течение минут или секунд [234].

Разработка технологий сетевой защиты – *программа Network Defense.* Программа предусматривает создание технологии обнаружения сетевых атак, которая использует сводку данных по сети. Компьютерные сети США постоянно подвергаются атакам, и эти атаки, как правило, обрабатываются отдельными организациями по мере поступления информации об их совершении. Анализ обобщенных данных по широкому кругу сетей позволит выявить закономерности, видимые только на общем фоне. Такой подход позволит обнаружить повторяющиеся атаки, а также закономерности в технике атак и тем самым определить уязвимости. Использование обратной связи с системными администраторами, инженерами по безопасности и лицами, принимающими решения, позволит повысить информационную безопасность в государственных и коммерческих секторах США [234].

Разработка технологий защиты беспроводных сетей – *программа Wireless Network Defense.* В настоящее время беспроводные сети используются все чаще, а это значит, что увеличивается вероятность их случайной или умышленной компрометации. В связи с этим,

необходима проверка служебной и пользовательской информации. Анализируя полученную информацию, сетевые узлы определяют, какие частоты использовать, а также на какой узел дальше передавать данные. Программа Wireless Network Defense разрабатывает новые технологии устойчивого управления беспроводными сетями, сосредоточившись на повышении надежности беспроводных сетей. Сети нового поколения, базирующиеся на протоколах устойчивого управления беспроводными сетями, смогут оперативно выявлять проблемные точки с подозрительной активностью и автоматически адаптироваться к ухудшающимся условиям работы [234].

Создание киберсреды для безопасных распределенных динамических вычислений *– программа SDDC* (*Secure Distributed Dynamic Computing*). Программа SDDC предусматривает создание безопасной киберсреды для создания высокопроизводительных архитектур, сочетающих аспекты параллельных и облачных вычислений с динамическим наблюдением и адаптацией распределенных вычислительных систем к изменениям условий внешней среды. Реализация программы позволит обеспечить автоматизированный динамический контроль и распределение вычислительных ресурсов для обеспечения киберзащиты и поддержания автономного функционирования высокопроизводительных систем обработки больших данных в области мониторинга состояния передового базирования вооруженных сил и поддержки принятия тактических решений на поле боя [234].

4.10.9.2. Технологии информационного противоборства в технической сфере

Создание самоуничтожающейся микросхемы *– программа VAPR* (*Vanishing Programmable Resources*). Микропроцессоры сегодня широко используются практически во всех отраслях человеческой деятельности. В рамках программы VAPR разрабатываются физически самоуничтожающиеся микросхемы, превращающиеся по команде в неспособные к воссозданию элементы. По условиям программы такая «одноразовая» электроника не должна уступать современным коммерческим образцам по основным характеристиками, кроме того, она должна уметь самоуничтожаться при заранее заданных условиях, по команде извне или при попадании в заданное окружение [234].

Создание средств превентивной киберзащиты *– программа ACD* (*Active Cyber Defense*). Предполагается, что созданные по программе ACD технические средства при обнаружении подозрительной

активности в реальном времени активируют средства дезинформации и инициируют превентивные защитные действия по атакующей компьютерной сети [234].

Создание программных средств обхода блокировок в сети – *программа SAFER* (*Safer Warfighter Computing*). Программа SAFER предусматривает создание пакета утилит, который позволит обходить фильтрацию и блокировку по IP-адресам, используемую для создания «черных списков» сайтов и сервисов операторами связи. Одновременно пакет утилит позволит противостоять средствам фильтрации контента, которые перехватывают и анализируют трафик пользователя путем глубокой проверки содержимого пакетов на наличие заранее заданных сигнатур или ключевых слов [234].

Разработка информационно-технических средства проведения кибератак – *программа Logan*. Программа Logan обеспечит для ВС возможность расширить способности проведения компьютерных атак. Разработанные технические средства позволят разрушать и ослаблять информационные системы противника [234].

Разработка технологий управления ведение боевых действий в киберпространстве в режиме реального времени – *программа Plan X*. Целью программы является создание революционных технологий, которые позволят понимать, планировать и управлять кибервойной в режиме реального времени в крупных масштабах и в динамичных сетевых инфраструктурах. Предполагается создание фундаментальных стратегий и тактик, необходимых для доминирования на поле битвы в киберпространстве. Результатом программы станет удобный и интуитивно понятный интерфейс для управления боевыми действиями в киберпространстве [234].

4.10.9.3. Технологии радиоэлектронной борьбы

Разработка технологий радиочастотного картирования местности на поле боя – *программа Advanced RF Mapping*. Целью программы является возможность эффективного распределения электромагнитного диапазона и управление его использованием для обеспечения надежного функционирования систем связи и разведки, одновременно с подавлением и картированием таких же систем противника. В рамках данной программы планируется разработка системы комплексирования информации о состоянии и использовании электромагнитного диапазона, собираемой от совокупности распределенных сенсорных и вычислительных блоков, а также формирование рекоменда-

ций по используемым частотам для конкретных средств связи и разведки [234].

Разработка программных алгоритмов и методов адаптивной РЭБ *– программа BLADE* (*Behavioral Learning for Adaptive Electronic Warfare*). Несовершенство существующего подхода к разработке новых методов и средств РЭБ проявляется в том, что их разработка производится, как правило, в лабораторных условиях. Однако в течение некоторого времени после разработки и оценки их эффективности войска США оказываются уязвимыми перед новыми методами подавления. Кроме значительных затрат времени на разработку, методы РЭБ сегодня предназначены только для конкретного вида радиосигнала или радиосредства с известными характеристиками и, следовательно, являются неэффективными против адаптивных устройств радиосвязи. В качестве решения данной проблемы западные эксперты предлагают изменить подход к выработке эффективных мер РЭБ и перейти от лабораторной разработки методов подавления к адаптивному подходу в полевых условиях. В ходе реализации программы BLADE должна быть разработана сетевая система РЭБ, способная автоматически как подавлять средства и направления радиосвязи противника, так и формировать и реализовывать меры радиоэлектронной защиты для своих систем радиосвязи в полевых условиях [234].

Создание адаптивного средства постановки радиопомех *– программа ARC* (*Adaptive Radar Countermeasures*). Программа ARC предусматривает создание средств эффективного противодействия РЛС противника, работающим в адаптивном режиме, для повышения живучести собственных боевых авиационных средств. Разрабатываемые алгоритмы должны быстро обнаруживать и анализировать структуру сигналов, которые ранее не были известны и не содержатся в базе данных существующих систем РЭП, самостоятельно синтезировать помеховый сигнал и выдавать его в эфир в течение тактически оправданного интервала времени [234].

4.10.9.4. Технологии информационного противоборства в социально-психологической сфере

Проведение графо-теоретических исследований алгоритмов эффективного представления архитектуры социальных сетей *– программа GRAPHS* (*Graph-theoretical Research in Algorithm Performance & Hardware for Social networks*). Последние события в мире доказывают, что анализ социальных сетей может иметь критическое зна-

чение для безопасности государства. В настоящее время методы анализа социальных сетей находятся в начальном состоянии, когда реальные сети представлены в виде грубых и недостаточно адекватных графовых моделей. Данная программа ориентирована на разработку научного аппарата для математической формализации архитектуры социальных сетей. Это позволит более точно описать социальные сети, а также их изменения в пространстве и во времени [234].

Исследование процессов распространения информации в социальных сетях *– программа SMISC* (*Social Media in Strategic Communication*). Программа направлена на разработку алгоритмов выявления, отслеживания, формирования, развития и распространения идей, понятий и «мемов» в социальных сетях. В дальнейшем это позволит самостоятельно инициировать сообщения и дезинформацию в целях проведения информационных операций в социальных сетях с учетом особенностей конкретного социума, региона и интересов США. Программа исследует [234]:

- распространение сообщений в социальных сетях;
- распознавание структур пропагандистских кампаний и информационных операций на сайтах и в социальных сообществах;
- идентификацию участников кампаний, их ролей и истинных намерений;
- измерение эффективности компаний;
- противодействие враждебным кампаниям с помощью контрсообщений.

Разработка технологий выявления аномалий поведения *– программа ADAMS* (*Anomaly Detection at Multiple Scales*). Программа ADAMS разрабатывает приложения, предназначенные для выявления аномальных процессов, происходящих в обществе, наблюдения за неадекватным поведением отдельных индивидуумов и групп людей [234].

4.10.10. Оружие на новых физических и других принципах

Создание лазерного оружия воздушного базирования *– программа Endurance.* Программа Endurance направлена на создание технологии лазеров, размещаемых на БПЛА, которые смогут эффективно защищать большое количество военных воздушных платформ от управляемого вооружения класса «земля-воздух», обладающего опти-

ко-электронной системой наведения на цель на основе ИК-датчиков. Ключевой идеей программы является миниатюризация технологий всех компонентов лазера, создание новых систем высокоточного слежения за целью, ее идентификации, а также гибкой и легкой системы управления лучом лазера [234].

Разработка технологии перспективных волоконных лазеров для получения пучка излучения высокого качества *– программа SFANPBQ* (*Scaling Fiber Arrays at Near Perfect Beam Quality*). Программа FLASH нацелена на демонстрацию потенциальных возможностей набора легких высокомощных волоконных лазеров, способных генерировать пучок излучения высокого качества мощностью до 100 кВт. Особенностью волоконных лазеров является высокая электрооптическая эффективность, что позволяет использовать их в том числе для задач создания перспективных образцов высокоэнергетического лазерного оружия. Для достижения целей программы планируются [234]:

- значительное уменьшение массогабаритных параметров мощных волоконных лазеров при попутном увеличении их прочности в соответствии с тактической долгосрочной концепцией интеграции с воздушными судами;
- разработка и демонстрация потенциальных возможностей легких высокомощных фазированных лазерных решеток;
- интеграция технологий для компенсации атмосферной турбулентности при формировании и распространении луча.

Создание высокоэнергетических лазерных систем военного назначения *– программа HELLADS* (*High Energy Liquid Laser Area Defense System*). Программа HELLADS предусматривает разработку 150 кВт боевой лазерной системы, которая должна быть в гораздо легче и меньше, чем существующие лазерные системы такой же мощности, и обеспечивать возможность установки ее на борт воздушных судов тактического назначения для обнаружения пусков зенитных ракет и их поражения в полете лазерным лучом. При этом предполагается, что значительный прогресс в разработке микроэлектроники, систем накачки и охлаждения, оптики, новых металлических сплавов для монтажной части позволит сократить вес и объем системы без снижения мощности излучения [234].

4.10.11. Технологии транспортировки и транспорта

Разработка экспериментального наземного транспортного средства *– программа GXV* (*Ground Experimental Vehicle*). Программа GXV предусматривает повышение эффективности нового поколения наземных транспортных средств военного и специального назначения (в том числе создаваемых на основе транспортных платформ, разработанных с использованием инструментария и универсального языка высокоуровнего проектирования сложных киберфизических систем на основе иерархических графовых моделей и методов анализа иерархий в рамках проекта META). Исследования будут сосредоточены на фундаментальном увеличении показателей выживаемости экипажа и самого транспортного средства. Предусматривается разработка новых методов системной инженерии и проектирования с использованием подходов коллективного интеллекта наряду с автоматизацией функций человека-оператора и обоснованием путей повышения тактико-технических характеристик. Ключевым элементом реализации программы станет разработка гибкой адаптивной платформы, которая позволит достичь снижения массогабаритных размеров, сокращения численности операторского состава, повышения надежности контуров управления человеко-машинных систем и повышения их боевых характеристик [234].

Создание глубоководных всплывающих хранилищ *– программа UFP* (*Upward Falling Payloads*). Скрытому выполнению боевых операций часто мешают демаскирующие действия по доставке боевых грузов и топлива в район операции. Программа UFP предусматривает разработку специального мобильного подводного хранилища. Подводные капсулы должны иметь средства защиты от гидролокационных и радиолокационных средств разведки, кроме того, они должны иметь специальную защиту от преднамеренного механического повреждения. Помимо задач хранения полезной нагрузки такие хранилища могут выполнять и навигационные функции. Бункеры должны быть способны хранить свое содержимое в полной безопасности на протяжении нескольких лет и по первой же команде, поднимать свое содержимое на поверхность [234].

Разработка новых логистических технологий *– программа Petrel*. Программа предусматривает исследования и разработку передовых инструментов быстрого перемещения большого количества военных грузов и оборудования. Такие решения могут быть использованы, например, при переброске бронетанковой бригадной боевой груп-

пы из континентальной части США в район ТВД. Задачей программы является сокращение сроков развертывания механизированных частей сухопутных войск и обеспечение экстренной транспортировки особо важных предметов снабжения в любую точку мира за срок менее семи дней по цене, сопоставимой или чуть выше стоимости обычных морских перевозок. Программа призвана заполнить нишу между обычными воздушными и морскими перевозками за счет разработки нового вида транспортного средства, способного развивать высокую скорость как на воде, так и на суше. Технические подходы к обеспечению быстрой транспортировки по океану либо от судна к ТВД подразумевают использование традиционных и нетрадиционных, аэродинамических и гидродинамических концепций, а также инновационных приложений существующих технологий (например, экранопланы или дирижабли) [234].

4.10.12. Технологии новых материалов и биотехнологии

Разработка гибридного ротора из многокомпонентных материалов *– программа HyDem* (*Hybrid Multi Material Rotor Full Scale Demonstration*). Программа HyDem предусматривает разработку концепции цифрового производства с использованием аддитивных технологий направленных на существенное улучшение и достижение принципиально новых свойств функциональных изделий военного назначения за счет использования многокомпонентных материалов с заданными свойствами. В рамках программы планируется создание опытного образца гибридного ротора для подводных лодок класса Virginia и испытания его новых функциональных узлов и элементов в условиях, приближенных к реальному бою.

Разработка наноматериалов и материалов на основе биотехнологий, а также метаматериалов *– программа Nanoscale/Bio-inspired and MetaMaterials*. Программа предусматривает разработку научной базы для разработки материалов с особыми свойствами, например, с использованием компьютерных методов моделирования, на микро- и нано- уровне, в том числе метаматериалов, цифровых материалов, биотехнологических материалов для новых сенсоров и устройств подачи сигналов, а также материалов, предназначенных для имитации функций биологических материалов от молекулярного до макроскопического масштаба. Применение созданных материалов планируется для создания самовосстанавливающихся материалов, ин-

теллектуальных материалов, материалов для защиты от химического и бактериологического оружия, а также материалов с электростатическим зарядом.

Исследование наноразмерных и непредвиденных эффектов нанодиапазона и создания соответствующих инженерных устройств – *программа FNEEED* (*Fundamentals of Nanoscale and Emergent Effects and Engineered Devices*). Программа FNEEED направлена на изучение и понимание физических свойств и инженерных эффектов наномасштаба. Полученные результаты будут использованы при создании управляемых фотонных многочастотных приборов, сверхвысокочастотных магнитных датчиков, высокопроизводительных биохимических датчиков, известных и искусственно синтезированных молекул, ультра фильтрационных водовоздушных систем очистки, а также физических средств защиты на основе усовершенствованной брони. Примерами рассматриваемых в программе физических эффектов являются термодинамика абсорбции в металлогидридных системах, эффекты коррелированных электронных систем – например, сверхпроводимость и магнетизм. В настоящее время программа FNEEED направлена на разработку методов стабилизации кристаллических структур в ранее недостижимых областях высокого давления. Результаты программы могут быть использованы для создания экономически обоснованных производственных подходов к повышению твердости брони на основе применения фазы высокого давления вещества.

Формирование научного задела в области путей создания «живых фабрик» – *программа Living Foundries*. Фундаментальные исследования в области биоинформационной обработки данных для ускорения циклов проектирования генно-инженерных организмов. Программа предусматривает создание методов проектирования метаболических путей синтеза сложных биологических молекул и функции управления экспрессией (в клетках бактерий и дрожжей). Прикладные исследования по программе выполняются в рамках направления «технологии материалов и биотехнологии».

5. Примеры использования элементов сетецентрических войн в военных конфликтах последних десятилетий

Наиболее явно характер войн нового поколения с организацией военного управления на сетецентрических принципах проявился в ходе вооруженных конфликтов в Югославии, Ираке, Афганистане, Ливии, проводимых США, НАТО и их союзниками в период с конца XX по начало XXI веков. При этом ограниченным составом сил и средств, преимущественно авиацией и силами специальных операций, в очень сжатые сроки достигались ощутимые геостратегические цели. Это связано не только с применением новейших высокотехнологических систем вооружения, но и с достаточно глубокой проработкой вопросов теории современной сетецентрической войны в научном и практическом планах [10, 29].

В настоящее время ведется проработка вопросов применения концепции сетецентрической войны в геополитике. Свидетельством тому являются цветные революции в Сербии, Грузии и Украине, где разнородные информационные стратегии с использованием разрозненных неправительственных, часто молодежных, организаций и фонды смогли привести ситуацию к желательному политическому результату без прямого военного вмешательства. Таким образом, цель – подчинение своим интересам условно «независимых» государств, как основная задача войны - была эффективно достигнута сетевыми методами.

Рассмотрим основные особенности войн 6-го поколения с организацией военного управления на сетецентрических принципах на примере локальных войн и военных конфликтов конца XX – начала XXI веков.

5.1. Общие тенденции применения элементов сетецентрических войн в военных конфликтах начала XXI века

Анализ локальных войн рубежа XX–XXI вв. показывает, что вооруженное противоборство вступило в новую стадию сетецентрических войн, и государства, не подготовленные к ведению войны нового поколения, обречены на поражение, так как для противостояния массированному удару высокоточных воздушно-космических средств

надо иметь совершенно другие вооруженные силы. Они должны создаваться не на базе крупных сухопутных группировок войск, а, прежде всего, на базе эффективной стратегической системы воздушно-космической обороны, способной отражать длительные массированные удары высокоточных средств противника и на базе достаточного количества собственных высокоточных средств поражения различной дальности действия, а также средств на новых физических принципах, действующих в соответствии с законами войны нового поколения [163, 165].

По итогам анализа применения элементов сетецентрических войн в конфликтах рубежа XX–XXI вв. можно сделать следующие выводы, обобщенные в работе [315].

Достижения информационно-технической революции в военной сфере значительно расширили границы взаимодействия раздельно наступающих групп войск в операции – вся информация о положении дел стала доступна практически всем активным участникам вооруженной борьбы. Взаимодействие стало организовываться не путем объединения в решающих пунктах раздельных групп войск, а путем объединения их огневых и информационных возможностей. Это позволило впервые в истории военного искусства преодолеть пространственный, временной и информационный разрыв между войсками и органами управления. Новые информационные технологии обеспечивают устойчивое управление и постоянное взаимодействие пространственно разделенных тактических группировок войск, поддерживающих между собой связь и координирующих свои действия в интересах проведения совместных операций. Данное обстоятельство изменяет характер современных операций: все процессы управления и сами боевые действия становятся более динамичными, активными и результативными, исчезают тактические и оперативные паузы, которыми противник мог бы воспользоваться [315].

Операции получают новое содержание, изначально предполагающее проведение быстрых и решительных маневров не только на флангах, но и в глубоком тылу противника. При этом, как свидетельствует опыт военных конфликтов, такие действия могут вестись в форме центрально-сетевых операций разновидовых тактических группировок, управляемых из единого стратегического центра и одновременно действующих по отдельным ключевым элементам системы государственного и военного управления, частям и подразделениям «сил ответного удара (возмездия)» на всей территории противоборствующей стороны [315].

Основным фактором, определяющим характер современных операций, является не соотношение пространства и численности вооруженных сил, а наличие новых межвидовых мобильных соединений и частей, реализующих свои потенциальные возможности на основе сетецентрических методов разведки, управления и обеспечения. Существующий с давних времен принцип сосредоточения сил и средств на решающем направлении трансформируется в принцип сосредоточения усилий, реализуемый не методом сосредоточения войск (сил) на избранном направлении, а, главным образом, путем массированного и согласованного применения средств дальнего огневого, радиоэлектронного и информационного поражения.

Командиру каждой из относительно автономных группировок (групп) нет необходимости иметь в непосредственном подчинении какие-то конкретные специфические дорогостоящие системы вооружения – ему лишь необходимо сделать через сеть заявку на их применение в заданном районе в заданное время для решения конкретной задачи или довести текущую обстановку до вышестоящего командира, который, владея большей информацией, может принять более корректное решение с привлечением более разнообразных и наиболее соответствующих складывающейся обстановке средств вооруженной борьбы [315].

Основная задача сетецентрических операций – с первых минут войны захватить стратегическую инициативу переносом боевых действий в стратегическую глубину обороняющихся войск и не дать возможности обороняющейся стороне осуществить не только стратегическое, но и оперативное развертывание своих группировок вооруженных сил. В целом сетецентрические операции могут иметь преимущественно региональный масштаб, отличаться скоротечностью, избирательностью и значительной степенью поражения высокоточными средствами, быстротой маневра войсками (силами) и огнем, применением различных десантов, а также сил специальных операций и диверсионных групп. Огневые и электронные удары по объектам будут наноситься по всей глубине территории противника. Массированное применение высокоточных крылатых ракет в сетецентрических войнах будет осуществляться одновременно с нескольких стратегических воздушно-космических направлений, т.е. без сосредоточения основных усилий на одном направлении, что создаст исключительно сложную воздушно-космическую обстановку в зоне ответственности ПВО обороняющейся стороны. Здесь стоит отметить, что понятия «воздушное направление», «стратегическое воздушно-космическое направле-

ние» вследствие значительного повышения оперативных и боевых возможностей авиационно-ракетных группировок войск (сил) теряют свой смысл, так как разрывается существовавшая до 90-х гг. XX столетия жесткая связь между районами базирования авиации и направлениями (районами) их применения [315].

В то же время роль ВВС в реализации концепции сетецентрических войн значительно возрастает, так как боевая авиация благодаря своей мобильности и универсальности боевых возможностей нередко является единственным средством, способным своевременно отреагировать на критичную по времени угрозу и ликвидировать ее. Кроме того, решающее превосходство в области информационного противоборства можно обеспечить только на основе широкого применения средств разведки, систем наблюдения, управления и РЭБ воздушного и космического базирования [315].

Анализ наиболее крупных локальных войн и военных конфликтов, происходивших после в конце XX – начале XXI века, показал, что в последнее десятилетие взгляды на их цели и формы, а также способы применения в них вооруженных сил претерпели значительные изменения. Наиболее общими и основными из них, в соответствии с работами [269, 328], являются следующие:

1. Локальные войны и военные конфликты превратились из второстепенных действий, проводимых в интересах подготовки условий (плацдарма) для крупномасштабной войны, в самостоятельное действие с более конкретным перечнем конечных (частных) военно-политических целей и в настоящее время являются основным классом войн в современном мире.

2. В современных военных конфликтах в связи с совершенствованием высокоточных средств поражения противоборствующие стороны стремятся не просто решить основные задачи, достичь решительного перелома в ходе проведения первых операций, но и разрешить возникший конфликт в целом (принудить противника к миру), причем главенствующая роль отводится воздушно-морской операции и подрыву военно-экономического потенциала. Это приводит, во-первых, к определяющему значению первых операций для всего военного конфликта, а во-вторых – к увеличению значимости первых массированных ударов, повышению роли авиации и ракетных войск в них. При этом предполагается нанести основной урон как группировке противника, так и его военно-экономическому потенциалу с целью немедленного принуждения его к миру на выгодных условиях. Это требует четкого отслеживания органами разведки всех этапов разви-

тия конфликта, деятельности в них противника, в первую очередь средств огневого (ядерного) поражения и своевременного нанесения по нему превентивного удара.

3. Следствием из п. 2 является изменение самого характера вооруженной борьбы как столкновений вооруженных группировок на линии фронта. В современных условиях боевые действия все чаще ведутся без четко обозначенной линии фронта и характеризуются высокой воздушно-наземной маневренностью, тактической и огневой самостоятельностью соединений, частей и подразделений. Это приводит к необходимости непрерывного отслеживания группировки войск (сил) противника на всех этапах развития военного конфликта на всю глубину его территории и территории союзников, налагает более жесткие требования на своевременность разведывательного обеспечения и оперативность реагирования группировки войск на складывающуюся ситуацию.

4. В условиях войны, когда отсутствует четкий фронт и тыл, на первый план выдвигаются вопросы: планирования и ведения вооруженной борьбы с иррегулярными формированиями; обеспечения эффективных действий войск в условиях ограничений пространственных, временных на применение определенных видов средств поражения и т. д.; изучения не рассматривавшихся ранее участков территории как районов боевых действий, источников мобилизационных резервов противника.

5. В конфликтах резко возросла роль всех основных фаз (этапов) их развития и их влияние на результаты разрешения конфликта в целом. Это обусловлено появлением реальной возможности у военно-политического руководства стран разрешать конфликты не только на конечных фазах, но и в ходе любой из фаз (зарождение, обострение, кризис, разрешение кризиса, восстановление мира) их развития. Она основана на непрерывном, целенаправленном и адекватном реагировании не только вооруженных сил, но и на активном воздействии на складывающуюся военно-политическую обстановку информационными, экономическими и дипломатическими методами. Высокая интенсивность развития современных конфликтов, с одной стороны, и длительное время подготовки и создания соответствующей группировки войск, с другой, накладывают жесткие требования на временные характеристики периодов выработки политических решений. Как правило, современным конфликтам предшествуют информационные операции, направленные на дестабилизацию органов военного и государ-

ственного управления противника и создание положительного имиджа своих вооруженных сил.

6. Современные конфликты характеризуются высокой неопределенностью прогнозируемого состояния оперативно-стратегической (оперативной) обстановки на каждой фазе и разнонаправленностью ее дальнейшего развития. Как следствие, возникает высокая неопределенность характера предстоящих действий, что затрудняет процесс планирования как операций, так и мероприятий их обеспечения. Предполагается, что участвующие в боевых действиях группировки войск будут строиться в соответствии с концепцией сетецентрических войн. При этом необходимо учесть имеющейся опыт создания сил оперативного реагирования в виде так называемых целевых или объединенных оперативных формирований, «адаптированных» к конкретным условиям кризисной обстановки, т. е. находящихся в высокой степени боевой готовности контингентов войск из различных видов ВС, сведенных в одну «команду» и подготовленных для решения широкого круга задач в любом регионе мира.

Анализ конкретных военных конфликтов, в которых принимали участие вооруженные силы США и стран НАТО и в которых использовались элементы сетецентрической войны, позволил установить следующие закономерности их развития. При этом необходимо отметить, что данные конфликты носят ярко выраженный асимметричный характер – применение силы более сильного противника к более слабым.

В ходе своей повседневной деятельности государства и их вооруженные силы развертывают разветвленные системы информационного обеспечения и мониторинга (преимущественно в космическом и информационном пространствах), а также обеспечивают передовое присутствие своих вооруженных сил в местах проекции силы и потенциальных конфликтов. В этот же период производится накопление запасов дорогостоящего высокоточного оружия дальнего действия и наращивание современных видов ВВТ в количествах, достаточных для ведения крупномасштабной войны.

На начальных этапах конфликта (зарождение, обострение) для достижения военно-политических целей на первый план выдвигаются информационные, дипломатические и экономические формы воздействия на противника. Экономические ограничения: введение санкций, запрет на движения капитала, ограничения на передачу критических технологий и материалов – зачастую не позволяют противнику в необходимой степени производить современные виды ВВТ, снижают уро-

вень жизни населения и формируют благоприятную атмосферу по проведению информационных операций, направленных на дестабилизацию обстановки в стране-противнике. Дипломатические усилия в этот период направлены на отсечение от противника потенциальных союзников, поддержку оппозиционных внутренних сил, обеспечение будущей военной операции, легитимный характер и формальное международно-правовое прикрытие. Информационно-психологические операции, проводимые в этот период, имеют целью нанести заблаговременное психологическое воздействие на потенциального противника в интересах формирования элит с заданным мировоззрением, привития населению определенных ценностей и стереотипов, позволяющих, с одной стороны, прогнозировать его поведение и играть на внутренних противоречиях, а с другой – влиять на процессы принятия решений на всех уровнях управления. Информационно-технические операции имеют целью мониторинг и вскрытие потенциальных точек воздействия как на лиц, принимающих решения (служебные и личные телефоны, электронные адреса), так и на критическую инфраструктуру противника (телекоммуникационные и энергетические системы, объекты промышленности и производства ВВТ, транспорт, системы государственного и военного управления).

На следующих этапах конфликта (обострения, кризиса) производится наращивание военного присутствия в местах потенциального конфликта, преимущественно за счет увеличения численности сил и средств ВВС и ВМС. При этом, особенностью конфликтов рубежа XX–XXI вв. является незавершенность процесса стратегического развертывания и создания полномасштабных группировок ВМС и ВВС к началу военных акций. Это объясняет стремление активной стороны в максимальной степени добиться внезапности нападения путем реализации возросших ударных возможностей сил передового присутствия. Кроме того, наращивание боевого и численного состава группировок до уровня, предусмотренного планом проведения операций, происходит уже в ходе боевых действий. Наращиваются возможности космической и воздушной разведок в местах конфликта, ведется активная радио- и оптоэлектронная разведка дислокации сил и средств противника, в особенности систем ПВО, а также объектов критической инфраструктуры. Одновременно ведется создание и поддержка оппозиционных сил в стране-противнике, создание вооруженного ядра оппозиции, основу которого составляют силы специальных операций активной стороны.

Проводятся информационно-психологические операции по дискредитации государственных институтов власти в глазах населения, а также по дезорганизации личного состава вооруженных сил и подавлению их воли к сопротивлению. Через сеть Интернет ведется координация акций гражданского неповиновения, выступления маргинальных и недовольных групп населения. Ведется подкуп и шантаж влиятельных лиц государственного и военного управления с целью обеспечить их невмешательство в ситуацию под гарантии личной и финансовой безопасности. Ведется активная информационная операция в мировых СМИ по дискредитации противника в глазах мировой общественности и подготовки благоприятной атмосферы для принятия решений о начале военной операции против противника. Производится сосредоточение дипломатических усилий на получение формального международного одобрения по разрешению кризиса военным способом.

Активная фаза кризиса, когда он перерастает в вооруженный конфликт, как правило, связана с нанесения комплексного удара высокоточными средствами поражения морского и авиационного базирования по разведанным и хорошо изученным объектам критической инфраструктуры на территории противника и, в первую очередь, по средствам ПВО. Удар позволяет минимизировать ответные действия противника и не допустить существенных потерь сил и средств активной стороны. Эффективное использование ВТО обеспечивается космическими средствами разведки и навигации, а коррекция направления ударов и контроль их результатов – применением разведывательных БПЛА.

Одновременно силами кибероперациий и средствами РЭБ проводится радиоэлектронный удар с целью подавления радиолокационных систем ПВО, нарушения функционирования системы государственного и военного управления, подавления средств радио- и телевизионного вещания противника, нарушения функционирования телекоммуникационных и энергетических сетей, а также банковских и транспортных систем. Скорее всего, будет отсутствовать четко выраженное направление главного удара, поскольку удары по противнику будут наноситься со всех направлений на всю глубину территории противостоящей стороны.

Результаты оценки конфликтов рубежа XX–XXI вв. показывают, что с появлением в вооруженных силах высокоточного оружия дальнего действия в количествах, достаточных для ведения крупномасштабной войны, разгром противника как одна из важнейших целей

всех войн прошлого может достигаться лишь нанесением массированных ударов ВТО по его объектам стратегического значения. Что касается живой силы противника, то она может не подвергаться огневому воздействию. Удары будут наноситься также по важнейшим объектам государственного управления и экономики. В этих условиях отпадает необходимость оккупировать территорию противника, лишенного экономики, а его политический строй, оказавшийся в международной изоляции в условиях ведения перманентной информационной войны, с высокой долей вероятности развалится самостоятельно.

В ходе последующих этапов вооруженного конфликта для нанесения ударов в условиях уничтожения средств ПВО противника будут активно использоваться авиация и разведывательно-ударные БПЛА. Выбор объектов для поражения будет определяться с учетом конкретных задач, которые определяются исходя из реальной обстановки. Активные сухопутные боевые действия будут вестись в условиях отсутствия четко выраженного фронта и тыла. Группировки будут создаваться в короткие сроки на основе боеготовых воинских формирований, обладающих высоким уровнем стратегической мобильности и способности к ведению автономных действий. При этом сухопутные силы будут задействоваться лишь для окончательного закрепления успеха. Действия сухопутных сил будут проходить в условиях абсолютного радиоэлектронного подавления противника и информационного превосходства над ним. Применение сухопутных сил на тактическом уровне будет вестись с координацией действий с вооруженными формированиями оппозиции и при поддержке их авиацией. В сухопутных тактических операциях будут широко задействованы подразделения сил специальных операций, морской пехоты. В случае необходимости проведения незаконных акций, на которые имеется международный формальный запрет, или в интересах избегания имиджевых потерь для решения тактических задач будут широко привлекаться частные военные компании и наемники, контролируемые спецслужбами активной стороны.

В период боевых действий будут активно вестись информационно-психологические операции, направленные на дезорганизацию личного состава вооруженных сил противника, формирование позитивного имиджа активной стороны среди населения страны-противника, а также финансовые операции, направленные на подкуп и склонение к измене высших государственных и военных должностных лиц.

Таким образом, основным содержанием современных и будущих сетецентрических войн могут стать совместные наземно-морские и воздушно-космические сетецентрические операции, представляющие собой зону многочисленных сражений, боев и ударов, проводимых рассредоточенными по всему пространству ТВД взаимосвязанными и взаимозависимыми тактическими группировками войск (сил). При этом наличие единой информационно-управляющей среды позволяет рассматривать совокупность таких группировок как группировку оперативно-стратегического или стратегического масштаба. Количество сил, развернутых (базирующихся, дислоцирующихся) в конкретном объеме пространства, будет не столь существенно, чем возможность своевременного наращивания ими усилий в любом районе боевых действий. Кроме того, разбросанность главных группировок наряду с быстротой действий аэромобильных сил позволит в реальном масштабе времени осуществлять изменение направления и вводить командование противостоящей стороны в заблуждение как о своих текущих намерениях, так и об общей оперативной обстановке.

5.2. Операция НАТО «Решительная сила» против Югославии (1999 г.)

Война стран НАТО на Балканах против Югославии была первой коалиционной войной в Европе после второй мировой войны. Рассмотрим особенности данного военного конфликта на основе анализа работ [2, 29, 95, 163, 171, 173, 174, 269, 301, 302].

Анализ действий боевой авиации и применения крылатых ракет в ходе операций НАТО свидетельствует о том, что в Югославии впервые получили применение формы и способы сетецентрической войны, отдельные элементы которой ранее были опробованы в войне в Персидском заливе (1991-1992 гг.), в Боснии и Герцеговине (1994-1995 гг.), а также в ходе операции «Лиса в пустыне» против Ирака (декабрь 1998 г.) [174].

Для выполнения поставленных задач командование НАТО создало авиационную и морскую группировки в составе свыше 950 самолетов, из них около 480 боевых и 30 разведчиков, 3 авианосца и около 50 других боевых кораблей. За период проведения воздушной операции удары наносились более чем по 30 городам и населенным пунктам Югославии. Всего ударам подверглись свыше 400 объектов, из них около 60% военных и до 40% гражданских объектов. В дальнейшем в ходе второго и третьего месяцев военных действий, перейдя

к массированным бомбардировкам всего спектра целей на территории Югославии, имея подавляющее преимущество в воздухе и последовательно наращивая состав авиационной группировки, командование НАТО перешло к планомерному уничтожению ее военно-экономического потенциала [174].

Важнейшей (если не главной) целью войны в Югославии для США и их союзников были всесторонние испытания в реальных боевых условиях новых высокоточных систем оружия, систем разведки, управления, связи, навигации, РЭБ, всех видов обеспечения, а также взаимодействия различных сил и средств. Полученная статистика позволила внести соответствующие уточнения и изменения в нормативные и уставные документы систем оружия и вооруженных сил [173].

К концу первого периода операции главные цели (экспериментально-испытательные) были достигнуты и военное командование США и НАТО поставило новые задачи, для решения которых понадобился еще один этап [173].

Второй период воздушно-космическо-морской ударной операции характеризовался следующими особенностями. После завершения основных программ натурных экспериментов по применению новых видов беспилотного высокоточного оружия и в результате практически полного подавления системы ПВО Сербии и Косово начался пилотируемый вариант воздушно-космическо-морской ударной операции. В этот период США и другие страны НАТО фактически «возвратились» в предыдущее поколение войн. Правда, следует отметить, что пилотируемая авиация выполняла некоторые задачи над территорией Югославии и в первый период операции. Это были эпизодические миссии, связанные с проверкой возможности использования ударной авиации, разработанной по технологии Stealth, с экспериментальной отработкой методов борьбы с достаточно сильной ПВО Югославии, построенной на основе активной радиолокации, а также с проверкой эффективности применения новых видов высокоточных бомб, сбрасываемых с большой высоты [173].

На территории Югославии боевые действия сухопутных группировок войск союзом НАТО не планировались и не велись. Воздушно-космическо-морская ударная операция проведена полностью бесконтактным способом в горно-лесистом Балканском театре военных действий с достаточно развитыми экономикой, инфраструктурой и ПВО Югославии [95, 173, 174].

Перечень объектов для поражения составлялся заранее в соответствии с концепцией «пяти колец Дж. Вардена», которая рассматри-

вает противника в качестве системы, состоящей из пяти радиальных колец. В центре – политическое руководство, затем следуют система жизнеобеспечения, инфраструктура, население и лишь в последнюю очередь – вооруженные силы.

При этом основные усилия по применению систем высокоточного оружия США и НАТО в этой фактически бесконтактной войне были направлены не на уничтожение живой силы и вооружения югославской армии, а на разрушение ключевых военных и экономических объектов, инфраструктуры и коммуникаций Сербии и Косово. В подавляющем большинстве случаев эти объекты были успешно поражены. Это обстоятельство является одной из важнейших характеристик образа войны нового поколения. Поскольку операция носила лишь экспериментальный, испытательный характер, то задача полного достижения стратегических и политических целей не ставилась. Именно поэтому полная победа не была достигнута [95, 173].

Следует подчеркнуть, что в ходе воздушно-космическо-морской ударной операции плановые удары по войскам Югославии не наносились. Отчасти это объясняется тем, что Югославия оказалась неготовой к ведению боевых действий в соответствии с формами и способами войн нового поколения. Вооруженные силы Югославии не только не представляли угрозы для сил НАТО, но и были просто не в состоянии препятствовать войскам альянса в их боевой работе. Удары по Югославии осуществлялись скорее попутно, при выполнении других задач [173].

Следует отметить, что на протяжении всего первого периода операции метеорологические условия в целом не благоприятствовали применению пилотируемых средств над территорией Югославии. Однако туманы, дожди и плотная низкая облачность мало сказывались на действиях авиации, поскольку та лишь доставляла до рубежей пуска высокоточные крылатые ракеты, которые и были главным оружием первого периода операции. Для объективной оценки эффективности боевого применения экспериментальных крылатых ракет плохая погода была даже более предпочтительной [173, 174].

По утверждению некоторых средств массовой информации в ходе ударов югославские ВС потеряли более 10 тыс. военнослужащих убитыми, 314 артиллерийских орудий и 120 танков. На пресс-конференции в Пентагоне 1 июля 1999 г. главнокомандующий войсками НАТО в Европе генерал У. Кларк доложил, что в ходе 78-суточной операции на территории Косово уничтожено 110 сербских танков и 210 боевых машин пехоты (БМП). Осенью 1999 г.

У. Кларк назвал уже другие цифры: уничтожено 93 сербских танка и 153 БМП. В действительности специально направленная команда НАТО обнаружила на территории Косова 60 единиц уничтоженной бронетехники и артиллерии. Отсутствие достоверной информации о потерях Югославии свидетельствует о плохо налаженном документировании результатов ударов. Уровень и порядок потерь югославских вооруженных сил позволяет сделать совершенно иные выводы. Абсолютно достоверно известно, что до начала войны у сербов имелось 1025 танков и 3750 артиллерийских орудий. Значит, в ходе всей войны силами НАТО попутно уничтожено менее 10% танков и орудий. Это полностью подтверждает первоначальную гипотезу о том, что плановые удары по войскам не наносились [173, 174].

Надо отметить, что российские и зарубежные СМИ неоднократно критически оценивали результативность действий НАТО именно в связи с неспособностью альянса нанести решительное поражение вооруженным силам Югославии. Однако еще раз повторим, что такая цель и не преследовалась. Главной задачей альянса являлось разрушение экономической инфраструктуры страны и системы ее государственного и военного управления [173].

5.2.1. Использование разведывательно-ударной боевой системы как основы для проведения бесконтактной операции

Удары по военным и экономическим объектам Сербии и Косово в ходе новой в военном искусстве воздушно-космическо-морской операции наносились не группировками ВВС и ВМС, которые там формально существовали, а специально созданными на их базе разведывательно-ударными боевыми системами (РУБС). Основой РУБС являлись космические системы информационного обеспечения, а также воздушные и морские носители высокоточного оружия. Самолеты ВВС и ВМС США и других стран НАТО действовали как элементы РУБС, доставляя до рубежей пуска высокоточные крылатые ракеты, нацеленные на конкретные критические объекты военного и промышленного значения, и находясь при этом за пределами досягаемости средств ПВО Югославии. В условиях односторонних ударов НАТО по объектам экономики Югославии высокоточными крылатыми ракетами вооруженные силы Югославии оказались неспособными противодействовать противнику [95, 173, 174].

5.2.2. Использование высокоточного оружия как основного средства поражения

Самолеты ВВС и ВМС США и других стран НАТО взлетали с авиабаз на территории США, стран НАТО в Европе и авианосцев в Адриатическом море и, не входя в зону действия югославских ПВО, доставляли до рубежей пуска высокоточные крылатые ракеты, нацеленные на конкретные критические точки военных и промышленных объектов. Запуск ракет производился с высоты 8-9 тыс. м, после чего самолеты уходили за новыми боекомплектами или возвращались на авиабазы США [173, 174].

Крылатые ракеты морского базирования запускались с кораблей и подводных лодок ВМС США, которые находились в Адриатическом море и также входили в разведывательно-ударные боевые системы. Крылатые ракеты воздушного и морского базирования поражали цели на дальностях 300-800 км от рубежей пусков [95, 174].

В течение первых шести недель операции были испытаны новейшие крылатые ракеты воздушного базирования, хотя в целях дезинформации они проходили под известным старым шифром AGM-86 с добавлением определенных индексов. В этот же период были испытаны также новые крылатые ракеты морского базирования AGM-109, носителями которых были корабли и подводные лодки ВМС США. Эти ракеты наводились на цели с использованием космической навигационной системы GPS, весь полет этих крылатых ракет осуществлялся без электромагнитного излучения для измерения высоты своего полета. На конечном участке полета, непосредственно в районе цели, для точного наведения на конкретную критическую точку объекта активировалась оптическая система DSMAS [174].

Были испытаны также новые модификации управляемой крылатой ракеты AGM-130 с телевизионной командной системой наведения (носитель – самолет F-15E). В конце первого периода войны были отмечены испытания и кассетных авиабомб CBU-97 с самоприцеливающимися боевыми элементами для поражения бронетанковой техники (носитель – стратегический бомбардировщик B-1B) [174]. В ходе второго периода операции США впервые были испытаны на точность поражения новые управляемые авиабомбы JDAM, JSOW, WCMD, которые специально сбрасывались с высоты более 23 тыс. м (носитель – стратегический бомбардировщик B-2A) с наведением по сигналам космической навигационной системы NAVSTAR [173].

Вместе с тем, во втором периоде главным оружием операции стали обычные неуправляемые авиабомбы. Это можно объяснить только тем, что США и другие страны НАТО использовали второй период операции для того, чтобы избавиться от излишков оружия прошлого поколения войн. Они в больших количествах утилизировали старые авиабомбы, разрешая недостаточно подготовленным летчикам сбрасывать их там, где те считали нужным. Этим также объясняются многочисленные промахи, поражения гражданских объектов и обстрелы колонн беженцев. Необходимость утилизации старых боеприпасов послужила одним из факторов затягивания военных действий [173].

Система ПВО Югославии была создана, как и в большинстве других стран, на базе активной радиолокации для борьбы именно с пилотируемой авиацией над собственной территорией. Для решения данных задач эта ПВО была достаточно эффективной, однако подобная система, будучи адекватной войнам прошлого поколения, оказалась совершенно беспомощной в борьбе с массированными налетами высокоточных крылатых ракет противника, действовавших на предельно малых высотах в условиях географически сложной, покрытой лесной растительностью местности с горными хребтами, вершинами, ущельями и оврагами. Зенитная артиллерия Югославии практически не оказала положительного влияния на отражение массированных налетов крылатых ракет, хотя несколько десятков крылатых ракет из более тысячи примененных все же были сбиты этими средствами. При этом зенитная артиллерия не являлась первоочередным объектом нападения сил НАТО [173].

По официальным данным Пентагона для нанесения ударов по 900 объектам экономики было использовано 1,2-1,5 тыс. высокоточных крылатых ракет, большинство из которых являлись экспериментальными. В ходе первого периода операции только высокоточными крылатыми ракетами воздушного и морского базирования была полностью (100%) разрушена нефтяная промышленность, 50% индустрии боеприпасов, 70% авиационной промышленности, 40% танковой и автомобильной промышленности, 40% нефтехранилищ, 100% мостов через Дунай, 70% автомобильных и железных дорог. Остальные объекты и цели поражались пилотируемыми самолетами в ходе второго периода операции, когда система ПВО Югославии была полностью выведена из строя [95, 163, 171, 173, 174].

5.2.3. Достижение информационного превосходства за счет наращивания средств связи, управления, разведывательного и навигационного обеспечения

Ракетно-бомбовые удары по Югославии в 1999 г. были начальной проверкой в боевых условиях американской глобальной информационной системы управления, создаваемой в интересах ведения сетецентрических войн и предназначенной для централизованного управления в реальном масштабе времени действиями вооруженных сил США как в крупномасштабных войнах, так и в региональных конфликтах. Впервые в ходе агрессии США проверили на практике систему управления военными действиями на глобальном уровне непосредственно из Пентагона, для чего команды об ударах по наиболее важным объектам на территории Сербии и Косово отдавались непосредственно из Вашингтона [95].

Космические средства военного назначения играли в операции не просто чрезвычайно большую и важную роль, но и являлись системообразующими военно-техническими инструментами ведения боевых действий. До начала операции США создали мощную группировку космических средств различного назначения в количестве 50 спутников. Над театром войны одновременно находилось от 8 до 12 космических аппаратов, которые совместно с воздушными и морскими носителями были основой разведывательно-ударных боевых систем. Из космоса велось непрерывное наблюдение за ТВД спутниками оптической разведки КН-1 (США), Helios-1A (Франция), радиолокационной разведки Lacross (США), а также осуществлялись управление, навигация, связь и метеообеспечение. Космические аппараты США системы GPS осуществляли навигацию новейших высокоточных крылатых ракет воздушного и морского базирования. Космические аппараты SPOT (Франция) передавали телевизионное изображение земной поверхности и документировали экспериментальные удары по объектам экономики и инфраструктуры Сербии и Косово с целью определения реальной эффективности высокоточных крылатых ракет [95, 173].

Всего в ходе военных действий на Балканах США и НАТО было использовано около 120 космических аппаратов различного назначения, в том числе 36 спутников связи, 35 разведывательных, 27 навигационных и 19 метеорологических [174].

Впервые активно использовались средства космического навигационного обеспечения на основе спутниковой группировки GPS. Фактически все военнослужащие США в зоне боевых действий имели

приемники GPS, способные точно определить местонахождение бойца в любой точке и в любых условиях. Также в Югославии впервые широко использовались GPS для наведения ВТО независимо от погоды и времени суток [174].

5.2.4. Достижение информационного превосходства за счет массированного использования средств радиоэлектронной борьбы

В ходе воздушно-космическо-морской операции силами НАТО одновременно проводилась операция РЭБ, которая кроме мощного помехового заградительного и прицельного подавления радиоэлектронных средств Югославии государственного и военного назначения включала множество высокоточных огневых ударов по другим радиоизлучающим объектам. Противорадиолокационными ракетами, наводившимися на любые зафиксированные источники излучения электромагнитной энергии, поражались радиолокаторы, зенитные ракетные комплексы, станции радиосвязи, узлы обычной и сотовой связи, телевизионные станции, станции радиовещания и компьютерные центры. Специальными высокоточными ракетами с пылевым графитовым и металлизированным наполнением головных частей поражались трансформаторные подстанции и релейная автоматика электростанций [173].

ПВО Югославии была полностью подавлена средствами радиоэлектронной борьбы, а высокоточными противорадиолокационными ракетами войск НАТО уничтожался практически каждый источник радиоизлучения. Как правило, уже после первого пуска зенитной ракеты даже самый совершенный зенитный ракетный комплекс ПВО Югославии, использующий в своей работе принцип активной радиолокации, был обречен на поражение независимо от того, оставался ли он после этого включенным или выключался. Каждая РЛС, кратковременно излучавшая электромагнитную энергию, непременно поражалась либо противорадиолокационной ракетой, либо ракетой с наведением на тепловое излучение двигателя транспортного средства РЛС или ее силовых агрегатов при выключенном состоянии самой РЛС. Это привело к тому, что в течение первых трех суток войны были выведены из строя 70% дивизионов подвижных ЗРК С-125 и С-75 [173].

По демаскирующему излучению маломощных радиолокационных прицелов и тепловому излучению двигателей были уничтожены

86% истребителей МиГ-29, 35% истребителей МиГ-21, 10% батарей мобильных ЗРК «Квадрат» [173].

Часть зенитных сил и средств ПВО, а также истребителей ПВО Югославии уцелели, но только благодаря тому, что они вообще не применялись в противоборстве с воздушным противником и находились в защитных укрытиях. Именно это обстоятельство не позволило США полностью реализовать программу отработки методов борьбы с ПВО противника, созданной на базе активной радиолокации [173].

Главный вывод, который следует сделать из результатов подавления ПВО Югославии, состоит в том, что в войнах нового поколения классическая ПВО, построенная на базе активной радиолокации, будет неэффективной. В войнах нового поколения активная радиолокация средств ПВО, так же как и другие источники радиоизлучения, становится системоразрушающей, так как поражается противником в первую очередь.

Впервые в ходе операции был проведен эксперимент по подавлению информационного потенциала противника: его теле- и радиостанций, ретрансляторов, редакций местных электронных и печатных средств массовой информации, которые использовались для освещения хода военных действий и пропаганды. При выборе целей США и другие страны НАТО не всегда придерживались норм международного гуманитарного права, регламентирующего правила ведения войны, о чем свидетельствует поражение телерадиоцентра сугубо гражданского назначения. В результате был полностью подавлен информационно-пропагандистский потенциал Югославии. Основными средствами подавления в операции РЭБ являлись самолеты ЕС-130Н и ЕА-106В, которые действовали за пределами зоны ПВО Югославии, а также практически все тактические истребители, которые доставляли до рубежей пуска высокоточные ракеты, самонаводящиеся на источник излучения [173].

5.2.5. Проведение информационно-психологических операций

Для обеспечения военной акции против Югославии до ее начала НАТО провела информационную войну. В ходе информационной войны подаваемая информация отличалась большим количеством недостоверных фактов и даже откровенной ложью. Главной целью являлось побудить мировое общественное мнение если не к поддержке, то, но крайней мере, к тому, чтобы оно не препятствовало вооруженному

вторжению НАТО на Балканы. Активное применение сил и средств психологических операций вооруженных сил США началось задолго до первых ударов ВВС НАТО по территории Югославии. Объединенная группа психологических операций вооруженных сил США совместно с соответствующими структурами Великобритании и ФРГ осуществляла широкомасштабное и активное информационно-психологическое воздействие как с помощью печатной, так и с помощью технической пропаганды [95].

Основными направлениями содержания материалов информационно-психологического воздействия на население и военнослужащих Союзной Республики Югославии явились [95]:

- разъяснение «гуманных» целей военной акции НАТО, предпринятой якобы во имя спасения косовских албанцев от «геноцида» и их «безопасного возвращения на родину»;
- убеждение в неизбежности и обязательности размещения в Косово международного военного контингента под эгидой НАТО;
- показ «монолитного единства» стран НАТО по косовской проблеме, их решимости добиться поставленных целей в конфликте;
- демонстрация военной мощи НАТО;
- дискредитация президента С. Милошевича и его ближайшего окружения;
- разжигание противоречий среди военнослужащих и населения Югославии (например, между армией и полицией или между населением и руководством государства).

В Македонию для поддержки сухопутной группировки НАТО были переброшены регулярные и резервные подразделения 4-й группы психологических операций, на базе которых была сформирована объединенная оперативная группа в составе 6-го регионального батальона психологических операций, 3-го батальона подготовки и распространения материалов психологических операций и роты «В» 9-го батальона тактических психологических операций. Вблизи г. Скопье специалистами этой группы были развернуты две легкие типографии, а также мобильные средневолновые радиостанции. Кроме того, в Македонию из Боснии была временно передислоцирована часть усиленного резервистами 96-го батальона по работе с гражданским населением. К проведению психологической операции против Югославии и для нейтрализации боснийских сербов активно привлекались специальные

подразделения, входящие в состав американского контингента сил по стабилизации в Боснии и Герцеговине [95].

Основными материалами печатной пропаганды явились листовки. Их содержание разрабатывалось специалистами 6-го регионального батальона, полиграфическое исполнение производилось 3-м батальоном подготовки и распространения материалов психологических операций. Листовки распространялись с помощью авиации (С-130, С-141) и беспилотных летательных аппаратов с использованием специальной авиационной тары (вместимость – 20-40 тыс. листовок) и авиационных бомб (30-80 тыс. листовок). Всего было распространено около 40 млн экземпляров листовок (в ходе войны в зоне Персидского залива было распространено 29 млн листовок) [95].

В целях наращивания информационно-психологического давления на Югославию по решению военного командования НАТО был сформирован специальный орган радио- и телевизионной пропаганды «Радио и телевидение союзных сил». С апреля 1999 г. в ее рамках в эфир начали выходить телевизионная станция «Объединенный голос НАТО» и радиостанция «Иван». Кроме того, к этой работе привлекались штатные радиостанции роты радио- и телевещания 3-го батальона подготовки и распространения печатной, аудио- и видеоинформации. Для обеспечения регулярного радио- и телевещания программ этих станций в район конфликта были передислоцированы на авиабазы Aviano (Италия) и Rammshtein (Германия) два самолета ЕС-130Е/J 193-го авиакрыла Национальной гвардии ВВС США. Самолеты ежесуточно барражировали в сопровождении истребителей по периметру югославской границы на высоте 9-10 тыс. метров и вели трансляцию радио- и телепередач на сербскохорватском и албанском языках в течение 2,5 ч [95].

Основным мотивом радио, телепередач являлся тезис о том, что НАТО не воюет с сербским народом, а операция «Союзная сила» направлена против «..преступного режима С. Милошевича, проводившего политику геноцида в отношении косовских албанцев и повинного в развязывании братоубийственной войны на Балканах» [95].

Одновременно осуществлялось подавление каналов теле- и радиовещания Югославии. Выполнение этой задачи облегчалось тем, что за первые недели бомбардировок было разрушено или серьезно повреждено до 80% объектов телекоммуникаций Югославии. Для повышения эффективности работы самолетов ЕС-130 командование НАТО планировало распространить в населенных пунктах Сербии и местах дислокации частей югославской армии значительное количе-

ство радиоприемников с фиксированными частотами. Запасы таких радиоприемников были созданы на авиабазах ВВС США в ФРГ [95].

5.2.6. Основные выводы

Важным итогом военной кампании против Югославии стало понимание европейскими членами НАТО уровня своего отставания от США в части реализации концепции сетецентрических войн. Опыт войны в Югославии стал основой для интенсивного реформирования вооруженных сил европейских стран с целью их адаптации к войнам нового поколения. Данный опыт позволил обосновать целесообразность сокращения сухопутных войск не только США, но и других стран НАТО, а также постепенной перестройки их вооруженных сил в двувидовой функциональный состав: стратегические ударные и стратегические оборонительные виды сил [173, 174].

Операция против Югославии подтвердила возрастающее значение ВВС и ВМС как важнейших составляющих разведывательно-ударных боевых систем. Следует ожидать, что во всех военных конфликтах будущего эти два вида вооруженных сил будут представлять основу стратегических ударных сил. При этом полностью изменяется способ применения ВВС и ВМС. Они превращаются в «транспортное средство» доставки огромного количества беспилотных высокоточных крылатых ракет до рубежей пуска, находящихся за пределами зон поражения ПВО противника [173].

Война в Югославии открыла новую скрытую гонку вооружений нового поколения – высокоточные крылатые ракеты воздушного и морского базирования, средства их доставки, а также навигационные средства, системы управления и высокоточные средства обороны от их массированных налетов. Понятно, что наилучшие позиции получат страны, лидирующие в области создания высокоточного оружия и средств обороны, построенных на базе отказа от использования принципа активной радиолокации [173].

В 1998 г. стоимость крылатой ракеты как морского, так и воздушного базирования оценивалась примерно в один миллион долларов. В 1998 г. США на закупку крылатых ракет было израсходовано 50 млрд долларов, на 1999 г. в бюджете было выделено 48,7 млрд долларов, а в 2000 г. – уже 60 млрд [173].

Внедрение концепции сетецентрической войны обосновывает необходимость изменения не только вооружения, но также состава и структуры вооруженных сил. Однако даже в наиболее развитых стра-

нах структура вооруженных сил, формы и способы их применения будут меняться не сразу, а по мере принятия на вооружение и накопления достаточного количества высокоточного оружия. В течение некоторого времени вооруженные силы таких стран будут развивать потенциал ведения войны нового поколения, одновременно сохраняя способность выполнять большое количество задач оперативно-тактического и даже стратегического уровня, относящихся к войнам прошлого поколения [173].

Американскими экспертами отмечается, что действия армии США в Югославии показали пример того, каким образом противник будет противостоять вооруженным силам США в возможных конфликтах нового века: действуя распределенными малыми подразделениями, широко применяя мобильные системы ПВО, массово используя маскировку, камуфляж и укрытия, а также информационные операции. При этом экспертами признается, что войска НАТО были вынуждены прибегнуть к неоптимальным методам нападения в силу необходимости минимизировать собственные потери [2, 29].

5.3. Операция США и их союзников «Иракская свобода» («Шок и трепет») в Ираке в 2003 г.

Прообразом сетецентрической войны стала операция союзных войск против Ирака в 2003 г. В этой войне были применены новые формы и способы боевых действий. Ниже представлены ключевые особенности данного военного конфликта на основе анализа работ [95, 174, 269, 291, 294-299, 301].

При подготовке к войне США, применив военную хитрость, сумели ввести в заблуждение иракское руководство о том, что они собираются вести войну в рамках сухопутной наземной операции. Вооруженные силы Ирака готовились к такому варианту войны и ушли в глубокую оборону, ожидая наземных военных действий. Однако США и их союзники начали против Ирака бесконтактную войну с активным применением средств ВТО.

Руководство союзников помимо экономических и политических целей ставили и военную – разгром армии Ирака и проверка в боевых условиях концепции боевых действий и переброски войск, системы управления вооружением, боевого управления, тыловой транспортной системы. В войне была задействована группировка войск

США и Великобритании в зоне Персидского залива, а также воинские контингенты вооруженных сил Австралии и Польши [174].

К началу операции в регионе была создана крупная группировка ВВС, ВМС и сухопутных войск, насчитывавшая до 2,8 млн военнослужащих, более 1000 боевых самолетов, 47 стратегических бомбардировщиков B-52H, B-1B, B-2A, свыше 100 боевых кораблей, из них 35 носителей КРМБ Tomahawk (870 КРМБ), современные силы РЭБ, спутниковые системы разведки и навигации. Управление коалиционной группировкой сухопутных войск в ходе подготовки и ведения операции осуществляли штаб 3 ПА, управление группировкой сухопутных войск США – штаб 5 АК (оба штаба дислоцировались в г. Кэмп-Дауха, Кувейт) [291].

Наземную фазу операции против Ирака осуществляла коалиционная группировка, в составе которой насчитывалось до 112 000 человек, до 500 танков, более 1 200 боевых бронированных машин, около 900 орудий, РСЗО и минометов, свыше 900 вертолетов и до 200 зенитных ракетных комплексов [174].

Учитывая свои ошибки в результате предыдущих кампаний, командование вооруженных сил союзников ввело в качестве обязательного элемента наземное наступление группировок бронетанковых и механизированных войск в сочетании с десантами. Наступление на Багдад группировки наземных войск велось по двум операционным направлениям с территорий [174]:

- Кувейта (направление главного удара);
- Иордании (второе направление).

Основными задачами группировки войск «Юг», действующей на направлении главного удара, были [174]:

- разгром иракских войск на оборонительных рубежах вдоль рек Тигр и Евфрат;
- взятие под контроль южных нефтеносных районов Ирака;
- выход к Багдаду и его блокирование.

Оперативное построение войск осуществлялось в один эшелон с выделением общего резерва.

Основными задачами группировки войск «Запад», действующей на втором направлении, были [174]:

- захват важных объектов (аэродромов, плотин, транспортных узлов), расположенных в пустынных западных и северо-западных районах Ирака;
- контроль дорог, соединяющих Багдад с Иорданией и Сирией.

Выполнение задач осуществлялось небольшими группами и, как правило, на вертолетах [174].

12 апреля 2003 г. была развернута коалиционная группировка наземных войск «Север». Группировка «Север» совместно с курдскими вооруженными формированиями при поддержке боевой авиации коалиционных сил решали задачи по разгрому иракских войск и взятию под контроль нефтеносных районов на севере страны.

При подготовке и в ходе войны США на практике проверили сетецентрическую концепцию ведения боевых действий. Война против Ирака в 2003 г. носила воздушный и, частично, наземный характер, информационное обеспечение и управление войсками осуществлялось с широким использованием космических средств. Количество выпущенных крылатых ракет морского и воздушного базирования составило 1000, что более чем в три раза больше, чем в операции «Буря в пустыне». При этом анализ участия тактической авиации в региональных конфликтах показывает устойчивую тенденцию к увеличению доли применения ею высокоточного оружия. В частности, в операции против Ирака в 2003 г. этот показатель был в 8,5 раза больше, чем в 1991 г. [95].

С началом сухопутной части операции действиям сухопутных войск были присущи высокая активность, выбор для нанесения ударов наиболее слабых мест в иракской обороне, широкий маневр, хорошее взаимодействие, в том числе с тактической авиацией. Соединения и части наступавших войск в интересах скорейшего решения задач широко использовали удары по стыкам оборонявшихся корпусов и дивизий Ирака, обход противника, выброску и высадку для захвата важных в оперативно-тактическом отношении районов и рубежей десантов. Войска вступали в бой без тыла, без заблаговременной разведки, но боеприпасы и топливо приходили, в основном, вовремя, а растянутые коммуникации не слишком влияли на снабжение. Встречая жесткую оборону иракцев (там, где это было), войска, как правило, избегали втягивания в затяжные действия и старались поразить встретившегося противника при помощи тактической и армейской авиации, а также дальнобойных огневых средств [174].

Ниже представлены основные особенности военного конфликта в Ираке с акцентом на применение в нем элементов сетецентрической войны.

5.3.1. Экономическое противоборство

Войну в Ираке нельзя рассматривать изолированно от экономического противоборства, главным содержанием которого стала блокада Ирака. С 1991 г. в соответствии с резолюцией Совета Безопасности ООН осуществлялось эмбарго на торговлю Ирака с другими государствами. Соответственно состоявшие на вооружении Ирака образцы вооружения и военной техники морально устарели, требовали ремонта и глубокой модернизации. Поэтому вполне закономерно, что к началу боевых действий в 2003 г. общее соотношение основных сил и средств коалиционной группировки и Ирака составляло 4,4:1, а по авиации – 8:1 [174].

Непосредственно перед началом операции подкупом были выведены из активных действий 50% командующих армейских округов и республиканской гвардии. На подкуп командующих выделялось до 10 млн долларов, в результате три из семи армейских корпусов не принимали активного участия в боевых действиях. ЦРУ оплатил предательство командующих военными округами и обеспечил вывоз их семей из Ирака на завершающем этапе операции. Война в Ираке – это новая война, война, основанная на визуальных, пропагандистских и прочих поражающих воображение противника эффектах [174].

Пентагон и спецслужбы США также готовили кибератаки на банковский сектор Ирака с целью блокировать финансовые транзакции и заморозить миллиарды долларов на банковских счетах, принадлежащих как членам семьи С. Хусейна, так и иракскому правительству. Это должно было подорвать финансовую систему страны перед союзным вторжением и блокировать функционирование государственных служб, снабжение войск, а также выплату денежного довольствия военнослужащим. Однако в связи с тем, что специалисты высказывали опасения, что, поскольку банковские сети Ирака имели прямой выход на европейские сети, такая атака может вызвать полномасштабный мировой сбой финансовых транзакций, данной атаки не последовало [95].

5.3.2. Реализация концепции обезоруживающего удара

При реализации концепции обезоруживающего удара как основы первой части операции были массированно задействованы силы ВВС и средства ВТО. При этом за сутки до начала первого массированного ракетно-авиационного удара был введен круглосуточный ре-

жим разведки стратегическими самолетами-разведчиками. Одновременно началась постановка помех сетям управления войсками, а за шесть-восемь часов до массового взлета авиации была осуществлена постановка радиоэлектронных помех средствам предупреждения и радиолокационного наведения истребителей Ирака, в результате чего системы разведки и управления ПВО были парализованы [95].

Для завоевания господства в воздухе основные усилия были сосредоточены на огневом подавлении пунктов управления и средств ПВО, поражении самолетов Ирака до их взлета, разрушении аэродромов. Эффективному выполнению перечисленных мероприятий во многом способствовала тщательная разведка системы ПВО с помощью космических, морских, воздушных и наземных средств [95].

В первом массированном ударе (продолжительностью 2,5 ч) было задействовано до 100 крылатых ракет морского базирования Tomahawk и около 600 боевых самолетов, выстроенных в четыре эшелона [95]:

- ударный эшелон КРМБ Tomahawk, запущенный двумя волнами с кораблей ВМС США, которые находились в Персидском заливе и Красном море;
- эшелон подавления системы ПВО и дезинформации системы государственного и военного управления Ирака с участием более 170 боевых самолетов;
- два ударных эшелона с участием соответственно 303 и 122 боевых самолетов.

Всего за первые двое суток боевых действий было совершено 2107 самолето-вылетов. В результате комбинированного применения крылатых ракет Tomahawk, малозаметных самолетов F-117A, вооруженных авиабомбами с лазерной системой наведения, самолетов РЭБ различных типов и истребителей-бомбардировщиков F-4G Wild Weasel силы ПВО Ирака и, в частности, его ЗРК в первые же часы боевых действий оказались подавленными настолько, что уже через сутки американцы сочли возможным ввести в действие легкоуязвимые бомбардировщики B-52, а от зенитного ракетного огня пострадал только один американский самолет [95].

Все воздушные вылеты проводились в соответствии с заранее разработанным графиком. При этом первые авиационные удары наносились уже через несколько минут после ударов крылатых ракет Tomahawk. Тщательно координировались действия самолетов РЭБ, истребителей, их сопровождения, истребителей-бомбардировщиков, штурмовиков и самолетов-заправщиков. Большую роль в решении этой за-

дачи сыграли самолеты дальнего радиолокационного обнаружения и управления ВВС E-3A Avaks и ВМС E-2C Hawkeye. Один самолет E-3A позволял осуществлять одновременную проводку 2000 самолетов, отличать свои самолеты от самолетов противника, передавать данные о местонахождении обнаруженных самолетов непосредственно на борт своих истребителей. Помимо того самолет E-3A ретранслировал истребителям-бомбардировщикам данные о наземных целях противника, собранные и обработанные разведывательными самолетами и аппаратами космической разведки. Именно ими обеспечивалась эффективная, по мнению специалистов Пентагона, борьба с иракскими подвижными пусковыми установками ракет «Scud» [95].

Примерно через сутки после того, как система ПВО Ирака была надежно подавлена и господство в воздухе стало бесспорным, к участию в воздушной операции были привлечены стратегические бомбардировщики B-52. Самолеты B-52 осуществили «ковровое» бомбометание в районах расположения четырех бронетанковых и механизированных дивизий республиканской гвардии Ирака, развернутых к северу от Кувейта, а также проводили систематические удары по авиабазам [95].

К особенностям в проведении воздушной наступательной операции в этой войне относятся: массированное использование крылатых ракет Tomahawk с обычным зарядом для ударов по точечным целям, прикрытым сильной ПВО, а также самолетов дальнего радиолокационного обнаружения для контроля воздушной обстановки и наведения истребительной авиации; применение стратегических бомбардировщиков B-52 для ударов обычными средствами, самолетов F-117A Stealth и противоракетных средств, основанных на новых принципах действия [95].

Характерными чертами воздушного наступления явились значительное повышение точности бомбовых ударов благодаря широкому использованию управляемых средств поражения и массированное применение новейших авиационных средств. Совершив в обеих Иракских операциях примерно одинаковое количество боевых вылетов (41 тыс. – в 1991 г. и 46 тыс. – в 2003 г.) с применением практически одинакового числа высокоточных средств поражения, авиация поразила, по данным американской прессы, почти в 4,5 раза больше целей, чем 12 лет назад (4 500 и 19 900 соответственно). Это было достигнуто значительным повышением эффективности высокоточного оружия и средств разведки. При этом, если в первой войне против Ирака только отдельные типы американских самолетов (F-117, F-15E и некоторые

другие) были оснащены высокоточным оружием, то во второй Иракской войне практически вся ударная авиация и большинство вертолетов США имели на борту ВТО и были способны поражать цели с высокой вероятностью [95].

Эффективность применения боевой авиации, оснащенной высокоточным оружием, в операциях и локальных войнах последних лет приведена в табл. 5.1 и 5.2 по данным из работы [95].

Таблица 5.1. Боевой состав военно-морских сил коалиции с участием США к началу операции «Шок и трепет» [95]

Корабельный состав	**Октябрь, 2002 г.**	**Ноябрь, 2002 г.**	**Декабрь, 2002 г.**	**Январь, 2002 г.**	**Февраль, 2003 г.**	**Март, 2003 г.**
Количество кораблей	44	52	45	56	87	125
США	19	21	18	22	44	75
Великобритания	3	7	7	8	21	22
Австралия	5	5	5	5	5	5
Носители КРМБ	10	11	8	11	20	35
Боезапас КРМБ	237	280	196	300	529	869
Количество АУГ	1	2	1	2	4	6

Таблица 5.2. Применение авиационных средств поражения США и их союзниками в ряде военных операций [95]

Показатель	**«Буря в пустыне» (Ирак, 1991 г.)**	**«Решительная сила» (Югославия, 1999 г.)**	**«Несокрушимая свобода» (Афганистан, 2001 г.)**	**Военная операция США и их союзников против Ирака (Ирак, 2003 г.)**
Общее количество использованных:				
бомб и ракет	256 000	23 000	22 000	29 000
высокоточных боеприпасов	20 500	8 000	12 500	20 000
доля высокоточного оружия, %	8	35	57	68

Таблица 5.3. Результаты применения крылатых ракет в операциях против Ирака [95]

Показатель	1991	2003
Применение крылатых ракет морского базирования:		
количество пусков КРМБ	330	800
количество пораженных целей	60	790
Применение боевой авиации:		
количество самолето-вылетов	41 300	45 600
количество пораженных целей	45 50	19 900
Потери летательных аппаратов коалиционных сил:		
боевых самолетов	38	1
боевых вертолетов	16	6

В ходе ведения боевых действий проявилась устойчивая тенденция к осуществлению одновременного разгрома первых и вторых эшелонов иракских войск вслед за массированным применением высокоточного оружия наземного и воздушного компонентов при широком использовании тактических воздушных десантов и аэромобильных частей [95].

Анализ опыта боевых действий в зоне Персидского залива показывает, что реализация способа одновременного поражения группировки противника стала возможна при наличии следующих условий, таких как [95]:

- достаточное количество высокоточных средств, осуществляющих глубокое поражение объектов противника;
- значительное повышение огневой мощи, ударной силы и подвижности боевых формирований тактического уровня.

Анализ опыта проведения наземной операции показывает, что можно выявить некоторые особенности действий соединений сухопутных войск США в операциях в Персидском заливе [95]:

- переход к постановке боевых задач по объектам, а не рубежам;
- планирование боевых действий с использованием единых, непрерывно обновляющихся цифровых, а не топографических карт;
- уклонение от прямых боевых столкновений с противником, вместо фронтальных атак на противника;
- ведение наступлений соединений и частей преимущественно в предбоевых порядках.

При этом, наличие большого количества систем ВТО позволило осуществлять:

- одновременные массированные удары средствами воздушного и наземного компонентов;
- одновременные и последовательные групповые, а также одиночные удары.

5.3.3. Достижение информационного превосходства за счет использования космических средств связи, управления, разведывательного и навигационного обеспечения

Только наличие подавляющего технологического превосходства (развитых систем управления, связи, разведки, радиоэлектронной борьбы, информационного противоборства, оружия, моделирования боевых действий, поддержки принятия решений и осуществления планирования при широком использовании новых информационных технологий и систем) позволило командованию коалиционными вооруженными силами достаточно гибко подойти к выбору способов и форм военных действий в Ираке. По мнению зарубежных и отечественных специалистов, созданные системы управления, связи, разведки и поражения обеспечивали в целом эффективное управление и надежную связь, детальное изучение и оценку обстановки в ожидаемых районах боевых действий. Они позволяли использовать различные средства поражения, осуществлять их координированное применение в режиме реального времени – практически сразу после обнаружения, распознавания и определения координат объектов космическими, воздушными или наземными средствами разведки [291].

Реализация на практике сетецентрического принципа ведения военных действий означала переход от действий по заранее составленному плану к таким действиям, когда выбор объектов поражения противника и распределение по ним конкретных сил и средств проводятся непосредственно перед нанесением поражения выбранным целям. Таким образом, получив полное информационное превосходство над противником, который фактически лишился возможности вести осмысленные и скоординированные боевые действия, группировки коалиционных сил США и их союзников достигли самосинхронизации боевых действий [95].

Основной вывод из опыта Иракской войны состоит в том, что победу в ней одержали интегрированные в единую современную си-

стему управленческая, интеллектуальная, психологическая, связная, информационная, навигационная, разведывательная, техническая и поражающая составляющие (подсистемы) системы ВС США и их союзников. В целом технологическое превосходство армии США и их союзников базируется на многих элементах, а именно на всестороннем и многочисленном использовании космических средств связи, разведки и навигации [291].

Наиболее значительную роль сыграли средства космической разведки США. К началу боевых действий в состав орбитальной группировки космической разведки США входило 29 космических аппаратов, из которых 4 – видовой разведки (оптической и радиолокационной), а остальные – радио- и радиотехнической разведки [291].

Разведку из космоса вели спутники оптико-электронной разведки Key Hole, радиолокационной разведки Lacrosse, а также радио- и радиотехнической разведки Ferret, Aquacade и Shale. Накануне операции орбитальная группировка была увеличена за счет запуска с североамериканского континента новейших разведывательных спутников типа Magnum и Vortex. Космическая разведка обеспечивала просмотр объектов на территории Ирака с периодичностью до 20 минут и разрешением до 0,3-0,4 м [95].

В начальной фазе операции для обеспечения командования многонациональных сил разведывательными данными в интересах применения средств РЭБ в зоне Персидского залива была развернута широко разветвленная система технических средств разведки. Наземная группировка сил и средств разведки насчитывала до 1000 постов радио- и радиотехнической разведки. В целом силы и средства технической разведки выполнили задачи по добыванию разведывательной информации о группировке иракских войск и характеристиках их радиоэлектронных средств в целях их подавления [95].

В ходе боевых действий было задействовано большое количество средств коммуникации: 300 систем телефонной связи, 30 компьютерных сетей и множество спутниковых терминалов, ежедневно обслуживавших примерно 700 000 разговоров, не говоря уж о передаче более 150 000 информационных сообщений [95].

Военные действия в Ираке еще раз подтвердили большое значение спутниковых систем связи в управлении войсками при подготовке операций и в ходе ведения боевых действий. Спутниковые системы связи обеспечивали защищенную связь объединенного центрального командования и военно-политического руководства США, военного руководства высших уровней иерархии управления с частя-

ми и подразделениями, а также связь между подразделениями. Для этого использовались как военные (DSCS, Milstar, Flitsatcom и др.), так и многочисленные коммерческие спутниковые системы связи. Особенностью активной фазы войны в Ираке являлось ведение операций на огромной территории без четко выраженной линии фронта, когда очень велик разброс сил и средств. В таких условиях только с помощью спутниковых средств связи возможно обеспечить оперативное руководство войсками [291].

В интересах обеспечения управления наземным, воздушным и морским компонентами американского контингента войск активно задействовались каналы военных спутниковых систем связи. Так, 3-я эскадрилья космических операций (авиабаза Шривер), которая управляла системой DSCS, контролировала функционирование в зоне ответственности объединенного центрального командования ВС США более 500 пользователей, а 4-я эскадрилья обеспечивала работу более 1400 пользователей, принимавших непосредственное участие в операции. Большое распространение получили спутниковые телефоны для связи мобильных групп и даже отдельных военнослужащих с командирами и друг с другом. Для этого широко использовались системы персональной спутниковой связи гражданского назначения GlobalStar, Inmarsat и Iridium [291].

Кроме того, ключевое значение спутниковые системы связи имели для оперативного доведения до подразделений разведывательной информации, получаемой с помощью интегрированной разведывательной системы, в том числе и от беспилотных разведывательных летательных аппаратов Global Hawk и Predator [291].

Использовавшиеся системы, комплексы, средства, органы разведки обеспечивали эффективное обнаружение сил и средств (объектов) противника, в том числе на больших дальностях, а автоматизированные системы управления войсками позволяли в кратчайшие сроки организовывать взаимодействие различных систем оружия по огневому поражению противника. Кроме того, в ходе боевых действий прошла практическую апробацию концепция сопряжения информационных систем вооруженных сил государств блока НАТО. Так, было реализовано взаимодействие между американскими и английскими информационными системами, в частности обеспечивался прием разведывательных данных от самолетов СК-4А (Великобритания), оснащенных контейнерной разведывательной станцией «Карток», американскими средствами приема и обработки разведывательной информации [291].

В операции в Ираке впервые была успешно применена система TBMCS (Theater Battle Management Core System), координировавшая вылеты самолетов, относящихся к разным видам вооруженных сил (ВВС и палубной авиации ВМС) [95].

В тактическом и оперативном звеньях был применен комплекс боевого управления FBCB (Force XXI Battle Command Brigade or Below), который представляет собой систему графического отображения информации на тактическом уровне с точностью до отдельного военнослужащего. Это позволило в режиме реального времени принимать и отображать на экранах компьютеров электронные карты местности командиров всех звеньев, в том числе действовавших автономно, данные космической и воздушной разведки, БПЛА и полностью отказаться от бумажных топографических карт [95].

В данной операции командование ВС США широко использовало усовершенствованные комплекты аппаратуры автоматизированной системы управления FBCBB-BFT на уровне бригады и ниже. Эти комплекты применялись для повышения эффективности боевого управления и оперативности получения данных о тактической обстановке. Так, в течение трех месяцев подготовки к ведению боевых действий в части и подразделения (до роты включительно) 3-й механизированной, 101-й воздушно-штурмовой и 82-й воздушно-десантной дивизий, а также в подразделения морской пехоты США было поставлено около 1 200 комплектов FBCBB-BFT. Они были установлены на пунктах управления объединенного центрального командования сухопутных войск США, в командно-штабных машинах М577, основных боевых танках M1A2 Abrams, боевых машинах пехоты M2A2 и M2A3 Bradley, автомобилях повышенной проходимости типа Hummer и вертолетах армейской авиации АН-64 Apache и СН-47 Chinook. Кроме того, 50 таких комплектов было поставлено в подразделения группировки ВС Великобритании. Основным предназначением данной аппаратуры являлось обеспечение автоматизированного контроля перемещения своих сил и средств и формирование для всех пользователей единой карты (картины) тактической обстановки в режиме реального времени. В частности, обеспечивалось отображение координат конкретных единиц боевой техники, опасных участков местности (минные заграждения, противотанковые рвы и др.), решение навигационных задач в условиях ограниченной видимости (туман, задымленность, песчаные бури и темное время суток), а также информационный обмен формализованными текстовыми сообщениями и графической информацией. В состав комплектов АСУ FBCBB-BFT вошли

аппаратно-программные средства (специализированные компьютеры типов AN/UYK-128 и EW2000, приемники космической радионавигационной системы NAVSTAR), дополнительно оснащенные приемопередатчиками международной системы подвижной спутниковой связи INMARSAT [291].

В ходе боевых действий данные о местоположении сил и средств определялись с помощью системы NAVSTAR и совместно с разведывательными данными передавались для их комплексирования по каналам системы INMARSAT на передовой пункт управления объединенного центрального командования (г. Кэмп-Дауха, Кувейт) [291].

Таким образом, в системе управления тактического уровня формировалась единая база навигационных данных о местоположении своих сил и средств, а также объектов противника. Источниками информации для базы были результаты автоматической передачи и распределения данных о местоположении своих средств, определенных по сигналам космической навигационной системы NAVSTAR, а также силы и средства разведки, сообщения командиров, средства опознавания «свой-чужой» и беспилотные летательные аппараты [95].

Обобщенная информация по каналам спутниковой связи передавалась в подразделения, участвовавшие в боевых действиях. Обновление единой картины тактической обстановки на экране пользователей осуществлялось автоматически благодаря использованию динамической фильтрации данных. Тактическая информация отображалась на экранах дисплеев на фоне электронных карт или видеоизображений местности в виде стандартных пиктограмм, обозначающих места дислокации боевой техники. Обновление данных о местоположении сил и средств происходило автоматически с периодичностью один раз в час – при длительной стоянке, один раз в 5, 10 или 15 мин – во время движения, а также по запросу. В случае необходимости время опроса могло изменяться пользователем [291].

В интересах формирования единой карты (картины) тактической обстановки для командований СВ, ВВС и ВМС система FBCBB-BFT сопрягалась с глобальной системой оперативного управления ВС США. В ходе операции, по оценке американского командования, были подтверждены высокие эффективность и надежность работы аппаратуры FBCBB-BFT. Ее применение позволило значительно уменьшить количество огневых ударов по своим силам и средствам и точно определять, в частности, координаты сбитых или совершивших вынужденную посадку вертолетов, а также вышедших из строя боевых машин [291].

Передача сообщений в автоматизированных системах управления звена «бригада и ниже» производилась в формализованном виде. Все передаваемые в системе сообщения подразделялись на четыре категории, в том числе предупреждения и тревоги, данные огневой поддержки, доклады командиров, а также информация о планировании боевых действий [95].

Высокую эффективность показали новые средства радиосвязи, использовавшиеся в сетях обмена разведывательной информацией в тактическом звене управления. С их помощью впервые в ходе реальных боевых действий удалось продемонстрировать эффективность автоматизированного формирования электронной карты тактической обстановки, единой для различных звеньев (инстанций, ступеней) управления. В частности, впервые были применены в звене «взвод-рота» и разведывательно-поисковыми группами единые тактические терминалы JTT-B, которые дают возможность в режиме реального времени отображать получаемые по спутниковым и наземным каналам связи данные на электронной карте, выводимой на экран терминала [291].

Вместе с тем для описанной системы свойствен ряд недостатков. К ним относятся: неполное отображение данных о противнике, что объясняется ограниченными возможностями применявшихся комплектов аппаратуры, которые фактически были упрощенным вариантом АСУ FBCBB-BFT; задержки и нарушения в очередности передачи и приема сигналов (распоряжений) боевого управления, обмене предусмотренными видами сообщений в установленные сроки и с требуемым качеством; нарушения связи с командирами и пунктами управления при их передвижении [291].

По оценкам американского командования, система управления, построенная на основе сетецентрических принципов, в ходе боевых действий в Ираке показала высокую эффективность и надежность работы, а также удобство и простоту использования. В целом применение этой системы позволило повысить боевые возможности частей и подразделений ВС, оперативно получать данные о тактической обстановке, наносить высокоточные удары и свести к минимуму случаи ошибочного нанесения ударов по своим войскам, при этом в звене «бригада-рота» вся оперативная обстановка отслеживалась по электронным картам. В качестве основного недостатка системы отмечалось неполное отображение данных о противнике [95].

Развертывание и использование такой технологически развитой системы управления потребовало серьезных вычислительных ре-

сурсов. В связи с этим в зоне конфликта было использовано более 4 тыс. бортовых компьютеров и 100 высокопроизводительных серверов обработки данных [95]. Так, вычислительные средства штаба армейского корпуса были способны отслеживать до 1000 наземных целей в час [174].

Вместе с тем высокая технологичность и компьютеризированность боевых действий формирует слабые места ВС. Опыт боевых действий в Ираке показал, что в сетецентрической войне все виды ВС в огромной степени зависят от космических средств разведки, связи и навигации. Именно это предопределяет их уязвимость, так как данные виды обеспечения могут быть нейтрализованы путем создания соответствующих помех. В ходе операции в Ираке были случаи, когда десант, высадка которого планировалась в Иракской пустыне, оказался в Иране, ракеты, выпущенные по Багдаду, попадали на территорию Турции, а 27 марта штурмовик А-10А расстрелял свою же колонну бронетехники. Данные факты подтверждают, что самая совершенная техника не может функционировать без человека и зачастую именно человеческий фактор должен вносить определяющую роль в принятие решений на поле боя [174].

5.3.4. Использование беспилотных и робототехнических средств

В войне с Ираком 2003 г. ВС США продолжилось наращивание интенсивности использования различного рода беспилотных, дистанционно управляемых и робототехнических средств.

Как следует из материалов, опубликованных в открытой печати, с 8 марта по 2 мая 2003 г. БПЛА Global Hawk, чьи полеты контролировались с континентальной части США, совершил 16 боевых вылетов общей продолжительностью свыше 350 часов. Этот показатель составляет лишь 3% от общего количества разведывательных полетов авиационной группировки. Вместе с тем, по оценкам специалистов, именно этим аппаратом добыто более 55% всех данных о важных и так называемых критичных по времени объектах и целях [95].

В ходе боевых действий ВС США продолжили широкое использование разведчиков на основе БПЛА. При проведении операций на долю БПЛА-разведчиков пришлось 85% всей воздушной фоторазведки [174]. Благодаря этому у командиров был доступ к информации о расположении боевых единиц противника в реальном времени. Причем время доведения информации до потребителей не превышало

10 мин. Точность определения координат в режиме радиолокационной съемки местности составляла, по некоторым данным, около 10 м. Практический потолок достигал 20 км при максимальной продолжительности полета 40 ч [95].

Также в операции в Ираке нашли применение роботизированные дистанционно управляемые инженерные машины, которые использовались в ходе преодоления полосы обеспечения подразделениями и частями 2-го бронекавалерийского полка и 1-й механизированной дивизии армии США [95].

5.3.5. Достижение информационного превосходства за счет применения средств радиоэлектронной борьбы и информационно-технических воздействий

Убедительным подтверждением постоянно возрастающего значения радиоэлектронной борьбы в ВС США являются результаты операции «Шок и трепет» в зоне Персидского залива. Эти примеры практического применения сил и средств радиоэлектронной борьбы свидетельствуют о том, что РЭБ на современном этапе приобретает характер крупномасштабных действий и вносит значительный вклад в достижение успеха в информационном противоборстве сторон [95].

В интересах ведения РЭБ в войне с Ираком привлекались тринадцать частей и подразделений, в том числе три бригады разведки и РЭБ из состава 3-го и 7-го армейских и 18-го воздушно-десантного корпусов, восемь батальонов разведки и РЭБ и две отдельные роты разведки и РЭБ. Всего насчитывалось около 120 постов постановки помех и 30 вертолетов – постановщиков помех.

Авиационная группировка сил и средств РЭБ насчитывала свыше 100 самолетов (34 – EF-111A, 3 – EC-130H, 46 – F-4G, 39 – EA-6B). Кроме того, 100% авиации, участвующей в нанесении ударов, было оснащено средствами индивидуальной радиоэлектронной защиты от средств ПВО.

Высокая эффективность, продемонстрированная самолетами РЭБ в ходе вооруженного конфликта, подтверждена следующими фактами. Самолеты EA-6B Prowler, базировавшиеся на шести многоцелевых авианосцах, осуществили свыше 1600 самолето-вылетов общей продолжительностью 4600 ч, при этом был осуществлен запуск более 150 управляемых ракет Harm по позициям РЛС иракской системы ПВО. Под прикрытием радиоэлектронных помех самолеты F-4G Wild

Weasel осуществляли пуски противорадиолокационных ракет Standart Arm и Harm, уничтожая РЛС в полосе пролета ударной авиации [95].

Действия ВВС поддерживали EF-111A Raven, совершившие более 900 самолето-вылетов, и семь-девять EC-130H Compass Call. В ходе обеспечения прорыва системы ПВО и в последующих действиях тактической авиации коалиционная группировка осуществляла дезорганизацию управления ПВО Ирака комплексным применением крылатых ракет, самолетов F-117A Stealth, самолетов тактической и палубной авиации, а также самолетов РЭБ [95].

При радиоподавлении экраны радиолокаторов зенитно-ракетных комплексов полностью засвечивались, поэтому обслуживающий персонал был не в состоянии выделить на экране полезный информационный сигнал и осуществить эффективное целеуказание наземным средствам ПВО. Такое воздействие помех резко снизило боевые возможности группировок ВС Ирака по поражению воздушных целей. Кроме того, силы США нанесли высокоточные удары самонаводящимися ракетами по радиоизлучающим, теплоизлучающим и теплоконтрастным элементам ПВО [95, 173].

Главным выводом по результатам подавления ПВО Ирака является то, что в войнах нового поколения классическая ПВО на основе активной радиолокации будет уничтожена практически сразу же после начала боевых действий за счет массированного применения самонаводящегося на радиоизлучение оружия [173].

По сообщениям зарубежной печати именно благодаря самолетам РЭБ, которые явились одним из основных элементов обеспечения достижения превосходства в воздухе, была освобождена от воздействия иракской ПВО зона воздушного пространства на больших и средних высотах над всей территорией страны, что обеспечило полное доминирование авиации многонациональных сил [95].

В ходе бомбардировки Багдада 26 марта 2003 г. прошли боевые испытания электромагнитной Е-бомбы (бомба на новых физических принципах), после применения которой на несколько часов была парализована работа иракского телевидения [174].

Кроме того, анализ действий стратегической авиации США в зоне Персидского залива позволяет предположить, что с помощью крылатых ракет старого парка АСМ-86С бомбардировщики В-52 произвели испытание генераторов электромагнитного импульса для вывода из строя электростанций, линий электропередач, узлов связи и РЛС. Следовательно, уместно говорить о появлении нового боевого средства, которым является радиоэлектронное оружие. Приоритетными

целями радиоэлектронного оружия были ретрансляторные и передающие радио- и телестанции, линии электропередачи и энергосистемы. При этом для поражения таких целей использовались новые образцы нелетального оружия – графитовые бомбы и микроволновое оружие [95].

Поражающий эффект графитовых бомб достигался путем создания над объектом облака площадью до 200 кв. м из произведенных на основе углерода и обладающих сверхпроводимостью тонких волокон. При соприкосновении волокон с токонесущими элементами (изоляторы, провода и т.д.) происходило короткое замыкание и вывод из строя электроцепей [292, 293].

В ходе антииракской кампании ВВС США опробовали применение в Ираке микроволнового оружия, выполненного в виде боевой части стандартной крылатой ракеты Tomahawk. Длительность поражающего импульса микроволнового излучателя в несколько раз короче импульса лазерной установки, необходимой для поражения одной и той же цели, что существенно повышает эффективность его боевого применения. Эксперты США оценивают микроволновое оружие как чрезвычайно эффективное для борьбы с электронными компонентами систем контроля и управления, так как мощный миллисекундный импульс может привести к выходу из строя радиоэлектронной аппаратуры на значительном удалении от генератора. При этом такой импульс обладает хорошей проникающей способностью (благодаря использованию различных токопроводящих линий: металлических труб, вентиляционных шахт, линий связи и др., – импульс может распространяться на значительные расстояния), что позволяет использовать его генераторы для вывода из строя аппаратуры в защищенных пунктах управления и связи. Основная цель применения подобных средств поражения в Ираке – вывод из строя систем управления ПВО. Насыщенность данных систем электроникой, а также наличие высокочувствительных компонент в составе РЛС ПВО делает эти системы наиболее подходящей мишенью для микроволнового оружия. При этом, командование коалиционных сил относилось к применению этих боеприпасов с особой осторожностью, так как крылатые ракеты достаточно эффективно сбиваются средствами ПВО, а это могло привести к попаданию отдельных узлов и деталей принципиально нового средства поражения к противнику, а от него – в третьи страны, что привело бы к утрате США приоритета в микроволновом оружии [2].

Характерно, что за несколько месяцев до начала иракской кампании многими экспертами давались оценки, согласно которым по-

добные боеприпасы могли появиться не ранее 2005 г. Это позволяет говорить о том, что по итогам кампании 1999 г. против Югославии, в которой впервые были применены средства вывода из строя систем энергоснабжения типа графитовых бомб, руководством Пентагона было принято решение об интенсификации работ по созданию эффективного радиоэлектронного оружия [2].

Следует также отметить, что ряд потерь авиационной техники коалиционных сил был связан с отказом их электроники в результате применения США микроволнового оружия. Это может свидетельствовать о том, что технология микроволновых боеприпасов еще недостаточно отработана. Можно говорить также и о том, что еще не найдено эффективной защиты собственных электронных систем от воздействия микроволнового излучения [2].

В первые часы ведения операции средствам РЭБ союзников, несмотря на их усилия, не удалось нарушить коммуникации и каналы связи. Однако уже в последующие дни войны они нарастили средства подавления систем радиосвязи, за счет чего иракские соединения и части фактически были отрезаны от основных сил и длительное время находились без управления со стороны высшего военного руководства в Багдаде. В сложной радиоэлектронной обстановке иракское командование фактически утратило возможность координировать действия отдельных соединений и частей и влиять на ход и исход военных действий [95, 291].

В первой войне против Ирака проводимые информационно-технические воздействия на системы управления и связи зарекомендовали себя положительно. Так, во время проведения операции «Буря в пустыне» за счет разрушения здания в центре Багдада, принадлежавшего фирме AT&T и являющегося одним из центральных телекоммуникационных операторов, удалось фактически парализовать систему государственного управления Ирака. Данный положительный опыт был успешно развит и в операции «Шок и трепет», причем готовиться к проведению кибератак США стали заблаговременно до начала войны [95].

В системы ПВО, закупленные Ираком в одной из западноевропейских стран, были внедрены закладки типа «логические бомбы», в результате чего непосредственно во время войны эти системы не смогли быть задействованы [292].

С началом войны Пентагон и спецслужбы получили приказ вывести из строя системы связи, которыми пользовались иракские военные и правительство. Помимо взрыва вышек сотовой связи было

применено электронное подавление сигналов спутниковых терминалов и кибератаки на серверы иракских телефонных и телекоммуникационных компаний фиксированной связи. США также обратились за содействием к международным телекоммуникационным компаниям, попросив их отключить определенные транспортные каналы [95].

5.3.6. Информационно-психологические операции

В 2002-2003 гг. в интересах обоснования проведения военной операции против Ирака администрацией США была предпринята всемирная информационная операция с целью доказательства того факта, что режим С. Хусейна представляет опасность для международного сообщества. Ирак обвинялся в возобновлении разработки оружия массового поражения и в сотрудничестве с международными террористическими организациями, прежде всего с Аль-Каидой. Именно эта информационная операция по дискретизации Ирака в глазах мирового сообщества и формирование необходимого общественного мнения в пользу проведения военного вторжения позволили приступить к военным действиям без санкции ООН.

Сразу после окончания войны в Ираке начала работу «группа исследования Ирака», занимавшаяся поиском оружия массового поражения, предположительно скрывавшегося режимом С. Хусейна. В 2004 г. эта группа закончила свою работу, отметив в итоговом отчете, что к началу военной операции коалиционных сил Ирак не располагал оружием массового поражения.

В период подготовки и проведения операции союзных войск информационно-психологические операции планировались в целях выполнения следующих задач [95]:

- обеспечить одобрение и поддержку действий США и их союзников на международном, региональном и местном уровнях, представить США в качестве надежного, способного справиться с ситуацией защитника интересов мирового сообщества, свести до минимального уровня региональную поддержку Ирака;
- способствовать консолидации стран, поддерживающих войну с Ираком, и обеспечить тесное взаимодействие будущих многонациональных сил.

Решение перечисленных задач было возложено на оперативную группу. В нее входили подразделения 193-го авиационного крыла сил специальных операций ВС США и 4-й группы психологических

операций, в том числе ориентированного на Ближний Восток 8-го регионального батальона психологических операций, 9-го батальона тактических психологических операций, отдельных подразделений психологических операций для поддержки частей и соединений 18-го воздушно-десантного корпуса и командования специальных операций, а также батальона подготовки и распространения материалов психологических операций со штатными техническими средствами. Общая численность военнослужащих психологических операций в этой войне достигала 650 человек [95].

Стратегический план ведения психологической операции на период ведения боевых действий разрабатывался развернутой в штабе объединенного центрального командования ВС США оперативной группой из числа военных и гражданских специалистов 4-й группы психологических операций и был детализирован до тактического звена [95].

Накануне вторжения американцы провели широкомасштабную акцию: с помощью электронной почты были разосланы послания на арабском языке иракским генералам с призывами к невыполнению приказов С. Хусейна. В электронных сообщениях, составленных ведущими американскими военными психологами, подчеркивалось, что если граждане Ирака помогут предотвратить использование оружия массового поражения, то США сделают все необходимое, чтобы защитить их самих и членов их семей [95].

В этот же период, по данным информационного агентства Reuters, в офисы багдадских компаний и государственных учреждений поступили сотни посланий, направленных подразделениями психологических операций американской армии. В них содержалась просьба к иракскому населению накормить и вылечить потерявшихся солдат [95].

С первых дней войны командованием сил специальных операций использовались следующие формы психологического воздействия на войска и население противника [95].

1. Традиционные формы психологического воздействия – радио- и телевещание, устная и печатная пропаганда. Широковещательную радиопропаганду обеспечивали 10 развернутых в приграничных с Ираком странах наземных радиостанций. Непрерывное вещание пропагандистских передач осуществлялось с борта самолета EC-130E Commando Solo из состава 193-го авиакрыла Национальной гвардии ВВС США [95].

Среди мирного населения и военнослужащих ВС Ирака были распространены простейшие транзисторные радиоприемники, фиксированно настроенные на нужную частоту. Материалы для специальных передач готовились в объединенной редакции, состоявшей из саудовских, американских, египетских, кувейтских и британских специалистов психологических операций. За время конфликта в эфире прозвучали 3 250 выпусков новостей, 13 интервью с иракскими военнопленными, 40 пресс-релизов и интервью, а также около 190 материалов пропагандистского характера. Ежедневно, до 10 с половиной часов в сутки на территории приграничных с Ираком стран осуществляли радиовещание на арабском языке ретрансляторы программ «Голос Америки» и «ВВС» [95].

С началом боевых действий подразделения и части радиоэлектронной борьбы приступили к подавлению государственной радиостанции Ирака «Голос Багдада». В интересах радиопропаганды при вхождении в радиосети иракских подразделений широко использовались войсковые средства связи [95].

2. Видеопропаганда, которая осуществлялась путем широкого распространения видеокассет пропагандистского содержания. Основу их содержания составляли показ мощи американской армии, демонстрация новейшего вооружения, военной техники и высокой выучки военнослужащих многонациональных сил, а также критика режима С. Хусейна [95].

3. Устное вещание через передвижные звуковещательные станции, установленные на автомобилях высокой проходимости и вертолетах. В целях оказания тактической поддержки и принуждения иракских солдат к сдаче в плен командирам частей и подразделений многонациональных сил было придано в общей сложности 60 групп специалистов со звуковещательными средствами, которые действовали в интересах общевойсковых соединений и частей [95].

4. Печатная пропаганда – за время операции силами психологических операций было распространено свыше 30 млн экземпляров листовок. Основной способ их распространения – сброс агитационных авиабомб М129А1 с истребителей-бомбардировщиков F-16, самолетов ЕС-130Е и В-52 и с использованием других средств, в том числе воздушных шаров и т. п. [95].

Листовки разрабатывались специалистами 4-й группы психологических операций американских вооруженных сил и, по замыслу авторов, должны были разъяснять цели и задачи военной операции США, побуждать иракских военнослужащих к отказу от участия в бо-

евых действиях, доказывать неизбежность поражения иракского режима, разгрома иракских войск, побуждать иракцев к сотрудничеству с коалиционными силами и отказу от разрушения инфраструктуры страны [95].

Об объеме и эффективности такого воздействия можно судить и по таким данным: во время боевых действий в зоне Персидского залива на войска и население Ирака было сброшено более 30 млн листовок. 98% военнослужащих Ирака, сдавшихся в плен, заявили, что видели и читали листовки, 88% поверили в их содержание, 70% сдались по этой причине в плен [95].

5. Специально разработанная программа по работе с военнопленными в развернутых объединенным центральным командованием лагерях, а также на корпусных и дивизионных пунктах сбора пленных привлекались иракские перебежчики, дезертиры и диссиденты. Кроме того, с целью деморализации военнослужащих ВС Ирака Пентагон активно осуществлял широкомасштабную программу подготовки специалистов по работе с местным населением из числа добровольцев. С декабря 2002 г. на территории Венгрии велась подготовка людей, отобранных из проживающих в Европе и США арабов, негативно настроенных по отношению к режиму С. Хусейна. На начальном этапе войны эти специалисты были переправлены в Ирак для ведения активной информационно-пропагандистской деятельности против правящего режима и распространения в стране печатных, аудио- и видеоматериалов соответствующего содержания. Согласно планам Пентагона подобную подготовку в общей сложности должны были пройти 3 тыс. человек [95].

После завершения боевых действий часть личного состава подразделений психологических операций привлекалась к работе по организации деятельности средств массовой информации в местных администрациях. Таким образом, по оценкам аналитиков Пентагона, силы психологических операций внесли значительный вклад в достижение поставленных целей и обеспечение решения поставленных в ходе войны в Ираке задач.

5.3.7. Основные просчеты США и их союзников при ведении военных действий

Просчеты военно-политического руководства, разведки и войскового командования армии Соединенных Штатов Америки и их союзников по ОВС блока НАТО в планировании операции «Шок и тре-

пет» («Свободу Ираку») рассматриваются, главным образом, по результатам анализа и обобщения содержания работ [291, 294, 295, 296, 297, 298, 299].

1. Военно-политическое руководство США недооценило политику Турции по очень важному курдскому вопросу. В результате турки – верный партнер США по блоку НАТО – заняли жесткую позицию и запретили использовать свою территорию для создания северного фронта в операции против Ирака. Командование США вынуждено было направить 70-тысячный войсковой контингент в обход, через Суэцкий канал, в целях укрепления южного фронта. При этом были потеряны три недели, в течение которых американские войска практически бездействовали [291].

В результате отказа сопредельных с Ираком государств поддержать операцию «Шок и трепет» ее пришлось начинать только с территории Кувейта. При этом концентрация войск осуществлялась на ограниченной площади, начинать и вести наступление с которой оказалось весьма неудобно. Более того подготовка наступательной операции велась в ограниченные сроки. Летчики, артиллеристы и ракетчики не знали, какие цели и когда необходимо поражать. В результате в первые дни проведения сухопутной операции войска завязли в приграничных боях. Первоочередные стратегические задачи: рассечь Ирак по линии Насирия – Амара, собрать ударную группировку в междуречье Тигра и Евфрата (для наступления на Багдад) и нарушить военное и политическое управление – выполнить не удалось [291].

2. Операцию «Шок и трепет» заблаговременно объявили победной. Англо-американцы были убеждены, что иракцы не смогут оказать сопротивление войскам коалиции. Между тем прогнозы военно-политического руководства США на молниеносную войну («блицкриг») против Ирака оказались недостаточно обоснованными. При первых же столкновениях «высокоорганизованной армии союзников, вооруженной современной высокоэффективной техникой» с «необученной и морально подавленной» армией Хусейна, которая воюет старым советско-китайским оружием» (так, по крайней мере, ее описывали военные эксперты США), армии союзников увязли в боях и получили неожиданный для них отпор [298].

На полях сражений не было сцен массовой капитуляции военнослужащих Ирака и восстания иракского населения, как об этом писала американская пресса. Однако известны многочисленные случаи, когда иракцы, вооруженные техникой 70-х г., совершали рейды на

коммуникации союзников, растянутые на более чем 500 км, и наносили серьезные потери войскам коалиции [291].

3. Имела место ошибочная оценка военно-политического состояния Ирака на момент начала войны. Данный просчет подтверждают результаты первых двух недель ведения войны, которые оказались весьма неожиданными для командования союзных войск. Вполне понятно, что такой просчет был допущен разведывательными органами США. При всей мощной оснащенности и высоких технических возможностях систем, комплексов, средств и органов разведки они не смогли выявить военную инфраструктуру страны, не уяснили социально-политической обстановки в ней и в целом не вполне представляли, «с кем имеют дело». Провал работы американской разведки привел к существенным ошибкам военного командования в планировании сухопутной операции и, вполне естественно, породил «цепную реакцию проблем» военного и политического характера, ввергнувших страну в хаос практически сразу же после окончания активной фазы боевых действий [291].

4. Основываясь на неточных, часто ложных разведывательных данных, военное командование коалиции недооценило способность иракской армии к сопротивлению. Командование союзников недооценило боеспособность армии Ирака, в частности, численность сил, готовых оказать сопротивление, и уровень их технической оснащенности. Как следствие, в данный регион был направлен недостаточный контингент войск. По оценкам российских военных экспертов, в сухопутной операции в Ираке действовало примерно 40% от необходимого количества живой силы и техники. В результате военное командование коалиции было вынуждено дополнительно направить в район боевых действий еще порядка 100 тыс. военнослужащих. Это примерно столько же, сколько было направлено изначально.

Так, только в ходе операции потери коалиционных сил составили [298]:

- по людям: убитыми – до 487 чел., ранеными – 1621 чел., пропавшими без вести – 103 чел., пленными – 19 чел. (всего – 2330 чел.);
- по технике: танков – 118 ед., БМП (БТР) – 170 ед., автомобилей – около 100 ед., орудий – 12 ед., самолетов – 15 ед., вертолетов – 22 ед., БПЛА – 9 ед. (всего – 446 ед.).

К тому же 40% бронетехники коалиции пострадало в результате стрельбы иракской артиллерии. Современные танки Abrams и Challenger иракцы подбивали из гранатометов, выстрелами ПТУР, а также

подрывали на минах и ослепляли пулеметным огнем. Подчеркнем: все отмеченное выше убедительно подтверждает положение о том, что войну выигрывают все-таки люди, прежде всего за счет полевой выучки, морально-психологического и духовного состояния солдат и офицеров, их стойкости, мужества, грамотных и решительных действий непосредственно на поле боя [291].

5. Переоценка возможностей своих аэромобильных сил и морской пехоты по выполнению боевых задач в наземной операции. Попытки американского командования организовать и провести воздушно-наземную операцию силами аэромобильных частей закончились неудачей. Массированного применения вертолетов как отдельного рода войск не получилось. Поэтому уже на четвертые сутки аэромобильные части были распределены по группировкам и включены в состав наступающих войск в качестве подразделений разведки, огневой поддержки и сдерживания противника. К тому же организация, вооружение и боевая техника формирований аэромобильных сил и морской пехоты не были приспособлены для ведения ими длительных наземных операций в качестве «обычных» сухопутных войск. Как следствие, основная нагрузка легла на «тяжелые» механизированные и бронетанковые соединения [291].

6. Недостаточная оценка (прогноз) эффективности применения новых образцов вооружения и боевой техники войск коалиции в реальных условиях региона ведения боевых действий. Во всех предшествующих войнах США побеждали противника только путем применения Tomahawk и «умных» бомб, что создало эффект победной эйфории. Поэтому для военно-политического руководства страны и войскового командования «скромно» оказался в стороне и не был учтен тот факт, что ВС в тех войнах (операциях, боевых действиях), «оказывается», не участвовали. Новая война в зоне Персидского залива неожиданно изменила отношение англо-американских стратегов к высокоточному оружию, на которое они делали основную ставку. Несмотря на то, что высокоточное оружие проявило себя с самой лучшей стороны непосредственно на поле боя – оно поражало тактические цели с большого расстояния, но, с учетом его стоимости (стоимость крылатой ракеты как морского, так и воздушного базирования оценивается примерно в один миллион долларов), означает «стрельбу из пушки по воробьям». Поэтому коалиция, после расхода 70% запаса крылатых ракет морского базирования, вынуждена была повысить интенсивность боевого применения авиации, ствольной и реактивной артиллерии, а также других огневых средств сухопутных войск [291].

7. Войска союзников несли неожиданные небоевые потери от дружественного огня. Данный просчет указывает на неслаженность действий войск – чаще всего американцы попадали по британцам. Имел место и чрезмерный расчет на электронику. Кроме того, системы распознавания «свой-чужой» часто выходили из строя в условиях песчаной бури. Инциденты, получившие официальное название «дружественный огонь», происходили почти каждый день. Имел место случай, когда иракская разведывательно-диверсионная группа, находясь неподалеку от колонны войск союзных сил, вышла в эфир. Радиоисточник сразу же запеленговали, подготовили необходимые данные для удара и осколочно-фугасными артиллерийскими снарядами поразили своих военнослужащих [291].

8. Упущена задача поддержания боевого духа войск, которая усугублялась слабыми действиями тыла коалиционных сил. Партизанские рейды иракцев, которые действовали в значительно растянутых тылах войск коалиции, наносили ей существенный урон. Это вынуждало союзников задействовать часть войск для охраны колонн снабжения. Имело место и массовое недовольство солдат качеством новых армейских пайков. Неожиданно остро встал вопрос о сигаретах – нехватка табака в боевых условиях, «оказывается», снижает и без того не самый высокий боевой дух англо-американцев. К тому же в формированиях войск союзников отсутствовали штатные медицинские подразделения, способные проводить более серьезные процедуры, чем первая медицинская помощь. Это привело к чрезмерному использованию авиации при эвакуации. Например, из 1 300 эвакуированных военнослужащих (более 110 самолето-вылетов) только 50 действительно нуждались в серьезной медицинской помощи [291].

9. Формирования ВС США и их союзников не были готовы к решению не свойственных им задач по наведению порядка, локализации и усмирению массовых выступлений гражданского населения и предотвращению мародерства после окончания активных боевых действий [291].

Таково главное содержание основных просчетов, допущенных военно-политическим руководством, разведкой и командованием коалиционных сил в операции «Шок и трепет» («Свободу Ираку»), которые затруднили ведение боевых действий.

Основные выводы, вытекающие из просчетов. На современном этапе развития вооруженной борьбы для успешного ведения боевых действий настоятельно необходимы [291]:

- новые и эффективные системы, комплексы и средства, прежде всего управления, связи, разведки, навигации, РЭБ, информационного противоборства, огневого, ядерного и иного поражения объектов вероятного противника;
- новые методы, способы и подходы к построению систем военного назначения;
- совершенствование тактики ведения боевых действий, ее адекватность обстановке и адаптация к условиям ТВД и операционных направлений;
- новые методы (способы, приемы) работы должностных лиц всех специальностей и уровней иерархии управления;
- адаптация к конкретным условиям ведения боевых действий аэромобильных частей, формирований, оснащенных высокоточным оружием и другими новыми техническими средствами;
- новые подходы к «человеческому фактору» и исключение возможности ведения стрельбы (нанесения ударов) по своим войскам;
- новые, адекватные обстановке, методы (способы, приемы) защиты коммуникаций, войск, систем и информации;
- своевременная, хорошо продуманная, адекватная и адаптивная в отношении динамично изменяющейся обстановки система всестороннего обеспечения подготовки и ведения военных (боевых) действий в условиях определенных ТВД и операционных направлений;
- правильно построенная, адекватно и адаптивно действующая система устрашения противника, включающая интеллектуальное, волевое, информационное, психологическое, моральное, духовное и иное, подкрепленное необходимыми и достаточными силовыми атрибутами и высоким уровнем патриотизма.

Представленные выводы необходимо своевременно (заблаговременно) и неукоснительно учитывать практически, в том числе в условиях реальной подготовки и ведения любых современных операций. При этом особое внимание следует уделять воздушной, космической, морской и наземной составляющим – достаточной обеспеченности и требуемой эффективности управления, связи, разведки, навига-

ции, радиоэлектронного подавления и радиоэлектронной защиты, информационного, интеллектуального, психологического, технического, технологического и иного противоборства, маскировки, введения разведки противника в заблуждение, а также всех (разнообразных) средств поражения его объектов [291].

5.3.8. Основные выводы

По итогам операции в Ираке можно сделать вывод, что в настоящее время ВС США и ведущих зарубежных стран НАТО практически отработали вопросы организации и ведения операции (боя) и нанесения ударов по противнику поэтапным или одновременным применением ударных сил (войск), высокоточного оружия, средств РЭБ с одновременным проведением мероприятий стратегической и/или оперативной (тактической) маскировки, дезинформации и психологической войны [95].

Анализ применения оружия показывает постоянно растущую роль авиации и высокоточных крылатых ракет различных видов, особенно морского базирования (КРМБ) в военных действиях, а следовательно, и необходимость повышения эффективности средств противовоздушной и ракетно-космической обороны. Так, в операции 1991 г. «Буря в пустыне» за 40 суток воздушной кампании были применены 282 высокоточные крылатые ракеты. В 1999 г. наземная группировка альянса, развернутая в Албании и на территории Македонии, – 26,6 тыс. человек, была в 20 раз меньше по численности, чем в войне с Ираком. Вместе с тем за 78 суток воздушно-морской наступательной операции авиация НАТО совершила 35 тыс. боевых вылетов, выпустив более 1000 КРВБ и КРМБ, преимущественно с американских носителей. В операции 2003 г. «Лиса в пустыне» всего лишь за четверо суток было применено 425 крылатых ракет. Налицо рост применения высокоточных КР за сутки военных действий в 15 раз. Во второй войне в Персидском заливе интенсивность применения высокоточных КР, особенно КРМБ, резко возросла. По имеющимся данным за первые трое суток войны против Ирака применено около 1000 высокоточных КРМБ, в основном по объектам столицы Ирака – Багдада [269].

Следует подчеркнуть, что роль высокоточных КРМБ и КРВБ при проведении воздушно-космической операции, со временем будет возрастать. В табл. 5.4 приведен вариант расчетов по определению доли составных элементов в первой операции воздушно-космического

нападения (ВКН). Как видно из табл. 5.4, основная роль в достижении целей ВКН принадлежит военной авиации – до 60% объема решаемых задач, вслед за ней идут высокоточные КРМБ и КРВБ [269].

Таблица 5.4. Соотношение сил и средств ВКН в операции [269]

Общее количество сил и средств, привлекаемых к 1-й операции ВКН (%)	**Из них по элементам общей структуры 1-ой операции ВКН (%)**				
	ТА и палубная авиация	**Стратегическая авиация**	**КРМБ, КРВБ**	**БР с ОБЧ**	**Силы и средства обеспечения, в т.ч. КА; самолеты ДРЛО**
100	до 50	до 10	до 20	до 1-2	до 18

Необходимость информационного обеспечения массированного применения высокоточных средств диктует необходимость создания и поддержания постоянно действующей космической инфраструктуры, включающей необходимое количество КА различного назначения. Именно космическая инфраструктура составит системообразующую основу разведывательно-ударных боевых систем воздушного и морского базирования, способных без предварительной подготовки наносить массированные высокоточные удары по объектам любого государства в любом регионе нашей планеты [173].

Опыт войн показывает необходимость трансформации средств ПВО и ПРО, так как одной из основных задач обороны страны от воздушных средств нападения становится эффективное поражение высокоточных КРМБ и КРВБ в условиях активного противодействия средств РЭБ и массированного применения оружия, самонаводящегося на излучение. Решение задач ПВО-ПРО является чрезвычайно трудными, учитывая, что эффективная поверхность рассеивания (ЭПР) КРМБ и КРВБ в настоящее время составляет около 0,05 кв. м, что в 4000 и в 50 раз меньше ЭПР самолета В-52 и самолета В-1 соответственно. Это резко снижает дальность обнаружения КРМБ и КРВБ РЛС, что, в свою очередь, отрицательно сказывается на эффективности применения истребительной авиации, зенитно-ракетных комплексов (ЗРК) и зенитной артиллерии (ЗА) по их поражению. Кроме того, отдельной важной задачей ПВО в войнах будущего является надежное обнаружение, а затем эффективное поражение самолетов, выполненных по технологии Stealth (например, типа F-117A) [269].

Анализ результатов локальных войн в зоне Персидского залива, на Балканах, в Афганистане и Ираке свидетельствует о том, что

РЭБ трансформируется в один из основных элементов современных войн и наиболее значимую силу информационных операций. РЭБ как основа противоборства с ПВО и системами боевого управления противника становится неотъемлемой частью вооруженного противостояния любого масштаба. Поражающее и подавляющее воздействие сил и средств РЭБ по эффективности сопоставимо, а иногда и превосходит эффективность традиционных средств вооруженной борьбы. Основным принципом организации и ведения радиоэлектронной борьбы в военных операциях является целенаправленное использование позитивных и неблагоприятных факторов, возможностей и характерных особенностей, присущих объектам, системам управления, боевой технике, оружию и личному составу противника, в целях завоевания информационного превосходства [95].

В соответствии с оценками результатов учений, проводимых Министерством обороны США с целью выяснения потребности ВС в телекоммуникационных услугах, в случае одновременного участия ВС США в вооруженных конфликтах высокой интенсивности на двух ТВД суммарная пропускная способность линий связи, включая принадлежащие Минобороны системы спутниковой связи и арендуемые коммерческие линии дальней связи как космические, так и наземные (подводные), должна составлять не меньше 50 Гбит/с. Ежегодный прирост потребностей Минобороны США в среднем будет равен 15% от уровня предыдущего года. По другим оценкам потребность Минобороны в телекоммуникационных услугах в 2010 г. для обслуживания двух ТВД достигала 100 Гбит/с.

Основной объем передаваемой информации будет приходиться на данные тактической разведки (изображения, видео, данные для планирования боевых действий), которые составят около 57% от всего информационного потока ВС. Следующий основной потребитель телекоммуникационных ресурсов – автоматизированные системы управления войсками на ТВД и системы автоматизированного управления оружием. На их долю приходится около 31% трафика.

Обмен информацией с высшим военно-политическим руководством государства будет составлять 4%. На информацию боевого обеспечения приходится 3%. Обмен информацией с системами управления и оповещения стратегического звена составит 1%, прочий объем трафика – 4%. На долю ТВД будет приходиться около 48% от общего информационного потока ВС. Трафик с ТВД на континентальную часть США составит 35%, а передача информации с территории США на ТВД – около 17%.

Однако распределение потоков информации в значительной степени зависит от условий и характера (сценариев) ведения боевых действий. Существенно вырастет значение систем спутниковой связи. Анализ распределения используемых линий связи для информационного обеспечения абонентов (таблица 5.5) показывает, что именно на них придется основная нагрузка при передачи информации.

Таблица 5.5. Вклады родов связи в управление (по объемам передаваемой информации) [273]

Спутниковая связь	более 50-60%
Радиорелейная связь	до 18-22%
Тропосферная связь	до 12%
КВ-, УКВ-радиосвязь	до 5-6%

Пропускная способность спутниковых линий связи в случае участия ВС США одновременно в двух вооруженных конфликтах на разных ТВД по состоянию, например, на 2010 г., составляла 4 Гбит/с. При этом большая часть трафика будет приходиться на арендуемые системы незащищенной широкополосной широковещательной спутниковой связи, предназначенные для вторичного распределения разведывательной информации, графической информации, изображений и видеозаписей [291].

5.4. Операции США и НАТО «Одиссея. Рассвет» и «Союзный защитник» в Ливии в 2011 г.

Оценивая итоги военных операций «Одиссея. Рассвет» и «Союзный защитник», проведенных в Ливии в 2011 г., можно констатировать абсолютное техническое превосходство США и стран НАТО в космической группировке, средствах РЭБ, крылатых ракетах морского и воздушного базирования, навигационных системах в оперативном и тактическом звене.

Ливийская война имеет много отличий от предшествующих войн, проведенных США и НАТО. Но, как и в предыдущих войнах, основу сил, проводящих операцию, составили ВВС и ВМФ, а также активное использованное ими ВТО. Вместе с тем особенностью конфликта стало дальнейшее развитие методов сетецентрической войны, в частности:

- применение мобильных групп сил специальных операций и частных военных компаний в ВС оппозиции;

- ведение сухопутной «шоссейной войны» в условиях высокой разведывательной осведомленности и существенной поддержки с воздуха;
- широкое использование средств информационного воздействия на силы противника как в технической, так и в психологической сфере;
- использование способов финансовой блокады и шантажа для достижения военных и политических целей.

Именно в Ливии был введен в оборот термин «шоссейная война». В «шоссейной войне» тактика против мятежников или «логика пустынной войны» сводилась к следующему: «наскок – удар – быстрое отступление без линии сплошного фронта». Также специфическими условиями войны были отсутствие фронта и тыла, маскировка под ополчение для максимального приближения, уничтожение заправочных станций, диверсионные действия, оборона оазисов, ограничение поставок военного снаряжения, боеприпасов и горючего для формирований оппозиционеров, уничтожение грузов на границе с Тунисом и Чадом. Среднестатистическое боевое столкновение в Ливии было сражением силами двух-трех армейских рот, максимум батальона [314].

5.4.1. Реализация концепции управляемого хаоса при дезорганизации государственного управления

Военно-политическая обстановка в Ливии начала обостряться в середине февраля 2011 г., вслед за волной состоявшихся антиправительственных выступлений населения в ряде арабских стран Ближнего Востока и Северной Африки. В результате этих событий были свергнуты президенты Туниса Б. Али и Египта Х. Мубарак, а также отправлены в отставку ряд правительств в других странах. 15 февраля 2011 г. массовые антиправительственные выступления синхронно начались в г. Бенгази и в ряде других городов Ливии, включая столицу страны г. Триполи. Демонстранты требовали ухода ливийского лидера М. Каддафи и его окружения, а также осуществления в стране перемен. Синхронность этих выступлений и их координация через сеть Интернет с самого начала говорила о том, что в Ливии имеет место не спонтанное развитие событий, а результат длительной подготовительной работы, проведенной в основном вне страны в соответствии с концепцией управляемого хаоса. По оценки ряда экспертов, антиправительственные выступления в Ливии (как, впрочем, и в других араб-

ских странах) были тщательно спланированы, подготовлены и запущены в интересах Франции и некоторых других западноевропейских государств. Последующие события явились заранее запрограммированной реализацией ливийской «арабской весны», согласованной Францией с США и странами НАТО [309].

Основанием того, что именно Франция является вдохновителем, организатором и наиболее активным участником военной операции НАТО в Ливии, более чем достаточно. Так, в июле 2011 г. президент Франции Н. Саркози в интервью СМИ указал, что происходящее в Ливии – это французская война, т.е. ведущаяся главным образом французами, по их инициативе и во имя их собственных интересов [309].

Стремительное обострение внутриполитической обстановки в Ливии в феврале-марте 2011 г. оказалось неожиданным именно для ливийских властей и первоначально оказало деморализующее воздействие на государственные структуры и институты, а также на часть ливийского общества. Ряд ливийских политиков, военных и чиновников поспешили отказаться от верности М. Каддафи и переметнулись в лагерь оппозиции. При этом не исключено, что с этими перебежчиками давно общались и вели переговоры западные спецслужбы. При активном участии иностранных спецслужб и военных советников многонациональной коалиции создавались вооруженные формирования оппозиции. Их основу составляли: представители силовых структур, перешедшие на сторону оппозиции; молодежь; боевики различных исламистских группировок. Благодаря усилиям Запада и его союзников в арабском мире общая численность военизированных формирований оппозиции к маю 2011 г., по различным оценкам, достигла 10-11 тыс. человек. При этом активные боевые действия в составе оппозиционных отрядов вели военнослужащие западных и арабских государств. Притом, что если в начале конфликта они представляли собой фактически сборища необученных и слабо вооруженных людей, которые в основном сотрясали воздух демонстративной стрельбой и непрерывно отступали, то уже через пару месяцев они смогли переломить ситуацию в другую сторону. Имеющаяся информация позволяет утверждать, что одну из главных ролей в таких «превращениях» сыграли силы специальных операций и частные военные компании (наемники) из Великобритании, Франции, Италии и США [309, 310, 311].

Ливийские власти в условиях массовых акций гражданского неповиновения и провокаций со стороны воинских формирований оппозиции, когда обычными правоохранительными мерами стабилизи-

ровать обстановку не удалось, прибегли к применению против «оппозиции» национальных вооруженных сил, включая боевую авиацию. Это позволило начать информационную компанию по дискредитации режима М. Каддафи в глазах мирового сообщества под лозунгами, что последний ведет войну против собственного народа [309, 310].

Информационные атаки на М. Каддафи и развернутая в мире кампания дезинформации о ливийских событиях были настолько агрессивными и широкими, что ввели в заблуждение даже многих крупных мировых политиков, выступивших с заявлениями, осуждающими нынешний ливийский режим за «непропорциональное» применение силы, нарушения прав человека и т.д. Никто даже не попытался глубоко разобраться в сути происходивших событий, причинах столь быстрого обострения обстановки, источниках и происхождении оружия у оппозиции и принадлежности членов боевых отрядов оппозиции [309].

В результате под давлением информационных операций, проводимых западными СМИ, 17 марта 2011 г. Совет безопасности ООН принял резолюцию № 1973 об объявлении ливийского воздушного пространства бесполетной зоной и об ужесточении экономических санкций против Ливии (точь-в-точь, как в случае с Ираком). А уже 19 марта 2011 г. заблаговременно созданные коалиционные силы (США, Великобритания, Франция, Италия, Канада, Бельгия, Испания, Дания, Норвегия, Катар) начали против Ливии военную операцию, получившую напыщенное название «Одиссея. Рассвет». Общее управление операцией на ее начальном этапе осуществлялось объединенным командованием ВС США «Африком» [309].

К 31 марта 2011 г. западной коалиции не удалось ни физически уничтожить ливийского лидера, ни сломить его решимость сопротивляться агрессии до конца. В условиях затягивающихся безрезультатных боевых действий США решило дистанцироваться от непосредственного участия в боевой части операции и уступили общее командование коалиционными силами НАТО. В НАТО отказались от американского названия операции и придумали свое – «Союзный защитник». Данная операция проводилась с 31 марта по 31 октября 2011 г. [309].

Военная операция НАТО «Союзный защитник» проводилась в форме воздушной операции по блокированию и изоляции воздушного пространства Ливии, воздушных ударов по войскам, военным объектам и объектам стратегической инфраструктуры, центрам высшего государственного и военного управления страны. Со стороны среди-

земноморского побережья Ливия была блокирована военно-морскими силами США и НАТО, осуществляющими досмотр гражданских судов в целях недопущения поставок в Ливию оружия, боеприпасов и товаров двойного назначения. Также важной задачей НАТО являлось оказание воздушной поддержки вооруженным формированиям ливийской оппозиции, которая по замыслу НАТО должна самостоятельно вести сухопутные операции и в итоге взять власть в стране под свой контроль [309].

5.4.2. Реализация концепции обезоруживающего удара

Воздушная и морская группировки НАТО сыграли ключевую роль в ливийской военной операции. К ее началу, в марте 2011 г., в относительной близости от ливийских берегов была создана крупная группировка ВВС и ВМФ. Группировка включала в себя 316 самолетов из 14 государств: США – 153, Великобритания – 28, Франция – 29, Швеция – 8, Бельгия – 6, Канада – 11, Дания – 4, Норвегия – 6, Турция – 7, Нидерланды – 7, Иордания – 12, ОАЭ – 8, Катар – 8 [305]. Помимо этого, в состав авиационной группировки вошли самолеты разведки и радиоэлектронной борьбы RC-135, EC-130Y, EC-13J, EA-18G, базовой патрульной авиации P-3 Orion, а также заправщики КС-135Р и КС-10А [95].

В состав ВМС союзников вошли 39 боевых кораблей, подводных лодок, не считая вспомогательные суда 2-го и 6-го флотов США, из девяти государств Западной коалиции: США –12, Великобритания – 3, Франция – 6, Бельгия – 1, Канада – 1, Нидерланды – 1, Румыния – 1, Болгария – 1, Греция – 1. В том числе 3 корабля ВМС США с ракетами Tomahawk на борту и, включая авианосец Enterprise, десантные вертолетоносцы Kearsarge и Ponce, а также флагманский (штабной) корабль Mount Whithney [305].

С началом операции 20 боевых кораблей ВМС НАТО осуществляли морскую блокаду Ливии, контроль международного судоходства на предмет соблюдения другими странами эмбарго на поставки для Триполи оружия и другой продукции военного назначения. За это время остановлено для досмотра и проверки 1700 гражданских судов. В 122 случаях на остановленные суда высаживались досмотровые группы, восьми кораблям было приказано сменить курс [309].

США провели у ливийского побережья с начала марта 2011 г. военные маневры, в ходе которых корабли и самолеты 6-го флота

ВМС США пересекали в заливе Сидра линию морской границы Ливии. Учения кораблей 6-го флота США в ночь с 20 на 21 марта 2011 г. сопровождались групповыми ракетно-авиационными ударами по отдельным объектам на территории Ливии, в частности по городу Триполи и близлежащим населенным пунктам [305].

Первый ракетно-авиационный удар по территории Ливии состоял из трех волн налета. В последующем ракетно-авиационные удары трансформировались в серии, которые наносились как в ночное, так и в дневное время суток.

Главной целью союзников стали [305]:

- зенитно-ракетные системы С-200 ВЭ (по терминологии НАТО SA-5, Gammon), способные поражать цели на расстоянии до 240 км, размещенные в двух местах, которые позволяли Ливии контролировать полеты американских самолетов системы AWACS и противолодочных Р-3 над заливом Sidraa, который Ливия рассматривала как свои территориальные воды;
- около 12 батарей (до 132 пусковых установок) зенитно-ракетного комплекса С-125 «Печера-2М»;
- семь полковых комплектов (140 боевых машин) самоходных ЗРК «Квадрат».

Выбор таких первоочередных целей был обусловлен тем, что по предварительным данным Пентагона ПВО Ливии представляла собой серьезную угрозу для иностранных военных самолетов, находящихся в воздушном пространстве Ливия или рядом с ним. В дальнейшем коалиция атаковала не только объекты ПВО, но и объекты, относящиеся к системе военного и государственного управления. Атаки были произведены на ВС М. Каддафи, строения материально-технического обеспечения и склады амуниции, а также командные пункты [305].

Нанесение ракетно-авиационного удара по Ливии началось с боевого применения крылатых ракет морского и воздушного базирования. Всего 19 марта 2011 г. корабли ВМС США и Великобритании выпустили 112 крылатых ракет Tomahawk, уничтожив, как было заявлено, 20 из 22 подвергавшихся ударам целей [305].

В последующем пуски крылатых ракет стали производиться в значительно меньшем количестве. В качестве целей для поражения крылатыми ракетами выступали [305]:

- штабы ВС Ливии;

- правительственные пункты управления и резиденция М. Каддафи;
- штаб ВВС Ливии в Матейге к востоку от г. Триполи;
- база ВВС Ливии Аль-Гардабия (или Гардабия – Ghardabiya);
- узлы связи и базы ВМС, расположенной недалеко от аэропорта г. Шурт;
- радары раннего предупреждения ливийской системы ПВО и объекты связи;
- места дислокации и позиции войск, лояльных М. Каддафи;
- крупные пункты управления и связи военного и административного назначения в различных районах страны;
- мобильные батареи противокорабельных ракет.

Пуски крылатых ракет морского базирования осуществлялись из районов восточной части Средиземного моря с надводных кораблей и подводных лодок США и Великобритании. Tomahawk были выпущены с пяти американских кораблей – 2 крейсеров и 3 подводных лодок, входящих в группу ВМС США, действовавшую в Средиземном море (удаление от береговой линии 50-150 км) [305].

В ходе операции ВВС США и НАТО в боевых условиях впервые была применена тактическая крылатая ракета Tomahawk Block IV (TLAM-E). Данной модернизированной версией 30-летней ракеты были вооружены американские и британские корабли [306].

Стратегическая авиация, представленная бомбардировщиками B-2, использовалась для поражения наиболее важных целей на территории Ливии 2 000-фунтовыми управляемыми бомбами GBU-31B/JDAM. По данным штаба ВВС США все запланированные цели были поражены с заданной точностью. Самолеты B-2 нанесли удары по главному ливийскому аэродрому недалеко от Триполи, поразив управляемыми авиабомбами укрепленные ангары, в которых находились истребители и бомбардировщики ливийских ВВС. B-2 сбросили 40 бомб на этот стратегический объект. Бомбардировщики находились в полете 25 часов и 4 раза дозаправлялись топливом в воздухе. Подтверждение об уничтожении ливийского аэродрома экипажи бомбардировщиков получали после выполнения боевой задачи от средств разведки. Общая высокая эффективность применения самолетов B-2 была достигнута за счет возможности корректировки полетного задания и перепрограммирования экипажами бомбовой нагрузки на другие цели, осуществлявшихся в реальном масштабе времени. Ко-

мандование ВВС США считает, что B-2 были наиболее эффективны для действий на удаленных ТВД [305].

Особенностью стратегического использования ВВС НАТО явилось применение им уранового бронебойного оружия. Боеприпасы с обедненным ураном применялись, в основном, в первые сутки операции в Ливии, за короткое время американцы сбросили 45 бомб и выпустили более 110 ракет по ключевым ливийским городам, в которых проживало много мирных жителей. Вес некоторых бомб, сброшенных на Ливию, составлял около двух тонн [306].

Тактическая и палубная авиация ВВС и ВМС США и Великобритании, Франции и Италии также принимала активное участие в нанесении ударов как по Триполи, так и по другим объектам Ливии. Тактическая авиация США и НАТО совершала полеты с основных баз, расположенных в пяти странах: Франции, Италии, Великобритании, Кипре и Крите. Штурмовая авиация на начальном этапе операции совершала полеты с авианосцев в основном с северного, северо–западного и западного направлений [305].

Атака французских и американских ВВС протекала по стандартной схеме «предварительная разведка – создание постоянного поля контроля самолетами ДРЛО – выдвижение в район целей – постановка помех на рубежах ливийской ПВО – распределение целей – удар – отход» [306].

Самолеты Tornado наносили удары крылатыми ракетами Storm Shadow, для чего преодолевали расстояние в 3 000 миль туда и обратно, действуя с баз в Великобритании. Таким образом, рейд британских самолетов по своей протяженности стал самым длинным со времен войны с Аргентиной из-за Фолклендских островов в 1982 г.

В ночь с 20 на 21 марта 2011 г. был применен один из самых совершенных самолетов ВВС стран Запада – многоцелевой истребитель Eurofighter Typhoon ВВС Великобритании. В дальнейшем в ходе операции в Ливии отрабатывались различные тактические сценарии для этих самолетов, и прежде всего по обеспечению лазерного целеуказания выбранных для поражения наземных целей. Хотя летчики самолетов Typhoon, участвующие в операции «Объединенный защитник», способны осуществлять автономное лазерное целеуказание наземных целей, большинство боевых вылетов производилось парами – в составе самолетов Typhoon и Tornado, где один из самолетов осуществлял целеуказание, а второй применял оружие по назначенной цели. Это позволило авиационному командованию задействовать широкий арсенал авиационных боеприпасов, сохраняя более дорогостоя-

щее высокоточное оружие для выполнения задач, где необходимо было обеспечить минимальные побочные разрушения [306].

С 29 марта 2011 г. также впервые применены в боевых условиях тяжеловооруженный самолет поддержки сухопутных подразделений AC-130U [306].

ВВС Франции опробовали в Ливии высокоточные авиационные бомбы AASM (Armement Air-Sol Modulaire). При ударе по наземным целям в Ливии 19 марта 2011 г., эти бомбы были впервые применены для уничтожения колонны бронетехники в районе Бенгази в восточной части страны. Бомбы AASM также применялись для уничтожения зенитного ракетного комплекса С-125 советского производства, когда они были сброшены с самолета за пределами зоны его эффективного действия.

В общем, при проведении операции в Ливии ВВС Франции применили свыше 1600 авиационных средств поражения (АСП), включая авиабомбы и управляемые ракеты. В их числе 225 модульных АСП AASM, сброшенных с самолетов Rafale. Эти АСП были оснащены инерциально-спутниковой системой наведения с инфракрасной ГСН, функционирующей на конечном участке траектории [310].

Интенсификация применения авиации потребовала активного использования самолетов-заправщиков. Во время воздушной операции американские самолеты-заправщики C-135FR, Великобритании Vickers VC10 и Lockheed TriStar (RAF) постоянно барражировали над территорией Ливии, что обеспечивало круглосуточные действия авиации над Ливийской территорией [306].

В ночь на 4 июня 2011 г. силы НАТО впервые применили в боевых условиях вертолеты Apache ВВС Великобритании, базирующиеся на вертолетоносце Ocean, а также французские Tiger и Gazelle. Операция управлялась центром воздушных операций НАТО, который базируется на юге Италии. В дальнейшем основная нагрузка по огневому поражению легла на боевые вертолеты АН-64 Apache, вооруженные вакуумными ракетами Hellfire AMG-114N. Целями вертолетов являлись объекты, склады вооружения, заметные в различных диапазонах спектра – видимом, ИК, радиолокационном. Вертолеты действовали в темное время суток на предельно малых высотах (не более 50 м), применяя ракетное и артиллерийское вооружение. При нанесении воздушных ударов вертолетами многократно использовалось высокоточное оружие. По оценке командования многонациональных сил использование боевых вертолетов оказало существенное деморализующее

воздействие на личный состав правительственных войск Ливии. Одновременно снизились затраты на поражение целей [306, 310].

Общими итогами реализации концепции обезоруживающего удара силами ВВС являются следующие. В ходе операции «Объединенный защитник» с 31 марта по 31 октября 2011 г. интенсивность задействования авиации международной коалиции в Ливии составила 26 500 самолето-вылетов. Из этого числа 9 700 вылетов были боевыми. Воздушные удары по Ливии после 1 июля велись со средней интенсивностью 80-100 самолето-вылетов. В отдельные сутки число боевых вылетов доходило до 140 и более. Удельный вес числа боевых самолето-вылетов в общем числе самолетовылетов коалиционных сил составлял не более 30-35%. Это свидетельствует о возрастающем объеме задач обеспечения боевых действий в воздухе (разведка, РЭБ, целеуказание, боевое управление, дозаправка в воздухе, доставка грузов и т.д.). Однако фактически большинство полетов с пометкой «боевой вылет» выполнялось в условиях отсутствия авиации и средств ПВО. Самолеты союзников, как правило, действовали с высот и расстояний, не позволяющих эффективно применять средства ПВО. США и НАТО за последние 40 лет накопили громадный опыт борьбы с системами ПВО, выстроенными на основе устаревших советских комплексов С-75, С-125 и С-200. Такая система ПВО успешно подавлялась Израилем в Ливане и силами США и их союзников в Ираке и Югославии. Таким образом, такую систему ПВО можно практически бесполезной против современных вооруженных сил [306].

5.4.3. Достижение информационного превосходства за счет использования современных средств связи, управления, разведывательного обеспечения

Для обеспечения непрерывного наблюдения над зоной управления боевыми действиями в качестве сил дальнего радиолокационного обнаружения и управления (ДРЛОиУ) НАТО NAEW&CF (НАТО Airborne Early Warning and Control Force) действовали летательные аппараты Е-3D ВВС Великобритании, совместно с самолетами ДРЛОиУ Е-3А AWACS из состава сил НАТО Е-3А, французским Е-3F и машинами ВВС США Е-3В/С.

Первый самолет ДРЛОиУ был задействован в воздухе над ливийским театром военных действий 26 февраля 2011 г. при эвакуации из Ливии нефтяных специалистов и рабочих Великобритании. С апреля, когда началась военная операция, самолеты ДРЛОиУ налетали

около 1000 ч, что соответствует почти 105% изначально планировавшегося времени [305].

На предварительном этапе операции было задействовано как минимум 5 самолетов-разведчиков стран НАТО. Самолеты электронной разведки RC-135 Rivet Joint перехватывали радиопереговоры ливийских военных и передавали полученную информацию на БПЛА Global Hawk. Этот БПЛА наводил аппаратуру слежения на место расположения бронетанковых частей и определял его примерные координаты. В некоторых случаях и сами БПЛА первыми обнаруживали движущиеся цели. Затем Global Hawk передавал координаты аналитикам в наземном центре, а те отправляли данные на командный пункт для выдачи целеуказания. Оттуда координаты поступали на самолет ДРЛОиУ E-3 Sentry AWACS, который, в свою очередь, наводил на цели истребители F-16 и Harrier, а также другие боевые самолеты или БПЛА. Никогда ранее подобное количество разнородного современного ВВТ не использовалось столь интенсивно и комплексно в ходе одной военной кампании. Данное обстоятельство предъявило к качеству функционирования систем управления, и прежде всего систем автоматизации управления, связи и разведки тактического звена, исключительно высокие требования [305].

Вся операция сопровождалась усиленной работой системы радиоэлектронной разведки в круглосуточном режиме. Основная нагрузка легла при этом на Центр радиоэлектронной разведки (ЦРР) Франции (г. Мутциг, Эльзас). Именно на 44 отдел этого центра легла основная тяжесть обеспечения наведения на цель самолетов не только ВВС Франции, но и всего альянса. При этом 1, 2 и 5 отделы занимались сбором информации и анализом всего диапазона частот, помогая тем самым координировать удары и отслеживать перемещение войск ливийского режима. С середины марта 2011 г. объектами атак авиации стали передающие станции GSM-стандарта. Здесь в дело включились станции слежения, которые располагались в районе Сан-Лоран-де-ля-Саланк во французских Пиренеях. Их работа позволяла отслеживать поврежденные и вновь заработавшие передатчики в Ливии и тем самым корректировать нанесение авиаударов.

После разрушения основных узлов связи ливийская армия перешла на использование радиосвязи на высоких частотах. Здесь вновь вступил в действие ЦРР в г. Мутциг, который на тот период времени являлся единственным задействованным подразделением, который был в состоянии работать на этих частотах. Его антенны собирали в круглосуточном режиме информацию от источников северных райо-

нов Ливии. В указанной работе было задействовано более 20 отделов центра. Вся полученная информация направлялась незамедлительно в Центр сбора и изучения информации (CF3E) военной разведки на базе ВВС Крейл севернее г. Парижа. Там происходил ее окончательный анализ и данные поступали на посты тактического действия, которые уже и принимали окончательное решение о нанесении ударов. Ровно такая же схема была задействована и во время операции сил НАТО в Косово. Как показывает и та, и другая операции, данная схема явно не является оптимальной. Ливийской армии уже после нанесения основной массы авиаударов к середине лета, по данным Пентагона, удалось сохранить до 60% парка своей тяжелой техники. При этом надо учитывать, что авиация НАТО действовала фактически без всякого отпора со стороны ливийской ПВО. Из этого следует, что в случае активного задействования ПВО КПД авиации был бы на порядок меньше. Вместе с тем, анализ радиоперехватов не позволяет понять суть переговоров и готовящихся маневров противника (здесь обычно используется «эзопов язык» или местный диалект), а лишь определить место выхода станции в эфир. С учетом описанной иерархии передачи информация очень быстро устаревала. К этому надо добавить сложности и длительность перевода. Кроме того, здесь существуют свои «секреты» в виде использования ретрансляторов ограниченной мощности с направленной диаграммой направленности, которые довольно надежно маскируют местоположение абонента. Это особенно эффективно при использовании небольших мобильных групп в условиях пустыни [307].

В Ливии были опробованы новые средства организации взаимодействия между американскими, английскими и итальянскими информационными системами, в частности прием разведывательных данных от самолетов GR-4A Tornado (Великобритания), оснащенных контейнерной разведывательной станцией RAPTOR, американскими средствами приема и обработки разведывательной информации [314].

Разведывательно-поисковыми группами в звене «взвод-рота» были применены и единые тактические терминалы JTT-B, которые позволяют в реальном масштабе времени отображать получаемые по спутниковым и наземным каналам связи данные на электронной карте, выводимые либо непосредственно на собственный терминал, либо на экран подключенного к нему портативного компьютера. Это позволяло максимально использовать системы управляемого оружия, применение которых основывалось на данных, получаемых по каналам связи

в реальном масштабе времени от КРНС NAVSTAR, а также средств радиоэлектронной и оптической разведки [314].

5.4.4. Использование беспилотных и робототехнических средств

В ходе всей войны широко применялись беспилотные летательные аппараты. В альянсе посчитали, что их применение позволит наносить более точные удары, нежели те, на которые способны истребители [306].

Беспилотные летательные аппараты стали применяться в ходе ливийской кампании в 20-х числах апреля 2011 г. В их задачи входил сбор информации о противнике, а также нанесение ракетных ударов, разведка и доразведка целей, наблюдение за полем боя. БПЛА постоянно транслировали картину боя в реальном масштабе времени на экраны самолетов ДРЛОиУ E-3 AWACS. Для этого, в частности, привлекались американские беспилотные летательные аппараты Global Hawk и средства космической разведки. Остальные вылеты приходились на ведение разведки, патрулирование бесполетной зоны и полеты транспортной авиации. Однако, по оценке офицеров ВВС НАТО, количества БПЛА, принимавшего участие в операции, было недостаточно для обеспечения должного качества воздушной разведки и наблюдения [306].

Большую часть времени в ливийском небе находилось одновременно два американских БПЛА: MQ-1B Predator (дальность полета 740 км, продолжительность полета до 40 ч, практический потолок 7 600 м) и RQ-4 Global Hawk (практический потолок около 18 км, продолжительность полета до 30 ч) [306].

Широкое использование БПЛА для разведки целей, определения их местоположения и идентификации, оперативной выдачи целеуказания для применения ВТО и авиации, а также для контроля эффективности ударов позволило обоснованно обеспечить долю применения управляемых боеприпасов до 85% [306].

В результате наращивания количества БПЛА на втором этапе операции значительно повысилось качество разведки наземных целей. Кроме того, задействование американских стратегических разведывательных БПЛА Global Hawk позволило решать разведывательные задачи без захода в зону поражения огневых средств ливийских правительственных войск. Одновременно использование разведывательно-ударных БПЛА США Predator показало, что подобные образцы во-

оружения являются наиболее перспективными для применения в будущих конфликтах и войнах. Данные аппараты американцы активно использовали для уничтожения объектов на территории Ливии на протяжении всей военной кампании, хотя формально США на втором ее этапе непосредственного участия в боевых действиях не принимали [310].

5.4.5. Достижение информационного превосходства за счет применения средств радиоэлектронной борьбы и информационно-технических воздействий

Основной задачей сил в начальный период операции РЭБ было подавление систем и средств ПВО, предшествовавшее ее уничтожению ударами крылатых ракет и авиацией. В дальнейшем подразделения РЭБ сконцентрировались на нарушении функционирования радиолокационных систем вооружения сухопутных войск, а также систем управления войсками за счет подавления линий связи, а также радио- и телеретрансляторов в районах, лояльных к М. Каддафи.

К решению задач РЭБ при проведении операции были привлечены самолеты разведки и радиоэлектронной борьбы RC-135, EC-130Y, EC-13J, EA-18G, EP-3E. Их основная задача – подавление средств ПВО Ливии как с использованием аппаратуры РЭБ, так и с применением противорадиолокационных ракет Harm [305].

Впервые в боевых условиях в ходе операции был применен палубный самолет радиоэлектронной борьбы EA-18G Growler ВМС США. Как считают западные военные, во многом благодаря ему ни один американский, французский или британский самолет не был сбит ливийской системой ПВО. По сообщению вице-адмирала Б. Гортни (Bill Gortney), самолет EA-18G Growler не только справился с ливийскими ракетами «земля-воздух», но и помог повстанцам отбить нападение сухопутных войск правительства Ливии. Судя по всему, EA-18G Growler смог подавить коммуникации правительственных войск и парализовать вполне современные мобильные зенитные ракетные комплексы Crotal и «Оса», которые уцелели после ударов ракетами Tomahawk. Этот самолет также использовался для создания помех работе радаров для поддержки действий штурмовиков морской пехоты AV-8B Harrier против ливийских танков [306, 308].

Анализ результатов применения средств РЭБ показывает, что можно прогнозировать дальнейшее развитие массированного их применения, которые, начиная уже с войн США в Персидском заливе, за-

действуются в форме массированного радиоэлектронного удара. При этом основными способами действий сил и средств РЭБ являются: подавление источников любого электромагнитного излучения и всей системы радиоэлектронных средств; защита своих источников радиоэлектронного излучения; радиоэлектронное прикрытие от ударов носителей ВТО на маршрутах полета и в районах их применения [310].

В ходе войны в Ливии получили свое дальнейшее развитие приемы кибероперациий. Специалисты Пентагона в области кибервойны заблаговременно провели серию информационно-технических операций, позволивших им получить доступ к сети сотовой связи операторов Ливии, а также провести мониторинг телефонов, принадлежащих военнослужащим ливийской армии. В период, предшествующий операции, а также во время ее проведения это позволило проводить рассылки sms-сообщений и осуществлять прямые телефонные звонки на личные и служебные номера офицеров ливийских вооруженных сил с рекомендациями прекратить поддержку своего «скомпрометированного и обреченного на крах лидера», а также попытками убедить влиятельных ливийцев перейти на сторону оппозиции. Нередко послания включали и прямые угрозы: «У нас имеются GPS-координаты вашего командного пункта. Эти координаты запрограммированы в ракету Storm Shadow. Что вы собираетесь делать?». Ранее подобный метод воздействия применялся против правительственных войск в Ираке, где доказал свою эффективность [95].

Помимо этого с помощью кибернетических технологий осуществлялись оперативные действия в закрытых правительственных компьютерных сетях, а также телекоммуникационных системах критической инфраструктуры страны (прежде всего, энергообеспечения). По оценкам отдельных экспертов, степень информационно-технического доступа в телекоммуникационные системы Ливии достиг такой степени, что в любой момент основные системы жизнеобеспечения страны могли быть парализованы за счет их внешнего управления со стороны спецслужб США [95].

5.4.6. Информационно-психологические операции

По сообщениям зарубежной печати в ходе операции Пентагоном во взаимодействии с коалиционными войсками активно применялись силы и средства психологических операций. Доказательством тому является боевое применение самолета EC-130J Commando Solo из состава 193-го авиакрыла сил специальных операций США, с борта

которого велись радиопередачи на арабском, английском и французском языках, адресованные работникам портов и экипажам торговых судов и военных кораблей Ливии. Информация о применении сил и средств психологических операций в Ливии была косвенно подтверждена в ходе пресс-конференции начальника Объединенного штаба вооруженных сил США вице-адмирала Б. Гортни, который сообщил, что коалиционными силами в Ливии используются «специальные самолеты» [95].

В передачах, адресованных сухопутным подразделениям ливийской армии, содержались следующие требования: «Немедленно покиньте свои позиции. Режим М. Каддафи нарушает резолюцию ООН об окончании военных действий в вашей стране. Если вы немедленно оставите позиции, вам не будет причинен вред. Не пытайтесь глушить наши передачи» [95].

Пропагандистские радиопрограммы, которые транслировались силами психологических операций на частотах, используемых в вооруженных силах Ливии, решали конкретные тактические задачи. Командному составу вооруженных сил Ливии внушалась мысль о «преступной деятельности» режима М. Каддафи, от них требовалось прекратить боевые действия в районе конкретных населенных пунктов. В противном случае звучали угрозы командирам ливийской армии предстать перед международным трибуналом. В передачах для солдат акцент делался на эмоциональные способы психологического воздействия. Женский голос спрашивал ливийского солдата: «Почему, мой сын.., почему ты убиваешь наших людей?» А плачущий ребенок говорил: «Папа, ты мне нужен. Я не хочу, чтобы ты убивал детей. Я не хочу, чтобы ты убивал других отцов. Детям нужны их отцы. Папа, хватит воевать, пожалуйста, иди домой! Я жду тебя» [95].

Наряду с телерадиовещанием одной из основных форм информационно-психологического воздействия являлась печатная пропаганда. Авиация коалиции неоднократно распространяла листовки над населенными пунктами и позициями правительственных войск в Ливии. Основным содержанием разработанных органами психологических операций США печатных информационно-пропагандистских материалов было [95]:

- запугивание ливийских военнослужащих угрозой смерти, склонение их к прекращению боевых действий, дезертирству, оставлению оружия и боевой техники при отступлении;

- дискредитация ливийского лидера М. Каддафи – показ «незаконности и преступности» его действий, лишение его поддержки со стороны широких масс населения и военнослужащих;
- пропаганда военного превосходства сил коалиции;
- показ неизбежности поражения ливийского режима и бесполезности сопротивления.

Листовки, написанные на арабском языке, представляли собой простые (по оценкам специалистов, даже примитивные) агитационные материалы, призывающие «прекратить атаки против мирных ливийцев». Призывы «прекратить атаки» в листовках были совмещены с угрозами «..или вы будете уничтожены». По словам официального представителя военного командования операции, только к середине мая 2011 г. авиация распространила над территорией Ливии более 14 млн листовок [95].

5.4.7. Использование сил специальных операций и наемников

В Ливии были развернуты подразделения «спецназа» общей численностью около 50 человек – 30 военнослужащих из 22-го полка специальной авиадесантной службы SAS и полка специальной разведки SRR (Special Reconnaissance Regiment) [314].

Части и подразделения сил специальных операций Англии, Франции, Италии, ОАЭ и Катара приступили к активным действиям задолго до начала активной фазы воздушной операции. Их заброска в тыл ливийских войск осуществлялась как аэромобильным способом с десантированием личного состава непосредственно вне населенных пунктов для выполнения специальных задач, так и под «легендированием под журналистов», для чего большая часть СМИ Европы, Америки и Канады предоставила им прикрытие [314].

Бойцы британской SAS до начала активной фазы ливийской операции успели «публично» отметиться на территории Ливии, как минимум, два раза. Первый раз это было довольно удачно, так как удалось провести успешную эвакуацию британских граждан вскоре после начала массовых беспорядков. Второй «публичный» эпизод оказался малоприятным для британских SAS – группа их военнослужащих была задержана ливийскими повстанцами возле г. Бенгази [314].

Специальные операции спецслужб ЦРУ, МИ-6 и других западных стран по «оказанию военной помощи» привели к появлению «оп-

позиционных сил» и началу столкновений повстанцев с властями. Представитель НАТО 24 сентября 2011 г. по телеканалу CNN заявил, что «…британские, французские, иорданские и катарские «спецназовцы» в Ливии в течение последних дней начали активную фазу действий в Триполи и других городах, чтобы содействовать продвижению повстанцев». Кстати, именно спецназ британцев и французов разрабатывал план штурма Триполи и координировал действия повстанческих отрядов [314].

В период активной фазы операции точность определения координат целей, оперативность нанесения ударов, эффективное целеуказание не могли быть реализованы лишь исключительно одними космическими и авиационными средствами разведки. Поэтому значительный объем задач по обеспечению ракетно-авиационных ударов, особенно в ходе непосредственной авиационной поддержки, был выполнен с участием авианаводчиков из подразделений сил специальных операций [311, 314].

Спецназ также обеспечивал военные самолеты данными о целях для нанесения ударов и проводил разведывательные операции в г. Триполи. Штурм правительственного комплекса «Баб-аль-Азизия» ливийскими повстанцами возглавляли военнослужащие спецназа ОАЭ и Катара. Штурм ливийской дипломатической миссии под прикрытием бронетранспортера осуществили бойцы болгарского спецназа. Разведывательные подразделения НАТО следили за перемещениями М.Каддафи и навели авиацию на его кортеж. Таким образом, применение подразделений сил специальных операций позволило НАТО не задействовать в операции многочисленные боевые бригады, которые могли бы «увязнуть» в проведении наземных боевых действий [314].

В условиях ограниченной боеспособности военных формирований оппозиции блоком НАТО были предприняты меры по широкому использованию в военной операции частных военных компаний (наемников). Фактически по количеству наемников и частных военных организаций война в Ливии стоит на одном из первых мест. Так как наемники зачастую являлись бывшими военнослужащими спецназа Великобритании и Франции, четко отличить их от действующих военнослужащих специальных войск было очень сложно. В частности, ряд бывших военнослужащих SAS, которые после «якобы увольнения» поступили на работу в частные военные компании в Ливии, также участвовали в боевых действиях в этой стране. «Наемники» из частных военных компаний получили задачу выявить в г. Триполи самого М. Каддафи и членов его семьи и ликвидировать их. В среде повстан-

ческих рядов было так много британских и французских военных специалистов, что было не совсем понятно – офицеры ли они регулярной армии или отставники, нанятые министерством обороны или частной компанией в государственных интересах [314].

При этом реально в составе Переходного национального совета (ПНС) оппозиции участвовали три группы компаний военных услуг наемников. Первые, настоящие частные армии, непосредственно планировали и проводили боевые операции в интересах клиента. Вторые как консалтинговые компании обучали войска и консультировали ПНС. Третьи как логистические компании, осуществляли тыловую поддержку, строительство и обслуживание сложных систем вооружений [314].

В середине марта 2011 г. британское министерство обороны признавало, что 600 наемников, осуществлявших военные операции в Афганистане по линии частной охранной компании Black Watch, готовы к вторжению в Северную Африку [312].

К лету 2011 г. на территории Джамахирии уже присутствовали полноценные военные соединения наемников, занятые как обучением повстанцев, так и непосредственным участием в боях. В конце мая 2011 г. военные аналитики отмечали, что основными игроками на ливийской «площадке» стали тесно связанные с военной разведкой Франции фирмы Secopex (с представительством в Бенгази) и Safety & Security Solutions Group (зона действия – Мисурата). Помимо чисто разведывательных операций и обучения повстанцев обе структуры были задействованы и в доставке «гуманитарных грузов» (и не только) в Бенгази и Мисурату с Мальты. Логистику обеспечивает другая частная французская фирма Prolage, которая располагает собственными торговыми кораблями. За общую координацию их работы отвечали бывшие офицеры французской армии [312].

Большое внимание уделялось привлечению к военным операциям наемников из арабских стран, в частности из Иордании. Делалось это потому, что боевики, говорящие по-арабски, гораздо лучше ориентировались в обстановке и вызывали меньше подозрений, чем французы и англичане. По мнению журналиста газеты Asia Times П. Эскобара (Pepe Escobar), решающую роль в боях за Триполи 23-25 августа 2011 г. сыграли формирования из иорданских, колумбийских, британских и южноафриканских наемников [312].

5.4.8. Экономическое противоборство

Экономическая блокада северо-западной части страны в сочетании с авиационными и ракетными ударами по тыловым базам, а также замораживание финансовых активов ливийского правительства способствовали быстрому истощению запасов важнейших материальных средств и росту недовольства среди населения, проживавшего на территории, подконтрольной М. Каддафи, что во многом ускорило крах его режима. Как полагают на Западе, задействование финансово-экономических рычагов, включая расширение практики подкупов и шантажа влиятельных лиц, позволяет экономить значительные средства [314].

Уникальность Ливийской войны заключается и в том, что не менее эффективно, чем боевые действия, использовались финансовый подкуп и финансирование побега генеральских семей. В XXI веке это уже вторая операция (после Ирака), где финансовым оружием достигался прогресс, сопоставимый с эффектом воздушной операции [314].

НАТО в условиях, когда воздушная операция не дала возможности мятежникам захватить власть, пошли по другому пути. Основные усилия были сосредоточены на действиях ЦРУ, разведки и спецназа Франции, Великобритании и Италии. Этими действиями, в том числе, были и подкуп военных и дипломатов. Уже известно, что итальянская разведка вывезла в Италию семьи пяти генералов правительственных войск Ливии. Также итальянскими разведчиками была проведена работа примерно со 100 ливийскими военнослужащими. Таким образом, переход сухопутных частей на сторону оппозиции и случаи дезертирства военных летчиков на Мальту вместе с самолетами являются вполне закономерным следствием этой работы [314].

Так, А.Ф. Юнис, один из соратников М. Каддафи в революции 1969 г., все 40 лет слыл «человеком №2» в неформальной табели о рангах и более 20 лет в чине генерала армии бессменно занимал пост министра внутренних дел, считаясь «сторонником самого жесткого курса по отношению к оппозиции». Однако 22 февраля 2011 г. он дезертировал (официально считается, что «ушел в отставку») из г. Триполи и перешел в г. Бенгази, уведя с собой лично созданные им подразделения военной полиции [314].

В феврале 2011 г. ливийские военные разделились. Только часть армейских подразделений остались лояльными М. Каддафи, остальные же примкнули к повстанцам под воздействием финансовых предложений альянса или просто дезертировали. С мая 2011 г. офице-

ры бросали свои подразделения, исчезая в неизвестном направлении, а среди солдат, не понимающих за что они воюют, началось повальное дезертирство. При этом недовольство большой части ливийских военнослужащих и успешность финансовых операций было вызвано еще и тем, что М. Каддафи выделял среди них «своих» и соответственно платил им больше [314].

5.4.9. Основные просчеты при ведении военных действий

1. ***Невозможность достичь цели операции за приемлемое время.*** Увеличение времени проведения военной кампании с запланированных трех до семи месяцев показало неспособность Североатлантического союза организовать и провести в короткие сроки военную операцию против государства с ограниченными оборонными ресурсами. Это свидетельствует о переоценке альянсом своих возможностей, сил оппозиции и недооценке способности к сопротивлению режима М. Каддафи. Несмотря на огромные силы блока НАТО, задействованные в операции в Ливии, к лету 2011 г. Франция, Великобритания и США так и не смогли достичь окончательной победы над сторонниками М. Каддафи. Само полугодовое сопротивление ливийского народа является редким примером обороны против внешней агрессии заведомо превосходящего противника. Стоит напомнить, что режим С. Хусейна в Ираке, располагая несравненно более крупными военными возможностями, не продержался и нескольких недель [310, 312].

К середине лета 2011 г. исход ливийской кампании был далеко не однозначен. По оценкам ряда наблюдателей, в том числе бывшего руководителя французской разведки DST И. Бонне (Yves Bonnet), находившегося в течение месяца с миротворческой миссией в Ливии в июне-июле 2011 г., более трети ливийцев поддерживали М. Каддафи. На территориях, контролируемых его сторонниками, несмотря на военные действия, поддерживался образцовый порядок, позволивший Бонне назвать эти зоны «государством закона» [312].

Губительно сказались на итогах войны в Ливии для ЕС и НАТО завышенные представления о собственной армии, ее мощи и боеспособности, ведь М. Каддафи смог сопротивляться достаточно длительное время. При оценке обстановки в части, касающейся вопросов состояния и возможных действий противника, было недооценено морально-психологическое состояние ливийских войск. Руководство США и НАТО предполагало, что после первых ударов армия

М. Каддафи развалится, произойдет массовая сдача в плен. Но, несмотря на серьезные потери, бойцы сохранили свою боеспособность [312].

Ливийская армия образца марта 2011 г. и образца августа 2011 г. – это сильно отличающиеся по тактике, умениям и храбрости войска. Они очень быстро многому научились в ходе боев. Таким образом, задача, стоявшая перед НАТО и США по уничтожению фактически боевой мощи своего противника, осталась невыполненной. НАТО и США не смогли установить полный контроль над побережьем и западной территорией Ливии [312].

2. ***Эффективное использование ливийскими ВС старых и современных маскировочных технологий.*** Вполне вероятно то, что современные маскировочные технологии армия М.Каддафи смогла приобрести на нелегальных рынках оружия. Большую часть тяжелой боевой техники полковнику М. Каддафи удалось уберечь от бомбежек, заранее спрятав ее в гигантских подземных лабиринтах самой протяженной в мире ирригационной системы, имеющей официальное название «Великая рукотворная река». Ливийский «Водостан», находящийся на большой глубине и простирающийся на 4000 км в пустыне, стал «Великой искусственной рекой», которую М. Каддафи построил за 25 млрд долларов [314].

Еще одним «сюрпризом» стала полная неосведомленность разведки НАТО и США о приемах маскировки боевой техники. По использованию информационных технологий американская армия считается самой передовой в мире. Ее разведывательные центры непрерывно перерабатывают огромные объемы информации, поступающие со спутников и беспилотных разведчиков. Но тем не менее летчики Франции и Италии признавались, что сбрасывали бомбы на неизвестные объекты. Наличие подобной системы укрытия является одной из причин того, что наземные силы ливийской армии практически не понесли потерь [314].

Фактически итоги войны доказали, что старые маскировочные технологии способны обманывать и сводить на нет современные высокотехнологичные средства космической и воздушной разведки [314].

3. ***Недостаток ресурсов разведывательного обеспечения на первом этапе операции.*** Серьезной проблемой для многонациональных сил в начале операции явилось отсутствие в регионе необходимых средств разведки. В подобной ситуации органы военного управления альянса имели ограниченные возможности для идентификации назем-

ных целей и оценки результатов нанесения по ним авиационных ударов. При этом командование авиационной группировкой стран коалиции часто не располагало достоверными сведениями о поражаемых объектах, что привело к нанесению ударов по уже уничтоженным либо ложным целям. Такая ситуация позволила М. Каддафи длительное время сохранять значительное количество бронетанковой техники, складов вооружения и ГСМ, а также тактических ракет типа Scud. В результате сложившегося положения командование группировки к началу второго этапа кампании вынуждено было принять меры по усилению разведывательного обеспечения боевых действий. С этой целью в район кризиса были направлены дополнительные разведывательные самолеты и БПЛА, а также усилена агентурная разведка на территории Ливии [310].

4. ***Удары «по своим» силам и мирным жителям Ливии.*** НАТО в последние годы уделяло много внимания внедрению технических средств для исключения потерь от «дружественного» огня. Тем более странным и непростительным для ВС с самыми современными средствами разведки были факт авиаударов по мирным жителям и своим войскам в условиях почти полного отсутствия противодействия [313].

Вот лишь несколько примеров. Жертвами бомбардировки самолетов НАТО в районе г. Марса-эль-Брега, расположенного в 800 км к востоку от г. Триполи, стали двое повстанцев и двое врачей, 14 пострадали и 6 пропали без вести. В ходе одного из ракетных ударов вертолетов НАТО в пригороде Бенгази была уничтожена инфраструктура одной из частных французских военных компаний. Сколько людей погибло, в результате этой атаки не сообщалось, но известно, что их тела были сразу переправлены во Францию военным вертолетом [313].

8 августа 2011 г. ракеты упали на жилые дома и больницу в деревне Маджер под Злитаном (160 км к востоку от Триполи). Погибли 20 мужчин, 32 женщины и 33 ребенка [313].

По данным Ливийского общества Красного креста более 1100 мирных граждан были убиты в результате бомбежек НАТО, включая 400 женщин и детей. Всего с 19 марта 2011 г., когда начались бомбардировки, по 26 мая 2011 г. было зафиксировано 718 погибших и 4067 раненых мирных жителей, 433 из которых получили тяжелые ранения. Как недавно признал министр здравоохранения Ливии, в ходе гражданской войны с обеих сторон погибли не менее 30 тысяч человек (по другим оценкам 50 тысяч), свыше 50 тыс. человек было ранено, около

4 тыс. считаются пропавшими без вести. Все эти цифры весьма приблизительные, корректироваться они будут, вероятнее всего, в сторону увеличения [313].

5. ***Наличие внутренних военных и политических противоречий в блоке НАТО.*** Следует отметить, что в ходе операции коалиционных сил в Ливии в НАТО выявился ряд внутренних военно-политических проблем. В частности, государствам – членам альянса не удалось достичь консенсуса по вопросу о необходимости проведения военной операции. Отдельные страны блока отказались выделять свои войска для участия в боевых действиях, рассматривая военную активность Франции, Великобритании и США как стремление решить свои внешне- и внутриполитические задачи за счет других союзников [310].

Кроме того, значительными проблемами для НАТО стали неравномерность затрат и различный уровень участия в боевых действиях государств – членов альянса. Около 60% финансовых расходов пришлось на Францию и Великобританию. При этом после окончания военной кампании резко обострилась конкурентная борьба между союзниками по НАТО за доступ к углеводородным ресурсам и контроль за формированием новых властных структур в Ливии [310].

6. ***Дестабилизация региона после окончания операции.*** Завершение военной операции не привело к стабилизации военно-политической ситуации в Ливии и регионе в целом. Фактически можно констатировать, что в результате действий многонациональных сил в Ливии развитие ситуации в этой стране происходит по «иракскому сценарию». Вместо одного «одиозного» диктатора появилось множество неконтролируемых экстремистских группировок, деятельность которых способна привести к дальнейшей дестабилизации обстановки в регионе [310].

5.4.10. Основные выводы

Действия НАТО по «урегулированию» ливийского кризиса продемонстрировали ряд новых моментов в организации и проведении военных операций по разрешению кризисных ситуаций. Это обусловлено как специфичным характером современных кризисов, так и возросшими военными возможностями западных стран, прежде всего США. Кроме того, особенностью операции в Сирии стало дальнейшее развитие концепции «сетецентрической войны» и перенос ее методов в сферу политического и экономического противоборства [310].

Непосредственно военная операция коалиционных сил имела новые отличительные черты сетецентрических войн: бесконтактные военные действия без задействования сухопутных группировок войск; массовое применение высокоточного оружия; проведение операций информационного противоборства [310].

Однако в части планирования и непосредственного проведения военной операции необходимо отметить, что ливийский кризис продемонстрировал «громоздкость» существующих в НАТО на стратегическом уровне механизмов принятия коллективных решений на применение военной силы. Так, процедура согласования подходов союзников к разрешению ливийской проблемы заняла около месяца. При этом основная дискуссия развернулась вокруг вопроса об организации руководства коалиционной группировкой войск [310].

Операция подтвердила также отсутствие в странах альянса, за исключением США, необходимых для ее проведения средств связи и разведки стратегического уровня. Недостаток таких систем у европейских членов блока вынудил коалицию использовать в течение всей военной кампании американские силы и средства. Подобная ситуация сложилась и со стратегическими разведывательными самолетами, беспилотными летательными аппаратами и с высокоточным оружием. Данные проблемы стали прямым следствием растущего разрыва между боевыми возможностями вооруженных сил США и остальных стран НАТО. Кроме того, это свидетельствует о неспособности альянса самостоятельно, без участия США, проводить продолжительные операции. Подтверждением этому являются и меры, реализуемые руководством блока по итогам проведенной военной кампании. Так, принято решение о внесении изменений в программу развития военно-технических возможностей НАТО «Разумная оборона», предусматривающих наращивание современных видов ВВТ в странах альянса, а также более тесную координацию их деятельности в этой области [310].

Следует отметить, что, несмотря на возникшие проблемы политического характера, странам коалиции удалось за счет находящихся в регионе формирований в короткие сроки развернуть в районе кризиса довольно крупную группировку войск. Этому способствовала созданная как в Европейской зоне, так и в Средиземноморье соответствующая военная инфраструктура. Одновременно принятая в альянсе «военная» стандартизация обеспечила своевременную ротацию и эффективное использование многонациональных объединений и частей [310].

Коалиционные силы сумели обеспечить внезапность нанесения первых ударов по ливийским объектам (фактически сразу после принятия СБ ООН резолюции), однако статистические данные об эффективности боевого применения группировки указывают на достаточно низкий уровень результативности ее действий. В частности, количество самолето-вылетов коалиционной авиации было соразмерно численности правительственных войск (на двух военнослужащих армии М. Каддафи пришлось по одному самолето-вылету). Необходимо отметить, что самолеты часто возвращались на аэродромы с неизрасходованным боекомплектом. Возникали проблемы оперативно-технической совместимости авиационных средств связи, особенно на начальном этапе. В результате этого французские и американские летчики вынуждены были действовать только в своих зонах ответственности [310].

Управление силами и средствами на тактическом уровне в течение всей операции осуществлялось по национальным планам, что значительно осложняло координацию их действий с другими национальными контингентами. В рамках этих планов широко применялись подразделения сил специальных операций, морской пехоты, а также армейской авиации. Особенностью боевого применения сил специальных операций являлось то, что оно проводилось на ливийской территории незаконно и скрытно, так как выходило за рамки принятой СБ ООН резолюции по Ливии, и велось под прикрытием частных военных компаний и сил оппозиционных военных формирований. Следует отметить, что подразделения сил специальных операций сыграли основную роль в захвате ключевых населенных пунктов, в том числе и столицы страны – г. Триполи. При этом боевые вертолеты на протяжении всей операции оказывали непосредственную огневую поддержку как спецподразделениям стран коалиции, так и отрядам оппозиции. Активное использование сил специальных операций и частных военных компаний для подготовки отрядов оппозиционных сил и их консультирование по боевому применению способствовало достижению целей боевых действий без применения группировок сухопутных войск [310].

Следует отметить высокую эффективность применения беспилотных летательных аппаратов. В результате наращивания их количества значительно повысился уровень разведки наземных целей. Использование разведывательно-ударных БПЛА показало, что подобные образцы вооружения являются наиболее перспективными для применения в будущих конфликтах и войнах [310].

Важное место в ходе ливийской кампании занимали вопросы организации всестороннего обеспечения войск (сил). При этом затягивание конфликта на фоне финансово-экономического кризиса, охватившего подавляющее число основных стран-участниц коалиции, вызвало значительные проблемы с поставками высокоточных авиационных средств поражения и горюче-смазочных материалов. В частности, после 1,5 месяца ведения боевых действий запасы авиационных боеприпасов в ВВС Франции сократились до критического уровня, что вынудило руководство Министерства обороны ввести режим экономии боеприпасов и приступить к экстренным закупкам управляемых ракет и бомб [310].

Еще одним фактором, негативно влиявшим на военные возможности НАТО, явилась психологическая неготовность западных государств к войне. Одним из основных требований стран, выделивших силы и средства для участия в военной кампании, было исключение боевых потерь, что, в свою очередь, вело к снижению эффективности боевого применения авиации [310].

Оценивая в целом опыт ливийской кампании, следует отметить, что в ходе ее проведения на практике были отработаны способы ведения бесконтактной вооруженной борьбы высокоточными средствами авиации и ВМС в сочетании с массированным применением средств радиоэлектронной борьбы, сил специальных операций, задействованием потенциала частных военных компаний, использованием мобильных возможностей тыла. Результаты такой оценки показывают, что с появлением в ВС основных государств НАТО высокоточного оружия дальнего действия в количествах, достаточных для ведения крупномасштабной войны, разгром противника как одна из важнейших целей всех войн прошлого может достигаться лишь нанесением массированных ударов ВТО по его объектам стратегического значения. Что касается живой силы противника, то она может не подвергаться огневому воздействию. Удары будут наноситься также по важнейшим объектам государственного управления и экономики на всю глубину территории противостоящей стороны. В этих условиях отпадает необходимость оккупировать территорию противника, лишенного экономики, а его политический строй, оказавшийся в международной изоляции, наверняка развалится сам [310].

Ливийский конфликт подтвердил, что общей тенденцией развития военного потенциала стран Запада является достижение такого уровня военно-технического оснащения и организации войск (сил), который позволит добиваться быстрой победы над любым противни-

ком путем нанесения массированных высокоточных ракетных ударов в условиях абсолютного радиоэлектронного подавления противника и информационного превосходства над ним. Группировки будут создаваться в короткие сроки на основе боеготовых воинских формирований, обладающих высоким уровнем стратегической мобильности и способности к ведению автономных действий. При этом сухопутные войска будут задействоваться лишь для окончательного закрепления успеха [310].

С учетом размаха использования коалицией инфраструктуры для проведения операции в Ливии и количества участвовавших в ней стран можно констатировать, что в будущих войнах изменятся многие привычные представления не только в области стратегии, но и в области оперативного искусства и тактики. Такие войны будут иметь широкий пространственный размах, включающий сухопутный и морской театры войны, кроме того, будет отсутствовать четко выраженное направление главного удара, поскольку удары по противнику будут наноситься со всех направлений [310].

Одновременно ливийский кризис позволяет говорить о возникновении новой ситуации, когда абсолютное превосходство в технической и огневой мощи не является решающим фактором достижения быстрого успеха в военных действиях. Так, переход регулярных частей и подразделений ВС Ливии к партизанским методам ведения вооруженной борьбы позволил им долгое время оказывать вооруженное сопротивление при полном господстве противника в воздухе и организации блокады с моря. Такие асимметричные действия правительственных войск существенно снизили эффективность применения коалиционных сил и средств, а также привели к значительному затягиванию сроков всей военной кампании [310].

Итоги военной кампании в Ливии свидетельствуют о том, что страны Запада готовы применять военно-силовые методы для достижения своих военно-политических и военно-стратегических целей в будущем. Они также подтвердили намерения США и их союзников возглавить «борьбу народов за демократию», направляя процесс «демократического переустройства» против антизападных режимов в регионе [310].

В целом конфликт в Ливии подтвердил основные тенденции развития военного искусства западных стран и позволил им на практике проверить ряд новых концептуальных подходов к ведению современных и будущих войн. Кроме того, он показал, что одним из решающих факторов, обеспечивающих победу в войне, становятся ме-

роприятия, связанные с информационно-психологическим и экономическим воздействием на противника [310].

Опыт ливийской кампании выявил ряд новых тенденций, которые с высокой степенью вероятности будут использоваться Западом в дальнейшем. В частности, при достижении военно-политических целей на первый план выдвигаются информационно-психологические, дипломатические и экономические формы воздействия на неугодные режимы. Непосредственно в ходе военного конфликта будут комплексно применяться в первую очередь высокоточные средства поражения, в том числе большой дальности, позволяющие минимизировать ответные действия противника и не допустить существенных потерь своих сил и средств [310].

Одновременно ливийская кампания подтвердила возрастающее значение информационно-пропагандистского фактора, особенно в современных условиях, когда СМИ играют существенную роль в формировании общественного сознания. Так, в интересах обоснования необходимости вмешательства международного сообщества в разрешение кризиса в Ливии Западом активно проводилась целенаправленная дезинформация, когда акцент делался на «преступлениях» одной из противоборствующих сторон, замалчивая при этом деструктивные и противозаконные действия другой [310].

Активная деятельность НАТО по информационному воздействию на правительственные войска позволила полностью дезорганизовать ливийские вооруженные силы и подавить их волю к сопротивлению. Кроме того, многие ливийские чиновники высокого ранга, а также ряд военачальников перешли на сторону оппозиции [310].

В современных условиях важной целью психологических операций является заблаговременное воздействие на потенциального противника в интересах формирования элит с заданным мировоззрением, привития населению определенных ценностей и стереотипов, позволяющих, с одной стороны, прогнозировать его поведение и играть на внутренних противоречиях, а с другой – влиять на процессы принятия решений на всех уровнях управления. Активные дипломатические действия государств коалиции в короткий срок дали возможность привлечь на свою сторону и сторону ливийских оппозиционных сил широкий круг государств, в том числе арабских. При этом успех западных стран в «продавливании» резолюции СБ ООН по Ливии позволил придать операции легитимный характер и обеспечить действиям по уничтожению ливийского лидера формальное международно-правовое прикрытие [310].

Таким образом, в ходе ливийского конфликта был опробован и практически реализован эффективный способ отстранения от власти неугодных Западу режимов, который предполагает [310]:

- формирование протестных настроений и поддержку антиправительственных действий среди населения и элиты;
- создание и поддержку антиправительственных групп, партий и движений, а также подконтрольных Западу СМИ;
- проведение широкомасштабной антиправительственной кампании по дискредитации правящего режима и подрыву легитимности его власти;
- инспирирование жестокости властей по отношению к протестующему населению и провоцирование его на расширение антиправительственных выступлений;
- организацию массовых протестных действий, которые вынуждают власти жестко реагировать на них;
- организацию международного осуждения жестокости властей и скрытую поддержку радикальных группировок, провоцирующих ее;
- создание и поддержку параллельных структур власти в стране из состава оппозиции;
- привлечение к поддержке оппозиции международных организаций и структур, а также усиление экономического давления на режим и введение различных санкций;
- организацию международной кампании по признанию легитимности создаваемых оппозицией территориальных и национальных образований;
- провоцирование властей на применение силы в отношении таких образований;
- создание коридоров и зон безопасности вокруг районов, контролируемых оппозицией, с одновременным их расширением, а также ввод «ограниченных контингентов» войск с целью «защиты» населения;
- проведение ограниченной военной операции против неугодного режима (если это необходимо).

Политические эксперты Запада считают, что такой алгоритм действий является наиболее эффективным. Это также подтверждается сценарием, активно реализуемым уже и в отношении Сирии.

Заключение

Проведенный анализ последствий внедрения информационно-технической революции в системы вооружения показал, что основным путем повышения боевой эффективности систем вооружений на сегодняшний день становится оснащение их современными информационными системами, обеспечивающими сбор и анализ поступающей информации, наведение оружия на цель, боевое управление и связь между участвующими в военных действиях подразделениями. Это привело к «информационно-технической революции в военном деле», специфика которой состоит в том, что она опирается на значительный технологический прорыв именно в области информационных технологий. Причем если ранее основные усилия концентрировались на улучшении ударных и боевых компонентов вооруженных сил, то сейчас передовые улучшения затрагивают, в первую очередь, системы управления и разведки. Техническая сторона современной революции в военном деле основана, в первую очередь, на достижениях в области информатики и электроники, на улучшении характеристик точности и дальности действия оружия, полноте и оперативности разведки и наблюдения, повышении способности противодействовать и подавлять вражескую оборону и эффективно управлять войсками.

По мере развития средств вооруженной борьбы и военной техники в целом изменяются формы и способы их применения в войне, что неизбежно обусловливает изменение способов ведения военных действий. Отличительной особенностью развития современных средств вооруженной борьбы состоит в быстрой их информатизации, что резко увеличило боевые возможности последних, привело к коренной ломке организационных форм вооруженных сил и способов ведения военных действий всех масштабов. Именно за счет развития средств вооруженной борьбы произошел переворот в военной стратегии и военном искусстве в целом, который ознаменовался формированием и внедрением в практику военного искусства концепции сетецентрической войны.

При этом авторы концепции сетецентрической войны отмечают, что она является не революцией в военном деле, которая изменяет сущность войны, а скорее новый фактором, который мог бы позволить государственному и военному аппарату осуществлять более эффективное управление силами и средствами при условии, что Военная доктрина и вооруженные силы выстроены соответствующем образом. Анализ концепции сетецентрической войны показывает, что ее основ-

ная идея лежит не в новых формах и способах ведения боевых действий, а в изменении принципов управления войсками и оружием, переходе к сетевому принципу управления, а также включении всех сил и средств, участвующих в боевых действиях, в единое информационное пространство. Иначе говоря, это новый способ организации управления, который является реальным инструментом повышения боевых возможностей разнородных сил и средств за счет синергетического эффекта. А новые формы и способы ведения боевых действий, в большей степенью, следствием внедрения нового принципа сетецентрического управления.

Концепция сетецентрической войны – это теория качественного сдвига в военных технологиях управления. Вооруженные силы используя принципы сетецентрического управления, получают возможность более эффективного использования информации как в процессе принятия решений, так и в процессе использования своих боевых возможностей для решения поставленных задач. Это позволит вооруженным силам действовать более эффективно (быстро и качественно, целенаправлено и гибко). Важно, что эти новые возможности позволят применять вооруженные силы принципиально новым образом за счет интеграции действий боевых подразделений на более низких уровнях управления.

Таким образом, внедрение концепции сетецентрической войны обосновывает необходимость изменения не только вооружения, но также и состава, и структуры вооруженных сил. Однако даже в наиболее развитых странах структура вооруженных сил, формы и способы их применения будут меняться не сразу, а по мере принятия на вооружение и накопления достаточного количества средств вооружения, поддерживающих сетецентрические принципы управления. В течение некоторого времени вооруженные силы таких стран будут развивать потенциал ведения войны нового поколения, одновременно сохраняя способность выполнять большое количество задач оперативно-тактического и даже стратегического уровня, относящихся к войнам прошлого поколения.

Концепция сетецентрической войны активно внедряется в практику ведения боевых действий США и НАТО и уже была успешно апробирована в военных операциях, проводимых в Югославии, Ираке, Ливии, а новые сетецентрические технологические подходы тестируются на учениях и обыгрываются на симуляторах. Разработчики этой теории убеждены, что в ближайшем будущем она если не за-

менит собой традиционную теорию войны, то существенно и необратимо качественно изменит ее.

В современном глобализирующемся мире вся социально-экономическая, политическая и культурная структуры пронизываются информационными каналами, которые составляют сети сетецентрической системы. Поэтому дальнейшее развитие концепции сетецентрических войн позволит обосновать новые способы военного и невоенного противоборства, использующие особенности сетецентрического управления силами и средствами в едином информационном пространстве. Прежде всего, это способы смены государственной власти на основе технологий управляемого хаоса (так называемые «цветные революции»), технологии экономического давления, технологии информационной войны, а также технологии гибридной войны, совмещающие комплекс мер несилового давления с ограниченным и точечным применением вооруженных сил.

Список использованных сокращений

A2C2S – Army Airborne Command and Control System
AASM – Armement Air-Sol Modulaire
ABCS – Army Battle Command System
ABV – Assault Breacher Vehicle
ACAS-Xu – Airborne Collision-Avoidance System for Unmanned Aircraft
ACS – ANS Computer System
ACTUV – Anti-submarinewarfare Continuous Trail Unmanned Vessel
ADAM – Area Defense Anti-Munitions
AEA – Airborne Electronic Atack
AEHF – Advanced Extremely-High-Frequency
AEHF – Advanced Extremely High Frequency
AFATDS – Advanced Field Artillery Tactical Data System
AFSCN – Air Force Satellite Control Network
AQF – Advanced Quick Fix
ARM – Anti-Radar Missile
ASAS – All Source Analysis System
ATCCS – Army Tactical Command and Control System
AUV – Autonomous Underwater Vehicles
BITS – Battlefield Information Transmission System
BMEWS – Ballistic Missile Early Warning System
BROACH – Bomb Royal Ordnance Augmented Charge
C2OTM – Command-and-Control On the Move
C4IFTW – Command, Control, Communications, Computers, and Intelligence for the Warrior
C4ISR – Command Control Communications Computers Intelligence Surveillance Reconnaissance
CCJ – Core Component Jammer
CCSR – Communication Countermeasures Set Receiver
CEASAR – Communications Electronic Attack with Surveillance and Reconnaissance
CEC – Cooperative Engagement Capability
CIA – Central Intelligence Agency
CIGSS – Common Imagery Ground/Surface System Architecture
CIL – Command Information Library
CIS – Communication Interface System

CMP – Crypto Modernization Program
COBRA – Collection Of Broadcasts from Remote Assets
COIL – Chemical Oxygen Iodine Laser
CSSCS – Combat Service Support Command System
DAHI – Diverse & Accessible Heterogeneous Integration
DAMA – Demand Accessed Multiple Access
DAPA – Defense Acquisition Program Administration
DARPA – Defense Advanced Research Projects Agency
DCGS – Distributed Common Ground System
DDN – Defense Data Network
DEA – Defensive Electronic Attack
DII – Defense Information Infrastructure
DISA – Defense Information Systems Agency
DISARMER – Direct SAMpling Digital ReceivER
DISN – Defense Information Systems Network
DMS – Defense Message System
DODOS – Direct On-Chip Digital Optical Synthesis
DRR – Due Regard Radar
DRSN – Defense Red Switched Network
DSCS – Defense Satellite Communications System
DSMAC – Digital Scene Matching Area Correlation
DSN – Defense Switched Network
DSO – Defense Sciences Office
DSP – Defense Support Program
DTSS – Digital Topographic Support System
DVS – DISN VIDEO
DWDM – Dense Wavelength Division Multiplexing
DWS – Distributed Wargaming System
EBO – Effect-based Operations
EHF – Extremely High Frequency
EKV – Exoatmospheric Kill Vehicle
ETRAC – Enhanced Tactical Radar Corelator
FAADCIS – Forward Area Air Defense Command, Control Intelligence System
FAADS – Forward Area Air Defense System
FAB – Fast and Big Mixed-Signal Designs
FBCB – Force XXI Battle Command for Brigade and Below
FBCB2 – Force XXI Battle Command Brigade or Below
FBI – Federal Bureau of Investigation
FCS – Future Combat Systems

FFT/BFT – Friendly Force Tracking/Blue Force Tracking (Systems)
FODT – Fiber Optic Decoy Towed
FSRS – Frequency Selective Receiver System
GBCS-H – Ground Based Common Sensors – Heavy
GBMD – Ground-Based Midcourse Defense
GBSAA – Ground-Based Sense-And-Avoid
GCCS – Global Command and Control System
GCCS-J – Global Command and Control-Joint
GES – GIG Enterprise Services
GIG – Global Information Grid
GIG-BE – Global Information Grid-Bandwidth Expansion
GPS – Global Positioning System
GSM – Ground Station Module
GSSCS – Combat Service Support Control System
HAARP – High Frequency Active Auroral Research Program
HAPS – Helicopter Active Protective System
HARM – High-speed Anti-Radar Missile
HEL MD – High Energy Laser Mobile Demonstrator
HIRAT – High-power Ram Air Turbine
HISAR – Hughes Integrated Surveillance & Reconnaissance
HMMWV – High Mobility Multipurpose Wheeled Vehicle
HTV – Hypersonic Technology Vehicle
IEWCS – Intelligence and Electronic Warfare Common Sensor
IEWS – Integrated Electronic Warfare System
IMETS – Integrated Meteorological System
IMEWS – Integrated Missile Early Warning Satellite
INCANS – INterference CANcellation System
INEW – Integrated Network-E1ectronic Warfare
INSCOM – Intelligence and Security Command
IP/MPLS – Internet Protocol and Multiprotocol label switching
IPL – Image Product Library
IPM – Imaging Perception Module
IRC – Internet Relay Chat
ISTAR – Intelligence, Surveillance, Target Acquisition, and Reconnaissance
JAUS – Joint Architecture for Unmanned Systems
JC2 – Joint Command and Control System
JCIDS – Joint Capabilities Integration and Development System
JDAM – Joint Direct Attack Munitions
JEWCS – Joint Electronic Warfare Core Staff

JFC – Joint Functional Concepts
JHPSSL – Joint High Power Solid-State Laser
JIC – Joint Integrating Concept
JIVA – Joint Intelligence Virtual Architecture
JLTV – Joint Light Tactical Vehicle
JMCIS – Joint Military Command Information System
JOC – Joint Operating Concept
JOTS – Joint Operational Tracking System
JSAK – Joint State Area Command
JSTARS – Joint Surveillance Target Attack Radar System
JTRS – Joint Tactical Radio Systems
JTRS GMR – Joint Tactical Radio System's Ground Mobile Radio
JWARS – Joint Warfare System
JWICS – Joint Worldwide Intelligence Communications System
JTIDS – Joint Tactical Information Distribution System
LAR – Leaflet Artillery Round
LaWS – Laser Weapon System
LBU – Leaflet Bomb Unit
LCS – Littoral Combat Ships
LEAP – Lightweight Exo-Atmospheric Projectile
LIPM – LADAR Imaging Perception Module
MALD – Miniature Air-Launched Decoy
MANET – Mobile Ad hos Network
MBCOTM – Mounted Battle Command on the Move
MCS – Maneuver Control System
MFEW – Multi-Function Electronic Warfare
MHIV – Miniature Homing Intercept Vehicle
MIDB – Multi Intelligence Data Base
MILSTAR – Military Strategic and Tactical Relay
MIMO – MultIpleinput - MultipleOutput
MITT – Mobile Integrated Tactical Terminal
MKV – Multiple Kill Vehicle
MMWR – Millimeter Wave RADAR
MOSAIC – Multifunctional On the Move Secure Adaptive Integrated Communications
MRUUV – Multi Mission Reconfigurable Unmanned Undersea Vehicle
MTO – Microsystems Technology Office
MTS – Movement Tracking System
MUOS – Mobile User Objective System

MUOS – Mobile User Objective System
NCEJFC – Net-Centric Environment Loint Functional Concept
NCES – Net-Centric Enterprise Services
NCW – Network-CentricWarfare
NERO – Networked Electronic Warfare, Remotely Operated
NGJ – Next Generation Jammer
NGN – New Generation Networks
NIL – National Information Library
NIPRNet – Non-classified Internet Protocol Router Network
NITF – National Imagery Transmission Format
NMD – National Missile Def
NOSS – Naval Ocean Surveillance System
NSA – National Security Agency
NTM – National Technical Means
NUWC – Naval Undersea Warfare Center
OFBCS – Objective Force Battle Command System
ORS – Operationally Responsive Space
OSINT – Open Source Intelligence
P2P – Peer-to-Peer
PGS – Prompt Global Strike
PIMPF – Programmable Intelligent Multi-Purpose Fuze
PLSS – Precision Location Strike System
PLUSNet – Persistent Littoral Undersea Surveillance Network
PPAML – Probabilistic Programming for Advancing Machine Learning
PUH – Precision Urban Hopper
QDDR – Quadrennial Diplomacy and Development Review
RAT – Ram Air Turnbine
RCLCV – Remote-Controlled Light Combat Vehicle
REDOWL – Robotic Enhanced Detection Outpost With Lasers
RFW – Radio Frequency Weapon
ROV – Remotely Operated Vehicles
SALS – Sagitarius Airborne Launch System
SBIRS – Space-Based Infrared System
SBL – Space Based Laser
SDR – Software Defined Radio
SDS – Satellite Data System
SEE ME – Space Enabled Effects for Military Engagements
SINCGARS – Single Channel Ground and Airborne Radio System
SIPRI – Stockholm International Peace Research Institute

SIPRNet – Secret Internet Protocol Router Network
SMART – Scalable, Modular, Airborne, Relay, Terminals
SOA – Service-Oriented Architecture
SOMS B – Special Operations Media System B
SOSCOE – System of System Common Operating Environment
SPIN – Segmented, Polycentric, Ideologically integrated Network
SRR – Special Reconnaissance Regiment
SSL – Single Station Location
SSL-QRC – Solid State Laser Quick Reaction Capability
STSS – Space Tracking and Surveillance System
TADTE – Taipei Aerospace & Defense Technology Exhibition
TBG – Tactical Boost Glide
TBMCS – Theater Battle Management Core Systems
TCDL – Tactical Common Data Link
TCRCCES – Transportation Command Regulating and Command and Control Evacuation System
TDRSS – Tracking and Data Relay Satellite System
TES-A – Tactical Exploitation System (Army)
THAAD – Terminal High Altitude Area Defense
THEL – Tactical High-Energy Laser
TILL – Track Illuminator Laser
TRACS – Tactical Radio Acquisition and Countermeasures Subsystem
TSAT – Transformational Satellite Communications System
TSC – Theater Security Cooperation
TTD – True Time Delay
TTO – Tactical Technology Office
UAV – Unmanned Air Vehicles
UFO – UHF Follow-On
UGV – Unmanned Ground Vehicles
UPS – Undersea Persistent Surveillance
UPSIDE – Unconventional Processing of Signals for Intelligent Data Exploitation
URLM – Universal Launch and Recovery Module
USV – Unmanned Surface Vehicles
UUV – Unmanned Underwater Vehicles
UUVI – Unmanned Undersea Vehicle Initiative
VMF – Variable Message Format
VOIP – Voice Over Internet Protocols
WAASM – Wide-Area Airborne Surveillance System

WAND – Wireless Adaptive Network Development
WGS – Wideband Global SATCOM system
WGS – Wideband Global Satcom
WIN-T – Warfighter Information Network – Tactical
XSS – eXperimental Satellite System
АК – Авиационное командование
АЛВЦ – Автономная программируемая ложная воздушная цель
АМГ – Авианосная многоцелевая группа
АНБ – Агентство национальной безопасности
АСП – Авиационные средства поражения
АСУ – Автоматизированная система управления
АСУВ – Автоматизированная система управления войсками
АТО – Антитеррористическая операция
АТР – Азиатско-Тихоокеанский регион
АУГ – Авианосная ударная группировка
АФАР – Активная фазированная антенная решетка
АЦП – Аналого-цифровой преобразователь
ББМ – Боевая бронированная машина
БИУС – Боевая информационно-управляющая система
БМП – Боевая машина пехоты
БНК – Безэкипажный надводный корабль
БПЛА – Беспилотный летательный аппарат
БР – Баллистическая ракета
БРМД – Баллистическая ракета малой дальности
БРПЛ – Баллистическая ракета подводной лодки
БРСД – Баллистическая ракета средней дальности
БРЭО – Бортовое радиоэлектронное оборудование
БССЦУ – Бортовые системы сетецентрического управления
БТР – Бронетранспортёр
БЦВМ – Бортовая цифровая вычислительная машина
БЧ – Боевая часть
БЭ – Боевой элемент
ВВ – Взрывчатое вещество
ВВП – Внутренний валовый продукт
ВВП – Взлетно-посадочная полоса
ВВС – Военно-воздушные силы
ВВСТ – Вооружения, военная и специальная техника
ВВТ – Вооружение и военная техника
ВКН – Воздушно-космическое нападение

ВКО – Воздушно-космическая оборона
ВКС – Воздушно-космические силы
ВМГ – Взрывомагнитный генератор
ВМС – Военно-морские силы
ВОЛС – Волоконно-оптическая линия связи
ВС – Вооруженные силы
ВТО – Высокоточное оружие
ГАС – Гидроакустическая станция
ГАСС – Гидроакустическая система связи
ГЗЛА – Гиперзвуковой летательный аппарат
ГИУС – Глобальная информационная управляющая сеть
ГСМ – Горюче-смазочные материалы
ГСН – Головка самонаведения
ГШ – Генеральный штаб
ДА – Дальняя авиация
ДРЛОиУ – Дальнее радиолокационное обнаружение и управления
ДУМ – Дистанционно-управляемая машина
ЕСУ – Единая система управления
ЕСЭ – Единая сеть электросвязи
ЗА – Зенитная артиллерия
ЗИП – Запасное имущество и принадлежности
ЗПП – Забрасываемые передатчики помех
ЗРК – Зенитно-ракетный комплекс
ИА – Истребительная авиация
ИБ – Информационная безопасность
ИВ – Информационная война
ИК – Инфракрасный
ИО – Информационная операция
ИС – Информационная система
ИСУ – Инерциальная система управления
ИТВ – Информационно-техническое воздействие
ИЦТСС – Интегрированная цифровая территориальная система связи
КА – Космический аппарат
КВ – Короткие волны
КГБ – Комитет государственной безопасности
КНР – Китайская Народная Республика
КНШ – Комитет начальников штабов
КПД – Коэффициент полезного действия

КР – Крылатая ракета
КРВБ – Крылатая ракета воздушного базирования
КРМБ – Крылатая ракета морского базирования
КРНС – Космическая радионавигационная система
КСИ – Командование стратегических исследований
КУГ – Корабельная ударная группа
КШМ – Командно-штабная машина
ЛПР – Лицо, принимающее решение
МБР – Межконтинентальная баллистическая ракета
МВФ – Международный валютный фонд
МКА – Малый космический аппарат
МНР – Мобильные наземные роботы
МО – Министерство обороны
МСЭ – Международный союз электросвязи
НИОКР – Научно-исследовательская опытно-конструкторская работа
НИР – Научно-исследовательская работа
НК – Надводный корабль
НЛП – Нейро-лингвистическое программирование
ННА – Необитаемый надводный аппарат
НОАК – Народно-освободительная армия Китая
НОРД – Цикл «наблюдай, ориентируйся, решай, действуй»
НПА – Необитаемый подводный аппарат
НСД – Несанкционированный доступ
НУО – Национальный университет обороны
ОАЦСС – Объединенная автоматизированная цифровая система связи
ОАЭ – Объединенные арабские эмираты
ОБЭ – Операции, базирующиеся на эффектах
ОВ – Отравляющее вещество
ОВВС – Объединенные военно-воздушные силы
ОВМС – Объединенные военно-морские силы
ОВМФ – Объединенный военно-морской флот
ОВС – Объединенные Вооруженные силы
ОВЧ – Очень высокая частота
ОДАБ – Объемно-детонирующая авиационная бомба
ОДКБ – Организация Договора о коллективной безопасности
ОИК – Объединенная интегральная концепция
ОК – Объединенное командование
ОКК – Объединенное космическое командование

ОКР – Опытно-конструкторская работа
ОМБ – Объект морского базирования
ОМП – Оружие массового поражения
ООБ – Основная операционная база
ООН – Организация Объединенных Наций
ООФ – Объединенное оперативное формирование
ОПК – Оборонно-промышленный комплекс
ОС – Объединенные силы
ОСВ – Объединенные сухопутные войска
ОСК – Оперативно-стратегическое командование
ОФ – Оперативное формирование
ОФК – Объединенная функциональная концепция
ПА – Полевая армия
ПВО – Противовоздушная оборона
ПЗС – Прибор с зарядовой связью (матрица)
ПКО – Противокосмическая оборона
ПЛАРБ – Подводная лодка с баллистическими ракетами
ПЛИС – Программируемая логическая интегральная схема
ПЛО – Противолодочная оборона
ПНС – Переходной национальный совет
ПО – Программное обеспечение
ПОБ – Передовая операционная база
ПРО – Противоракетная оборона
ПСБ – Противоспутниковая борьба
ПсО – Психологическая операция
ПТРК – Противотанковые ракетные комплексы
ПТУР – Противотанковая управляемая ракета
ПУ – Пункт управления
ПЦП – Программно-целевое планирование
РБД – Ракета большой дальности
РИО – Радиоэлектронное информационное обеспечение
РЛ – Радиолокационный
РЛС – Радиолокационная станция
РР – Радио разведка
РРТР – Радио- и радиотехническая разведка
РСЗО – Реактивная система залпового огня
РТР – Радиотехническая разведка
РУБС – Разведывательно-ударная боевая система
РУК – Разведывательно-ударный комплекс
РХБЗ – Радиационная, химическая и биологическая защита

РЭБ – Радиоэлектронная борьба
РЭЗ – Радиоэлектронная защита
РЭНД – Американский стратегический исследовательский центр
РЭО – Радиоэлектронное оборудование
РЭП – Радиоэлектронное подавление
РЭПр – Радиоэлектронное поражение
РЭС – Радиоэлектронное средство
СБ – Совет безопасности
СБИС – Сверхбольшая интегральная схема
СВ – Сухопутные войска
СВ – Средние волны
СВКН – Средства воздушно-космического нападения
СВН – Средства воздушного нападения
СВЧ – Сверхвысокая частота
СЕВ – Система единого времени
СЗИ – Средства защиты информации
СК – Стратегическое командование
СККП – Система контроля космического пространства
СКО – Стратегическое командование операций
СМИ – Средства массовой информации
СНВ – Стратегические наступательные вооружения
СНГ – Содружество независимых государств
СОИ – Стратегическая оборонная инициатива
СОРМ – Система оперативно-розыскных мероприятий
СПРН – Система предупреждения о ракетном нападении
СРНС – Спутниковая радионавигационная система
ССО – Силы специальных операций
ССОП – Система связи общего пользования
СТП – Силы территориального применения
СУВО – Система управления войсками и оружием
СУО – Системы управления огнем
СУП – Силы универсального применения
СЦВ – Сетецентрическая война
СЦО – Сетецентрическая операция
США – Соединенные Штаты Америки
СЯС – Стратегические ядерные силы
ТА – Тактическая авиация
ТВ – Телевидение
ТВД – Театр военных действий

ТНК – Транснациональная корпорация
ТТХ – Тактико-технические характеристики
УАБ – Управляемые авиабомбы
УАК – Управляемый авиационный комплекс
УВД – Управление воздушным движением
УВЧ – Ультравысокая частота
УИС – Управляющие информационные системы
УКВ – Ультракороткие волны
УКР – Управляемая крылатая ракета
УР – Управляемая ракета
УФ – Ультрафиолетовый
ФАР – Фазированная антенная решетка
ФБР – Федеральное бюро расследований
ФРГ – Федеративная Республика Германия
ФРС – Федеральная резервная система (США)
ФРЭПр – Функциональное радиоэлектронное поражение
ЦАП – Цифро-аналоговые преобразователи
ЦАТУ – Центр административно-территориального управления
ЦАХАЛ – Вооруженные силы Израиля
ЦБ – Центральный банк
ЦРР – Центр радиоэлектронной разведки
ЦРУ – Центральное разведывательное управление
ЦУС – Центр управления сетью
ЧНЧ – Чрезвычайно низкая частота
ЭВМ – Электронная вычислительная машина
ЭМИ – Электромагнитное излучение
ЭМО – Электромагнитное оружие
ЭПР – Эффективная площадь рассеяния
ЮНА – Югославская народная армия
ЯБЧ – Ядерная боевая часть

Литература

1. Гареев М. А. Если завтра война. – М.: ВлаДар, 1995. – 238 с.

2. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. – М.: Харвест, 2004. – 426 с.

3. Гриняев С. Н. Мир 2013: события, факты комментарии. – М.: АНО ЦСОиП, 2014. – 328 с.

4. Пирумов В. С. Информационное противоборство. – М.: Оружие и технологии, 2010. – 252 с.

5. Пирумов В. С., Родионов М. А. Некоторые аспекты информационной борьбы в военных конфликтах // Военная мысль. 1997. № 5. С. 44-47.

6. Костин Н. А. Общие основы теории информационной борьбы // Военная мысль. 1997. № 3. С. 44-50.

7. Костин Н. А. Геополитический характер информационной борьбы в современном мире и ее проблемы накануне XXI века // Безопасность информационных технологий. 1999. № 1. С. 21.

8. Костин Н. А. Информационная борьба. Вопросы теории // Актуальные проблемы гуманитарных и естественных наук. 2011. № 11. С. 52-58.

9. Комов С. А. Информационная борьба в современной войне: вопросы теории // Военная мысль. 1996. № 3. С. 73.

10. Цымбал В. И. О концепции информационной войны // Информационный сборник «Безопасность». 1995. № 9. С. 21.

11. Прохожев А. А., Турко Н. И. Основы информационной войны // Анализ систем на пороге XXI века: теория и практика. – М., 1996. – С. 252-253.

12. Модестов С. А. Война, к которой готовится Америка: эволюция вооруженной борьбы в эпоху информатизации // ЭВНГ. 14.03.1996. № 048.

13. Буренок В. М., Ивлев А. А., Корчак В. Ю. Развитие военных технологий XXI века: проблемы планирование, реализация – Тверь.: КУПОЛ, 2009. – 624 с.

14. Буренок В. М., Ивлев А. А., Корчак В. Ю. Развитие военных технологий XXI века: проблемы планирование, реализация. – Тверь: КУПОЛ, 2009. – 624 с.

15. Гуржеянц Т. В., Дербин Е. А., Крылов Г. О., Кубанков А. Н. Информационные операции современности: Уч. пособие. – М.: ВАГШ, 2003. – 286 с.

16. Бедрицкий А. В. Реализация концепции информационной войны военно-политическим руководством США на современном этапе. Дис. … уч. степени канд. полит. наук. Спец. 23.00.04. – М.: Российский институт стратегических исследований, 2007. – 165 с.

17. Слипченко В. И. Войны шестого поколения: Оружие и военное искусство будущего. – М.: Вече, 2002. – 381 с. – URL: http://webreading.ru/conv/do_rtf.php?name=/books/sci_/sci_history/slipchenko_vladimir_voynyi_shestogo_pokoleniya (дата обращения 22.01.2014).

18. Новоселов С. В. Военно-политическая обстановка в мире и перспективы ее развития // Каспийский регион: политика, экономика, культура. 2013. № 1. С. 89-99.

19. Павловский Г. Мир после кризиса. Глобальные тенденции – 2025: меняющийся мир. Доклад Национального разведывательного совета США. – М.: Европа, 2009. – 188 с.

20. Романенко Ю. Угроза глобальной войны: движущие силы, противоборствующие коалиции и перспективы Украины. Доклад директора Центра политического анализа «Стратагема в клубе «Ленин» 12 декабря 2011 г.

21. Vitali S. Glattfelder J.B., Battiston S. The network of global corporate control. – Chair of Systems Design, ETH Zurich, Switzerland, 2011. – URL: http://www.newsru.com/finance/20oct2011/global_capitalism.html (дата обращения 22.01.2014).

22. Гордеев К. 2011: уроки, не усвоенные человечеством // Фонд Стратегической Культуры. 2011. – URL: http://www.fondsk.ru/pview/2012/02/01/2011-uroki-ne-usvoennye-chelovechestvom.html (дата обращения 22.01.2014).

23. Сивков К. В. Оценка вероятности мировой войны // Управление мегаполисом. 2009. № 2. С. 38-44.

24. Бурбаки В. Зачем Америке нужна «большая война» – URL: http://www.fondsk.ru/news/2011/12/27/zachem-amerike-nuzhna-bolshaja-vojna.html (дата обращения 22.01.2014).

25. Sustaining US Global Leadership Priorities for 21st Century Defense. – United States of America, Department of Defense. – URL: http://www.defense.gov/news/Defense_Strategic_Guidance.pdf (дата обращения 22.01.2014).

26. Тренин Д. Военно-политическая обстановка в мире в 2012 году // Военно-промышленный курьер. 2012. № 3. С. 24-32.

27. Вихров В. Доктрина Обамы: контроль над потоками энергоносителей в Китай // Центральная Азия [Электронный ресурс]. 13.01.2012. – URL: http://www.centrasia.ru/newsA.php?st=1326448140 (дата обращения 19.01.2016).

28. Фомин А. Н. Факторы риска в анализе современной военно-политической обстановки. Аналитический доклад. – М.: АНО «Центр стратегических оценок и прогнозов», 2013. – 27 с. – URL: www.csef.ru (дата обращения 22.01.2014).

29. Бобков Ю. Я., Тютюнников Н. Н. Концептуальные основы построения АСУ Сухопутными войсками ВС РФ: монография. – М.: Палеотип, 2014. – 92 с.

30. Комов С. А. О способах и формах ведения информационной борьбы // Военная мысль. 1997. № 4. С. 18-22.

31. Комов С. А., Коротков С. В., Дылевский И. Н. Об эволюции современной американской доктрины «информационных операций» // Военная мысль. 2008. № 6. С. 54-61.

32. Как США борется с Китаем [Электронный ресурс]. – URL: http://voprosik.net/kak-ssha-boretsya-s-kitaem/ (дата обращения 22.01.2014).

33. Китай как локомотив современного мира. Часть 1. Геополитический компас Китая // Независимый аналитический центр геополитических исследований [Электронный ресурс]. – URL: http://bintel.com.ua/ru/article/kitaj-kak-lokomotiv-sovremennogo-mira1/ (дата обращения 22.01.2014).

34. Наквим Н. Последствия сделки 2001 // Expert Online [Электронный ресурс]. – URL: http://esaconference.ru/wpcontent/uploads/files/pdf/Stryapchev-Eduard-Nikolaevich.pdf (дата обращения 22.01.2014).

35. Что год грядущий готовит миру? // Независимый аналитический центр геополитических исследований [Электронный ресурс], 2012. – URL: http://bintel.com.ua/ru/article/prognoz-razvitija-situacii-v-mire-v-2013-godu/ (дата обращения 22.01.2014).

36. Некоторые аспекты анализа военно-политической обстановки: Монография / Под ред. А.И. Подберезкина, К.П. Боришполец. – М.: МГИМО, 2014. – 874 с.

37. Воздушная армия кибероперацій КК ВВС США [Электронный ресурс]. – URL: http://pentagonus.ru/publ/22-1-0-1069 (дата обращения 22.01.2014).

38. Буренок В. М. К инновационной армии // Воздушно-космическая оборона. 2009. № 3. С. 16-25.

39. Буренок В. М. Базис следующего поколения войн // Вестник академии военных наук. 2011. № 3. С. 32-37.

40. Буренок В. М. Развитие системы вооружения и новый облик вооруженных сил РФ // Защита и безопасность. 2009. № 49. С. 14-16.

41. Буренок В. М. Новые технологии и новые войны // Защита и безопасность. 2011. № 3. С. 8-11.

42. Буренок В. М. Будущие войны // Вооружение и экономика. 2013. № 2. С. 37-43.

43. Кондратьев А. Е. Сетецентризм или гонка за временем. Сборник статей [Электронный ресурс], 2011. – URL: http://pentagonus.ru/load/1/obshhie_voprosy/a_kondratev_setecentrizm/18-1-0-751 (дата обращения 19.01.2016).

44. Кондратьев А. Е. Роботы и люди. Сборник статей. [Электронный ресурс], 2012. – URL: http://pentagonus.ru/load/1/obshhie_voprosy/kondratev_roboty_i_ljudi_tom_3/18-1-0-830 (дата обращения 22.06.2016).

45. Кондратьев А. Е. Сетецентрический фронт. Боевые действия в едином информационном пространстве // Национальная оборона. 2011. № 2. С. 10-18.

46. Кондратьев А.Е. Когда «сетецентризм» придет в российскую армию? // Вестник академии военных наук. 2012. № 2 С. 120-125.

47. Иванов М. С., Дахужев А. С. Война в информационном пространстве. Цели и результаты войны // Алгоритмические и программные средства в информационных технологиях, радиоэлектронике и телекоммуникациях: сб. статей II международной заочной научно-технической конференции. – Тольятти: ПВГУС, 2014. С. 97-101.

48. Кондратьев А. Е. Некоторые особенности реализации концепции «сетецентрическая война» в вооруженных силах КНР // Зарубежное военное обозрение. 2010. № 3. С. 11-17. – URL: http://factmil.com/publ/strana/kitaj/nekotorye_osobennosti_realizacii_koncepcii_setecentricheskaja_vojna_v_vooruzhjonnykh_silakh_knr_2010/59-1-0-432 (дата обращения 19.01.2016).

49. Кондратьев А. Е. Исследования «сетецентрических» концепций в вооруженных силах ведущих зарубежных стран // Зарубежное военное обозрение. 2010. № 12. С. 3-9. – URL: http://factmil.com/publ/obshhee/voennaja_mysl/issledovanija_setecentricheskikh_koncepcij_v_vooruzhjonnykh_silakh_vedushhikh_zarubezhnykh_stran_2010/72-1-0-251 (дата обращения 19.01.2016).

50. Кондратьев А. Е. Проблемные вопросы исследования новых сетецентрических концепций вооруженных сил ведущих зарубежных стран // Военная мысль. 2009. № 11. С. 61-74.

51. Кондратьев А., Баулин В. Реализация концепции «сетецентрическая война» в ВМС США // Зарубежное военное обозрение. 2009. № 6. С. 61-67. – URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2009-zvo/7813-realizacija-koncepcii-setecentricheskaja-vojna-v-2 (дата обращения 19.01.2016).

52. Кондратьев А. Е. Общая характеристика сетевых архитектур, применяемых при реализации перспективных сетецентрических концепций ведущих зарубежных стран // Военная мысль. 2008. № 12. С. 63-74.

53. Кондратьев А. Е. Трансформация ВВС США в рамках концепции «сетецентрическая война» // Аэрокосмическое обозрение: Аналитика, комментарии, обзоры. 2007. № 6. С. 54.

54. Кошкин Р. П. Геополитические итоги 2015 года и стратегические приоритеты России // Стратегические приоритеты. 2015. № 4 (8). С.4-14.

55. Дылевский И. Н., Комов С. А., Петрунин А. Н. Об информационных аспектах международно-правового понятия «агрессия» // Военная мысль. 2013. № 10. С. 3-12.

56. Базылев С. И., Дылевский И. Н., Комов С. А., Петрунин А. Н. Деятельность Вооруженных Сил Российской Федерации в информационном пространстве: принципы, правила, меры доверия // Военная мысль. 2012. № 6. С. 24-28.

57. Коротков С. В., Дылевский И. Н., Комов С. А. Американские операции в киберпространстве: вопросы теории, политики и права // Военная мысль. 2011. № 8. С. 72-78.

58. Рахманов А. А. Принципы и подходы к концептуальному проектированию сетецентрических систем // Известия ЮФУ. Технические науки. 2010. Т. 113. № 12. С. 125-134.

59. Рахманов А. А. Сетецентрические системы управления – закономерные тенденции, проблемные вопросы и пути их решения // Военная мысль. 2011. № 3. С. 41-50.

60. Боев С. Ф., Рахманов А. А., Слока В. К. Сетецентрические системы регионального уровня реального масштаба времени // Мехатроника, автоматизация, управление. 2009. № 3. С. 64-68.

61. Налетов Г. А. К вопросу о разработке концепции нетрадиционных войн и вооруженных конфликтов (Новые формы и способы ведения вооруженной борьбы) // Вестник академии военных наук. 2012. № 1. С. 29-34.

62. Стародубцев Ю. И., Бухарин В. В., Семенов С. С. Техносферная война // Информационные системы и технологии. 2011. № 1. С. 80-85.

63. Стародубцев Ю. И., Семенов С. С., Бухарин В. В. Техносферная война // Научно-информационный журнал «Армия и общество». 2010. № 4. С. 6-11.

64. Гречишников Е. В., Милая И. В., Санин И. Ю., Стародубцев Ю. И. Способ защиты вычислительной сети. Патент на изобретение RUS 2422892, 13.04.2010.

65. Нурышев Г. Н. Доктрины «управляемого хаоса» в современной глобальной геополитике // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. 2011. № 2. С.81-204.

66. Стародубцев Ю. И., Гречишников Е. В., Комолов Д. В. Способ обеспечения устойчивости сетей связи в условиях внешних деструктивных воздействий. Патент на изобретение RUS 2379753, 21.04.2008.

67. Гречишников Е. В., Дыбко Л. К., Ерышов В. Г., Жуков А. В., Стародубцев Ю.И. Способ обеспечения устойчивого функционирования системы связи. Патент на изобретение RUS 2405184, 12.05.2009.

68. Стародубцев Ю. И., Гречишников Е. В., Комолов Д. В. Использование нейронных сетей для обеспечения устойчивости сетей связи в условиях внешних воздействий // Телекоммуникации. 2009. № 2. С. 24-31.

69. Фархадов М. П., Душкин Д. Н. Сетецентрические технологии: эволюция, текущее положение и области дальнейших исследований // Автоматизация и современные технологии. 2012. № 1. С. 21-29.

70. Кругликов С. В., Липатов А. А. Развитие автоматизированных систем управления войсками и оружием с учетом сетевых технологий // Информационно-измерительные и управляющие системы. 2013. № 11. С. 39-47.

71. Арзуманян Р. В. Стратегические ориентиры армии США в новых условиях посткризисного мира. – М.: АНО «Центр стратегических оценок и прогнозов», 2012. – 20 с. – URL: www.csef.ru (дата обращения 22.01.2014).

72. Манойло А. В. Государственная информационная политика в особых условиях: Монография. – М.: МИФИ, 2003. – 388 с.

73. Почепцов Г. Г. Информационно-психологическая война. – М.: СИНТЕГ, 2000. – 180 с.

74. Почепцов Г. Г. Информационно-политические технологии. М.: Центр, 2003. – 384 с.

75. Расторгуев С. П., Литвиненко М. В. Информационные операции в сети Интернет / Под общ. ред. А.Б. Михайловского. – М.: АНО ЦСОиП, 2014. – 128 с.

76. Расторгуев С. П. Информационная война. – М.: Гелиос АРВ, 2006. – 240 с.

77. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.-корр. РАН Д.А. Новикова. – М.: Издательство физико-математической литературы, 2010. – 228 с.

78. Новиков Д. А., Чхартишвили А. Г. Прикладные модели информационного управления. – М.: ИПУ РАН, 2004. – 129 с.

79. Доклад ООН World Investment Report, приведенного по материалам статьи В. Иноземцева «Приближение к адекватности» // BusinessWeek Россия [Электронный ресурс], 2005. – URL: http://www.csef.ru/index.php/ru/component/csef/project/ (дата обращения 22.01.2014).

80. Воробьев И. Н., Киселев В. А. От современной тактики к тактике сетецентрических действий // Военная мысль. 2020. № 13. С. 365-399.

81. Буренов В. М. Философский фундамент военного строительства. Новый облик армии – высокая готовность предоставить оборонные услуги // Независимое военное обозрение [Электронный ресурс], 2011. – URL: http://nvo.ng.ru/concepts/2011-08-19/8_army.html (дата обращения 19.08.2016).

82. Копылов А. В. К вопросу о критике концепции "сетецентрических" войн (операций) в американских СМИ // Военная история и футурология [Электронный ресурс]. 2011. – URL: http://www.milresource.ru/Kop-NCW.html (дата обращения 19.01.2016).

83. Михайлов В. А. Разработка методов и моделей анализа и оценки устойчивого функционирования бортовых цифровых вычислительных комплексов в условиях преднамеренного воздействия сверхкоротких электромагнитных излучений. Дисс… докт. техн. наук / Михайлов В.А.– М.: НИИ «Аргон», 2014. – 390 с.

84. Арзуманян Р. В. Кромка Хаоса. Сложное мышление и сеть: парадигма нелинейности и среда безопасности XXI века. – М.: Регнум, 2012. – 600 с.

85. Macmaster H. R. On War: Lessons to be Learned. 2008.

86. Warden J. A. The Air Campaign: Planning for Combat. – National Defense University Press Publication, 1988.

87. Vego M. Net-Centric Is Not Decisive // U.S. Naval Institute Proceedings. 2003. – P. 52.

88. MilNET: военные сети США // Журнал «Хакер» [Электронный ресурс]. – URL: http://www.xakep.ru/post/39495/ (дата обращения 01.08.2007).

89. Соколов Ю. И. Риски высоких технологий. – М.: ФГУ ВНИИ ГОЧС (ФЦ), 2009. – 312 с.

90. Кондратьев А. Е. Боевые роботы США – под водой, в небесах и на суше // Независимое военное обозрение [Электронный ресурс], 2005. – URL: http://nvo.ng.ru/armament/2010-05-14/8_robots.html (дата доступа 23.06.2016).

91. Тайвань показал новую боевую ДУМ // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/88560-tayvan-pokazal-novuyu-boevuyu-dum.html (дата доступа 29.06.2016).

92. Беспилотные летательные аппараты: справочное пособие / под общ. ред. С.А. Попова. – Воронеж: Научная книга, 2015. – 619 с.

93. Робот стреляет первым // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/91499-robot-strelyaet-pervym.html (дата доступа 29.06.2016).

94. Копылов А. В. О слабых сторонах американской концепции «сетецентрических войн (операций)» // Военная мысль. 2011. № 7. С. 53-62.

95. Сидорин А. Н. Прищепов В. М., Акуленко В. П. Вооруженные силы США в XXI веке: Военно-теоретический труд. – М.: Кучково поле; Военная книга, 2013. - 800 с.

96. Heickero R. 152006 CCRTS. Sorne thoughts оп the application of military theory to Iпfоппatiоп Operations and Network Centric Warfare. Iпfоппatiот Operations/Assurance. – Stockhohn: Swedish Defence Research Agency.

97. Попов В., Федутинов Д. Тенденции развития систем передачи данных при использовании БЛА // Зарубежное военное обозрение. 2006. № 4. С. 47-51.

98. Кондратьев А. Е. Программа ВВС США «умный танкер» или новый подход к старой модели // Аэрокосмическое обозрение. 2008. № 1. С. 34-38.

99. Dekker A. Taxonomy of Network Centric Warfare Architectures. – Canberra, Defence Science & Technology Organisation DSTO Fern Hill. Department of Defence.

100. Clausewitz C-V (1832). On War. – Stockholm: Bonnier Fakta Bokforlag, 1832.

101. Strange J, Iron R. Understanding Centres of Gravity and Critical Vulnerabilities. Research paper. 2001.

102. NATO's Operational Planning Process. The COPD – Comprehensive Operations Planning Directive [Электронный ресурс]. – URL: https://semanticu.files.wordpress.com/2014/09/02-1100-1200-nato-operational-planning-process-copd.pdf (дата доступа 24.03.2017).

103. Echevarria A. J. Clausewitz center of gravity its not what we thought // Naval War College Review. 2003. Vol. 56, № 1.

104. Wanden J Centers of gravity in military operations // Preliminary draft. – Royal Swedish Defence College, 2004.

105. Боевые роботы в будущих войнах: выводы экспертов (Часть 1) // Независимое военное обозрение [Электронный ресурс]. 2016. – URL: http://nvo.ng.ru/armament/2016-03-04/1_robots.html (дата доступа 29.06.2016).

106. Боевые роботы в будущих войнах: выводы экспертов (Часть 2) // Зарубежное военное обозрение [Электронный ресурс]. 2016. – URL: http://nvo.ng.ru/armament/2016-03-04/5_robots2.html (дата доступа 29.06.2016).

107. Разгуляев А. Перспективные мобильные адаптивные сети передачи информации для СВ США // Зарубежное военное обозрение. 2008. № 1. С. 35-39.

108. Шнепс М. А. От IN к IMS. О сетях связи военного назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 1. С. 1-11.

109. Сизов В. Ю. Какие боевые роботы нужны России? // Военное обозрение [Электронный ресурс]. 2016. – URL: https://topwar.ru/91962-kakie-boevye-roboty-nuzhny-rossii.html (дата доступа 29.06.2016).

110. Бабинов В. И все же «мул» помог // Военное обозрение [Электронный ресурс]. 2016. – URL: https://topwar.ru/89265-i-vse-zhe-mul-pomog.html (дата доступа 29.06.2016).

111. Постников А. Н., Хамзатов М. М. Сухопутные войска будущего // Независимое военное обозрение [Электронный ресурс]. 2015. – URL: http://nvo.ng.ru/concepts/2015-09-11/4_future.html (дата доступа 23.02.2016).

112. Net-Centric Environment Joint Functional Concept. 2005. – URL: http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf (дата обращения 22.01.2014).

113. Bodnar J. W. The Military Technical Revolution – From Hardware to Information // Naval War College Review. 1993. Vol. 46. p. 7.

114. Абросимов В. К. Групповое движение интеллектуальных летательных аппаратов в антагонистической среде: Монография. – М.: Наука, 2013. – 168 с.

115. Верба В. С., Меркулов В. И., Харьков В. П. Оптимальное групповое управление беспилотными летательными аппаратами в сетецентрической системе // Информационно-измерительные и управляющие системы. 2013. № 11. С. 48-53.

116. Рябов К. Новости проекта CBARS (США) // Военное обозрение [Электронный ресурс]. 2016. – URL: https://topwar.ru/91693-novosti-proekta-cbars-ssha.html (дата доступа 29.06.2016).

117. Настоящее и будущее беспилотной авиации. Часть 1 // Военное обозрение [Электронный ресурс]. 25.01.2016. – URL: https://topwar.ru/89642-nastoyaschee-i-buduschee-bespilotnoy-aviacii-chast-1.html (дата обращения 29.06.2016).

118. Настоящее и будущее беспилотной авиации. Часть 2 // Военное обозрение [Электронный ресурс]. 28.01.2016. – URL: http://topwar.ru/89909-nastoyaschee-i-buduschee-bespilotnoy-aviacii-chast-2.html (дата обращения 23.02.2016).

119. Баталин Е. Создание в США оружия на новых физических принципах // Зарубежное военное обозрение. 2015. № 6. С. 31-40. – URL:http://pentagonus.ru/publ/sozdanie_v_ssha_oruzhija_na_novykh_fizicheskikh_principakh_2015/81-1-0-2615 (дата обращения 10.08.2016).

120. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты: Монография. – СПб.: Свое издательство, 2013. – 166 с.

121. Богданов А. Е., Попов С. А., Иванов М. С. Перспективы ведения боевых действий с использованием сетецентрических технологий // Военная мысль. 2014. № 3. С. 3-13.

122. Богданов А. Е., Попов С. А., Иванов М. С. Компенсационные способы борьбы с прицельными по частоте помехами в системах авиационной радиосвязи, использующих псевдослучайную перестройку рабочей частоты // Радиотехника. 2013. № 8. С. 85-90.

123. Исследование технических путей построения унифицированных радиосредств цифровой автоматизированной системы авиационной радиосвязи. Отчет о НИР: шифр «Сапсан» / Рук.: А.Д. Виноградов, отв. исп.: М.С. Иванов, исп.: С.А. Попов и др. – Воронеж: ВУНЦ ВВС «ВВА», 2013.

124. Иванов М. С., Березин А. В., Фокин С. В. Обоснование требований к системе авиационной радиосвязи Вооруженных сил Российской Федерации // IV Международная научно-техническая конференция авиационного факультета учреждения образования «Военная академия Республики Беларусь». – Минск: ВА РБ, 2013. – С. 108-111.

125. Иванов М. С., Попов С. А., Дахужев А. С. Направления и тенденции развития средств авиационной радиосвязи // IV Международная научно-техническая конференция авиационного факультета учреждения образования «Военная академия Республики Беларусь». 2013. С. 111-114.

126. Иванов М. С. Развитие спутниковых и сотовых платформ передачи данных // Воронежский форум инфокоммуникационных и цифровых технологий. Перспективные исследования и разработки в области информационных технологий и связи. – Воронеж, 2014. – С. 34-35.

127. Иванов М. С., Попов С. А. Применение теории сетецентрических войн войсками НАТО // Охрана, безопасность, связь 2013: материалы международной научно-практической конференции. Часть 2. – Воронеж: Воронежский институт МВД России, 2014. – С. 157-164.

128. Акбашев Б. Б., Балюк Н. В., Кечиев Л. Н. Защита объектов телекоммуникаций от электромагнитных воздействий. – М.: Грифон, 2014. – 472 с.

129. Иванов М. С., Рябков П. В., Петренко С. В. Причины формирования технических каналов утечки информации // Алгоритмические и программные средства в информационных технологиях, радиоэлектронике и телекоммуникациях: сб. статей II международной заочной научно-технической конференции. – Тольятти: ПВГУС, 2014. – С. 179-101.

130. Иванов М. С., Попов С. А., Дахужев А.С. Геоинформационные системы на службе армии // Информатика: проблемы, методология, технологии: Материалы XIV Международной научно-методической конференции, 7-8 февраля 2014 г. Том 6. – Воронеж: ВГУ, 2014. – С. 23-26.

131. Гриняев С. Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 232 с.

132. Laser Weapon System (LaWS) // YouTube [Электронный ресурс]. 08.04.2013. – URL: https://www.youtube.com/watch?v=OmoldX1wKYQ&feature=youtu.be (дата обращения 19.01.2017).

133. США намерены оснащать военные корабли лазерным оружием // Информационное агентство РИА-новости [Электронный ресурс]. 2013. – URL: https://ria.ru/world/20130409/931642.html (дата доступа 09.04.2013).

134. ВМС США вооружились лазерной пушкой, чтобы сбивать дроны, сообщают СМИ // Информационное агентство РИА-новости [Электронный ресурс]. 18.11.2014. – URL: https://ria.ru/defense_safety/20141118/1033980337.html (дата обращения 19.01.2017).

135. Area Defense Anti-Munitions (ADAM) // Lockheed Martin [Электронный ресурс]. 2012. – URL: http://www.lockheedmartin.com/us/products/ADAM.html (дата обращения 19.01.2017).

136. Lockheed Martin Demonstrates New Ground-Based Laser System in Tests Against Rockets and Unmanned Aerial System // Lockheed Martin [Электронный ресурс]. 27.11.2012. – URL: http://www.lockheedmartin.com/us/news/pressreleases/2012/november/1127-ss-adam.html (дата обращения 19.01.2017).

137. 2005 Defense Base Closure and Realignment Commission Report. – U.S. Department of Defense, 2007. – URL: www.brac.gov/docs/final/Volume2BRACReport.pdf (дата доступа 08.05.2013).

138. ГОСТ 50992-96. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008. – 12 с.

139. Marine Corps Systems Command Equipping Our Marines [Электронный ресурс]. – URL: http://www.marcorsyscom.usmc.mil/sites/cins/INTEL/SIGNINIT/JWICS.html (дата доступа 08.05.2013).

140. Ground-based Midcourse Defense [Электронный ресурс]. – URL: http://www.boeing.com/defensespace/space/gmd/index.html (дата доступа 08.05.2013).

141. Emanuelson J. Soviet Test 184 // Future Science [Электронный ресурс]. – URL: http://www.futurescience.com/emp/test184.html (дата доступа 03.03.2016).

142. Excalibur Prototype Extends Reach of High-Energy Lasers // DARPA [Электронный ресурс]. 03.06.2014. – URL: http://www.darpa.mil/news-events/2014-03-06 (дата обращения 19.01.2017).

143. Rheinmetall: Successful Target Engagement with High-Energy Laser Weapons // Defence-Aerospace.ru [Электронный ресурс]. 22.11.2014. – URL: http://www.darpa.mil/news-events/2014-03-06 (дата обращения 19.01.2017).

144. Полтавский А. В. Беспилотные летательные аппараты в системе вооружения / А.В. Полтавский // Научный вестник МГТУ ГА. 2011. № 163. С. 163-170.

145. Макаренко С. И., Бережнов А. Н. Перспективы использования сетецентрических технологий управления боевыми действиями и проблемы их внедрения в Вооруженных Силах Российской Федерации // Вестник Академии военных наук. 2011. № 4. С. 64-68.

146. Чекунов Е. Применение БЛА ВС США в военных конфликтах // Зарубежное военное обозрение 2010. № 7. С. 41-50.

147. 2015: начало заката эры беспилотных летательных аппаратов // Новости ВПК [Электронный ресурс]. – URL: http://vpk.name/news/124839_2015_nachalo_zakata_eryi_bespilotnyih_letatelnyih_apparatov.html (дата доступа 06.04.2016 г.).

148. Arquilla J. Ronfeldt D. F. Networks and netwars: the future of terror, crime, and militancy. – Santa-Monica: Rand Corporation, 2001. – 380 p.

149. Изборский клуб – ИДК. Доклад Изборскому клубу [Электронный ресурс]. – URL: http://www.dynacon.ru/content/articles/2318/ (дата обращения 22.01.2014).

150. Новичков Н. Зона действий – от Афганистана до Африки // Военно-промышленный курьер. 2012. № 6. С. 41-50.

151. Щербаков В. В грядущих войнах дроны составят основной класс летательных аппаратов // Военно-промышленный курьер. 2012. № 36 (453) С. 51-60.

152. Blaker J. R. Transforming military force: the legacy of Arthur Cebrowski and network centric warfare. – Greenwood Publishing Group, 2007.

153. Hersprin D. R. Rumsfeld's Wars: The Arrogance of Power. – Lawrence, Kans.: University Press of Kansas, 2008.

154. Smith E. A. Effects based Operations. Applying Network centric Warfare in Peace, Crisis and War. – Washington, DC: DoD CCRP, 2002.

155. Burke M. Information Superiority, Network Centric Warfare and the Knowledge Edge. – Salisbury: DSTO Electronics and Surveillance Research Laboratory, 2000.

156. Living Under Drones: Death, Injury and Trauma to Civilians From US Drone Practices in Pakistan [Электронный ресурс]. – URL: http://livingunderdrones.org/wpcontent/uploads/2012/09/Stanford_NYU_LIVING_UNDER_DRONES.pdf (дата доступа 06.04.2016).

157. McCormick J. M. Achieving battlespace awareness in network-centric warfare by integrating web and agent technologies // Battlespace Digitization and Network-Centric Systems IV. Edited by Suresh, Raja. Proceedings of the SPIE. 2004. Vol. 5441. pp. 61-68.

158. Операции американских беспилотников в Пакистане сравнили с терактами // Lenta.ru [Электронный ресурс]. – URL: http://lenta.ru/news/2012/09/25/drones/ (дата доступа 06.04.2016).

159. Hutchins S. G., Kleinman D. L., Hocevar S. P., Kemple W. G., Porter G. R. Enablers of Self-synchronization for Network-Centric Operations: Design of a Complex Command and Control Experiment // Proceedings of the 6 the international command and control research and technology symposium. – Annapolis: CCRP, 2001.

160. The implementation of network-centric warfare. – Washington. D.C. Office of the Secretary of Defense, 2005.

161. Vego M. Joint operational Warfare. – Washington. D.C. 2009.

162. Затуливетер Ю. С., Семенов С. С. Ориентир – достаточная оборона // Национальная оборона. 2014. № 10 С. 41-50.

163. Андриевский И. А. Некоторые аспекты современных форм и способов враждебного противостояния и вооруженного противоборства // Экономические отношения. 2012. № 1. С.46-63.

164. Сиденко К. С., Илларионов Г.Ю. Применение автономных подводных роботов в войнах будущего // Арсенал. Военно-промышленное обозрение. 2008. № 2. С. 86-93.

165. Бобриков А. А. Методика обоснования решений по огневому поражению противника // Военная мысль. 2011. № 11. С. 43-53.

166. Красильников Р. В. Системы борьбы с необитаемыми аппаратами – асимметричный ответ на угрозы XXI века. – СПб.: Инфо-да, 2013. – 106 с.

167. Иванов А. И., Лазутина Н. А., Сахабетдинов И. У. Сетецентрические аспекты группового поведения автономных подводных аппаратов // Труды конференции «Технические и программные средства систем управления, контроля и измерения». – М.: ИПУ РАН, 2010. – С. 548-551.

168. Гаврилкин С. Н. Основные направления развития и существующие проблемы создания подводной робототехники «двойного» назначения // Труды Всемирной морской технологической конференции. – СПб, 2012. – С. 18-20.

169. Rice J. A. Seaweb as a DTN pilot application // IETF Meeting, DTNRG session. 2006.

170. Фомин А. Н. Прогнозная оценка военно-политической обстановки и сценарии развития России в условиях прогнозируемых действий геополитических и региональных центров сил. Аналитический доклад. – М.: АНО «Центр стратегических оценок и прогнозов», 2013. – 83 с.

171. Путин: агент влияния или компрадор? Часть 2. // Мальчиша-Кибальчиша [Электронный ресурс]. 25.08.2009. – URL: http://malchish.org/index.php?option=com_content&task=view&id=298&Itemid=35 (дата обращения 26.06.2016).

172. Roy T. N. Deployable Autonomous Distributed System: Future Naval Capability in Undersea Warfare // SSC San Diego Biennial Review. Intelligence, Surveillance, and Reconnaissance. 2003. Vol. 3.

173. Капитанец И. М. Война на море. Проблемы развития военно-морской науки. 2001. – URL: http://militera.lib.ru/science/kapitanetz/02.html (дата обращения 22.01.2014).

174. Самардак В. А. Вооруженная борьба и ее развитие в XXI в. Часть 1. – URL: http://www.almanacwhf.ru/index.php?option=com_content&view=article&id=88:vooruzborba1&catid=17:13nomer&Itemid=21 (дата обращения 22.01.2014).

175. FY 2009-2034 Unmanned Systems Integrated Roadmap. – U.S. Department of Defence, 2009.

176. The Navy Unmanned Undersea Vehicle (UUV) Master Plan. – Department of the Navy, USA, 2004.

177. Min Zengfu, Kongiun Junshi Sixiang Gailun [An Introduction to Air Force Military Thinking]. – Beijing: PLA Press. pp. 379-380.

178. McHenry R. ACTUV ASW Continuous Trail Unmanned Vessel Industry Day. – USA, DARPA, 2010.

179. Резяпов Н. Асимметрические угрозы национальным интересам США // Зарубежное военное обозрение. 2005. № 3. С. 26-32.

180. Zhang Wannian, ed., Dangdai Shijie Junshi yu Zhongguo Guofang [China's National Defense and Contemporary World Military Affairs] – Beijing: Military Science Press, 1999. – 80 p.

181. Chen Yong, Xu Guocheng, Geng Weidong, Gao Jishu Tiaojian xia Lujun Zhanyi Xue [The Study of Ground Forces Campaign Theory under High Teclnology Conditions] – Beijing: Military Science Press, 2003. – 71 p.

182. Han, Gao Jishu Zhubu Zhanzhang Lilun Yanjiu. 184 p.

183. Xin Qin, Xinxihua Shidai de Zhanzheng [Warfare in the Iпformation Age]. – Beijing: National Defense University Press, 2000. 10 p.

184. Shen Weiguang, Xinxi Zhangzhen [The New "Oп War"]. – Beijing: People's Publishing House, 1997, 178 p.

185. Yun Shan, Zhimian Xin Junshi – Liaowang Xinwen Zhoukan, 16 p.

186. Song Yongxin, Guo Yizhong, Research into Ground Radar Station Countermeasures for Satellite Reconnaissance. – Nanjing Hangtian Dinazi Duinkang, 2006. – vol. 64, – pp. 37-39.

187. Song Yongxin, Guo Yizhong, Research into Ground Radar Station Countermeasures for Satellite Reconnaissance. – Nanjing Hangtian Dinazi Duinkang, 2006. – pp. 41.

188. Zhu Youwen et al. Gai Jishu Tiaojian Xia de Xinxi Zhan [Information Warfare Under High Technology Conditions]. – Beijing: Military Science Press, 1994, p. 3.

189. Source Center, Wu Chao, Jia Zhaoping, Chu Zhenjiang, Getting close to the mysterious 'informationized' Blue Force. – Beijing: Zhanyou Bao, 2006, p. 3.

190. Zhang, Dangdai Shijie Junshi yu Zhongguo Guofang, p. 80.

191. Макаренко С. И. Робототехнические комплексы военного назначения – современное состояние и перспективы развития // Системы управления, связи и безопасности. 2016. №2. С. 73-132. – URL: http://sccs.intelgr.com/archive/2016-02/04-Makarenko.pdf (дата обращения 20.01.2017).

192. Wang Lu, Zhang Xiaokang Analysis of C4ISR Systern in NCW and Analysis of Its Effectiveness // Lianyungang Zhihui Kongshi yu Fangzhen. 2006.

193. Li Xinqin, Tan Shoulin, Li Hongxia, Model, Simulation Actualization on Threat Maneuver Target Group on Sea // Qingbao Zhihui Kongzhi Xitong yu Fangzhen Jishu [Iпfoпnation Command and Control Systems and Simulation Technology]. 2005.

194. Tan Shoulin, Zhang Daqiao, Effective Range for Terminal Guidance Ballistic Missile Attacking Aircraft Carrier // Qingbao Zhihui Kongzhi yu Fangzhen Jishu [Iпfoпnation Command and Control Systems and Simulation Technology]. 2006. Vol. 28. № 4.

195. Ge Xinliu, Mao Guanghong, Yu Bo Xinxi zhan zhong daodan budui mianlin de wenti yu duici [Problems Faced by Guided Missile Forces in Information Warfare Conditions and Their Countermeasures] // Wo Jun Xixi Zhan Wenji Yanjiu [Military Science Editorial Group]. pp. 188-189.

196. Min Zengfu, Kongjun Junshi Sixiang Gailun [An Outline of Air Force Military Thought]. – Beijing: PLA Press, 2006. – pp. 377-378.

197. Мосалев В. Дистанционно управляемые и автономные подводные аппараты ВМС зарубежных стран // Зарубежное военное обозрение. 2006. № 6. С. 56-66.

198. Russia's Military Capabilities. «Great Power» Ambitions and Reality. – Berlin, 2009.

199. Sun Yiming, Yang Liping, Xinxihua Zhanzheng Zhong de Zhanshu Shuju Lian [Tactical data links in Information Warfare]. pp. 48-50.

200. Military Power of the People's Republic of China. Annual report to congress. – Office of the Secretary of Defense, 2009.

201. Нано- и микросистемная техника. От исследований к разработкам: Сборник статей под редакцией П.П. Мальцева – М.: Техносфера, 2005. – 590 с.

202. Альтман Ю. Военные нанотехнологии. Возможности применения и превентивного контроля вооружений. – М.: Техносфера, 2006. – 424 с.

203. Панов М., Маневич В. Военные конфликты на рубеже 2030 года // Зарубежное военное обозрение. 2008. № 1. С. 3-15.

204. Christensen Th. J. Posing problems without catching up: China's rise and challenges for U.S. security policy // Internet security. 2001. Vol. 25. № 4. P. 5-40.

205. Мясников В. Китай – современное вооружение на любой вкус // Независимое военное обозрение. 2014. № 1. С. 3-15.

206. Молитвин Л.О. Реализации концепции единого информационного пространства НАТО // Зарубежное военное обозрение. 2008. № 1. С. 23-27.

207. Олегин А. НАТО: Максимальная эффективность минимальными средствами // Отечественные записки. 2005. № 5. С. 23-27.

208. NATO after enlargement: New Challenges, New Miss., New Forces. 47 p.

209. The Fundamentals of British Maritime Doctrine. 38 p.

210. Шульман А. Ответ израильских военных на угрозы XXI века // Отечественные записки. 2005. № 5. С. 43-57.

211. Замков В. Новая армия поднебесной // Отечественные записки. 2005. № 5. С. 32-36.

212. Chinese Views of Future Warfare. 84 p.

213. Михайлов Р. Л. Радиоэлектронная борьба в Вооруженных силах США: военно-теоритический труд. – СПб.: Наукоемкие технологии, 2018. – 131 с.

214. China's Military Faces the Future. 53 p.

215. Заполев С. Разведывательное обеспечение перспективных формирований СВ США модульного типа // Зарубежное военное обозрение. 2008. № 10. С. 32-36. – URL: http://pentagonus.ru/publ/80-1-0-842 (дата обращения 10.03.2013).

216. Макаренко С. И., Михайлов Р. Л. Модель функционирования маршрутизатора в сети в условиях ограниченной надежности каналов связи // Инфокоммуникационные технологии. 2014. Том 12. № 2. С. 44–49.

217. Кобаяси Н. Введение в нанотехнологию. – М.: Бином. Лаборатория знаний, 2007. – 134 с.

218. Круглов Е. Перспективы развития американских авиационных средств РЭБ и тактика их применения в современных вооруженных конфликтах // Зарубежное военное обозрение. 2014. № 2. С. 57-63 – URL: http://pentagonus.ru/publ/perspektivy_razvitija_amerikanskikh_aviacionnykh_sredstv_rehb_i_taktika_ikh_primenenija_v_sovremennykh_vooruzhjonnykh_konfliktakh_2014/18-1-0-2480 (дата обращения 06.04.2016).

219. Максименков А. Основные программы ВВС США по созданию средств радиоэлектронной борьбы // Зарубежное военное обозрение. 2010. № 1. С. 54-58. – URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2010-zvo/7943-osnovnye-programmy-vvs-ssha-po-sozdaniju-sredstv (дата обращения 30.07.2014).

220. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292-376. URL: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата обращения 19.01.2017).

221. ADVanced All-electric Networked ship for SEA dominance [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Advansea (дата обращения 25.03.2017).

222. Яшин С. Перспективы развития авиационных групповых средств радиоэлектронной борьбы ВС США // Зарубежное военное обозрение. 2015. № 2. С. 70-75. – URL: http://pentagonus.ru/publ/perspektivy_razvitija_aviacionnykh_gruppovykh_sredstv_radioehlektronnoj_borby_vs_ssha_2015/16-1-0-2598 (дата обращения 06.04.2016).

223. Евграфов В. Развитие авиационных средств РЭБ и их применение в современных вооруженных конфликтах // Зарубежное военное обозрение. 2011. № 2. С. 60-65. – URL: http://pentagonus.ru/publ/razvitie_aviacionnykh_sredstv_rehb_i_ikh_primenenie_v_sovremennykh_vooruzhjonnykh_konfliktakh_2011/18-1-0-2449 (дата обращения 14.07.2016).

224. Исаков Е. Е. Устойчивость военной связи в условиях информационного противоборства. – СПб.: Изд. Политехн. ун-та, 2009. – 400 с.

225. Самсонов Л. П. Результаты экспериментального исследования возможностей создания помех радиорелейным и тропосферным станциям в диапазоне 50...600 МГц // Труды в/ч 25871. 1967. №7 (264). С. 73-84.

226. Электромагнитная пушка выстрелила с максимальной энергией [Электронный ресурс]. – URL: http://www.membrana.ru/particle/17662 (дата обращения 14.07.2016).

227. Противоракетный облик «San Antonio» в рамках усиления живучести американских АУГ: новый вызов для ВМФ России // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/89729-protivoraketnyy-oblik-san-antonio-v-ramkah-usileniya-zhivuchesti-amerikanskih-aug-novyy-vyzov-dlya-vmf-rossii.html (дата обращения 14.07.2016).

228. Гамзатов Ш. Состояние и перспективы разработки в США наземного варианта противоракеты «Стандарт-3» // Зарубежное военное обозрение. 2010. Т. 762. № 9. С. 39-41.

229. Ракета-перехватчик SM-3 (Standard Missile-3) // Досье: Черноморский флот [Электронный ресурс]. 2017. – URL: http://www.flot2017.com/file/show/none/12037 (дата обращения 14.07.2016).

230. Волков С. Космос как поле для битвы (Часть 1) // Воздушно-космическая оборона [Электронный ресурс]. 05.05.2008. – URL: http://www.vko.ru/koncepcii/kosmos-kak-pole-dlya-bitvy-1 (дата доступа 03.03.2016).

231. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93-101.

232. Волков С. Рост воздушной и космической мощи // Воздушно-космическая оборона [Электронный ресурс]. 28.01.2008. – URL: http://www.vko.ru/koncepcii/rost-vozdushnoy-i-kosmicheskoy-moshchi (дата доступа 03.03.2016).

233. Морозов И. В., Баушев С. В. Время нового вида обеспечения // Воздушно-космическая оборона [Электронный ресурс]. 09.10.2016. – URL: http://www.vko.ru/koncepcii/vremya-novogo-vida-obespecheniya (дата доступа 03.03.2016).

234. Клабуков И., Алехин М., Нехина А. Исследовательская программа DARPA на 2015 год (Review of DARPA FY 2015 Research Programs). – М., 2014. – 96 с.

235. Емельянов Ю. Взгляды руководства ВС США на ведение электронной войны в операциях XXI века с использованием сил воздушно-космического нападения // Зарубежное военное обозрение. 2015. № 9. С. 63-72. – URL: http://pentagonus.ru/publ/vzgljady_rukovodstva_vs_ssha_na_vedenie_ehlektronnoj_vojny_v_operacijakh_xxi_veka_s_ispolzovaniem_sil_vozdushno_kosmicheskogo_napadenija_2015/19-1-0-2636 (дата обращения 06.04.2016).

236. Андронов А., Шевров Р. Системы спутников-ретрансляторов, радиолокационной разведки и дистанционной съемки Земли // Зарубежное военное обозрение. 1995. № 3.

237. Меньшиков В. А., Перминов А. Н., Рембеза А. И., Урличич Ю. М. Основы анализа и проектирования космических систем мониторинга и прогнозирования природных и техногенных катастроф. – М.: Машиностроение, 2014. – 736 с.

238. Лавров В. Н. Аналитический обзор космических программ ДЗЗ России и зарубежных стран // ИнноТер [Электронный ресурс]. 2016. – URL: https://innoter.com/scientific-articles/1092 (дата обращения 03.03.2016).

239. Савин Л. В. Сетецентричная и сетевая война. Введение в концепцию. – М.: Евразийское движение, 2011. – 130 с.

240. Barnett T. The Seven Deadly Sins of Network-Centric Warfare. – US Naval Institute, 1999. – URL: http://www.thomaspmbarnett.com/published/7d.htm (дата обращения 20.03.2008).

241. Лавров В. Н. Космические съемочные системы сверхвысокого разрешения // ИнноТер [Электронный ресурс]. 2016. – URL: https://innoter.com/scientific-articles/1092 (дата доступа 03.03.2016).

242. Усов В. Применение коммерческих космических систем оптоэлектронной съёмки земной поверхности в интересах ВС США // Зарубежное военное обозрение. 2010. № 12. С. 53-59. – URL: http://pentagonus.ru/publ/materialy_posvjashheny/2000_nastojashhij_moment/primenenie_kommercheskikh_kosmicheskikh_sistem_optoehlektronnoj_sjomki_zemnoj_poverkhnosti_v_interesakh_vs_ssha/122-1-0-1659 (дата доступа 03.03.2016).

243. Kurc C. Technology Does Not Win Wars. Eurasia Critic. 2009. – URL: http://www.academia.edu/227957/Technology_Does_not_Win_Wars (дата обращения 10.01.2017).

244. Мант С. Д. Военно-разведывательные спутники // ProAtom [Электронный ресурс]. 2011. – URL: http://www.proatom.ru/modules.php?file=print&name=News&sid=3299 (дата доступа 03.03.2016).

245. Куприянов А. И., Шустов Л. Н. Радиоэлектронная борьба. Основы теории. – М.: Вузовская книга, 2011. – 800 с.

246. Романов А., Кошелев А. Космическая радиоэлектронная разведка США // Авиация и космонавтика. 1994. № 5-6. С. 45. – URL: http://epizodsspace.airbase.ru/bibl/a-i-k/1994/5-6/kosm-za-rub.html (дата доступа 03.03.2016).

247. Перунов Ю. М., Фомичев К. И., Юдин Л. М. Радиоэлектронное подавление информационных каналов систем управления оружием / Под ред. Ю.М. Перунова. – М.: Радиотехника, 2003. – 416 с.

248. Леньшин А. В. Бортовые системы и комплексы радиоэлектронного подавления – Воронеж: Научная книга, 2014.– 590 с.

249. Заполев С. Развитие систем сбора, обработки, анализа и распределения разведывательной информации в Сухопутных войсках США // Зарубежное военное обозрение. 2010. № 1. С. 42-50. – URL: http://pentagonus.ru/publ/razvitie_sistem_sbora_obrabotki_analiza_i_raspredelenija_razvedyvatelnoj_informacii_v_sukhoputnykh_vojskakh_ssha/23-1-0-1667 (дата обращения 10.03.2013).

250. Перунов Ю. М., Мацукевич В. В., Васильев А. А. Зарубежные радиоэлектронные средства / Под ред. Ю.М. Перунова. В 4-х книгах. Кн. 2: Системы радиоэлектронной борьбы. – М.: Радиотехника, 2010. – 352 с.

251. Добыкин В. Д., Куприянов А. И., Пономарев В. Г., Шустов Л. Н. Радиоэлектронная борьба. Силовое поражение радиоэлектронных систем / Под ред. А.И. Куприянова. – М.: Вузовская книга, 2007. – 468 с.

252. Радзиевский В. Г., Сирота А. А. Теоретические основы радиоэлектронной разведки. 2-е изд., испр. и доп. – М. Радиотехника, 2004 – 432 с.

253. Жуков В. Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. 2001. № 1. – URL: http://pentagonus.ru/publ/22-1-0-175 (дата обращения 10.01.2017).

254. Козирацкий Ю. Л., Прохоров Д. В., Козирацкий А. Ю., Голубев С. В. Основы информационной и радиоэлектронной борьбы: Учеб. пособие. – Воронеж: ВАИУ, 2009. – 192 с.

255. Осипов В. Ю., Ильин А. П., Фролов В. П., Кондратюк А. П. Радиоэлектронная борьба. Теоретические основы. Учеб. пособие для вузов. – Петродворец: ВМИРЭ, 2006. – 302 с.

256. Иванов И., Чадов И. Содержание и роль радиоэлектронной борьбы в операциях XXI века // Зарубежное военное обозрение. 2011. № 1. С. 14-20. – URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2011-zvo/8094-soderzhanie-i-rol-radiojelektronnoj-borby-v (дата обращения 10.01.2017).

257. Майбуров Д. Г. Анализ современных воздушных платформ радиоэлектронной борьбы иностранных государств // Проблемы безопасности российского общества. 2013. № 2/3. С. 91-96.

258. Романов Н.А. Военно-космическая разведка США в современных военных конфликтах // Pentagonus [Электронный ресурс]. – URL: http://pentagonus.ru/publ/voenno_kosmicheskaja_razvedka_ssha_v_sovremennykh_voennykh_konfliktakh_2012/105-1-0-2260 (дата доступа 03.03.2016).

259. Маршалов К. Американские космические аппараты оптоэлектронной разведки // Зарубежное военное обозрение. 2013. № 10. С. 64-68.

260. Маршалов К. Основные направления развития космических оптико-электронных средств вооруженных сил США // Зарубежное военное обозрение. 2015. № 12. С. 80-82.

261. Орбитальная группировка ВС США // Воздушно-космическая оборона [Электронный ресурс]. – URL: http://old.vko.ru/article.asp?pr_sign=archive.2004.18.17 (дата доступа 03.03.2016).

262. Стреналюк Ю. В. Военная активность в околоземном пространстве. Противоспутниковые системы. – М.: Центр по изучению проблем разоружения, энергетики и экологии при МФТИ, 2005. – URL: http://www.armscontrol.ru/course/lectures05a/yvs050428t.htm (дата доступа 03.03.2016).

263. О противоракетной обороне // Армейский сборник [Электронный ресурс]. 01.11.2012. – URL: http://army-news.ru/2012/11/o-protivoraketnoj-oborone/ (дата доступа 03.03.2016).

264. Компания Sierra Nevada сделает корабль Dream Chaser беспилотным // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/72771-kompaniya-sierra-nevada-sdelaet-korabl-dream-chaser-bespilotnym.html (дата доступа 03.03.2016).

265. Фаличев О. Неуловимые наблюдатели // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/79740-neulovimye-nablyudateli.html (дата доступа 03.03.2016).

266. Строгов С. Перспективные системы спутниковой связи военного назначения ведущих зарубежных стран // Зарубежное военное обозрение. 2009. № 5. С. 50-58.

267. Юферев С. Убийцы спутников // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/68950-ubiycy-sputnikov.html (дата доступа 03.03.2016).

268. Юферев С. Оружие под запретом. Часть 6: Ядерное оружие в космосе // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/64771-oruzhie-pod-zapretom-chast-6-yadernoe-oruzhie-v-kosmose.html (дата доступа 03.03.2016).

269. Остапенко О. Н., Баушев С. В, Морозов И. В. Информационно-космическое обеспечение группировок войск (сил) ВС РФ: Учебно-научное издание. – СПб.: Любавич, 2012. – 368 с.

270. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. № 1 (2). 2014. С. 13-21. – URL: http://cyberrus.com/wp-content/uploads/2014/03/13-21.pdf (дата обращения 10.01.2017).

271. Денисов Б. Б. Проблемы наращивания телекоммуникационного ресурса в интересах функционирования информационно-управляющих систем специального назначения [Доклад] // Мат. всероссийской научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения» / Под ред. Ю.В. Бородакия. – М.: АО «Концерн «Системпром», 2012.

272. Кобозев Ю. Н Перспективы развития систем связи и телекоммуникаций в информационно-управляющих системах специального назначения [Доклад] // Мат. всероссийской научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения». Том 4 «Телекоммуникации и связь в информационно-управляющих системах» / Под ред. Ю.В. Бородакия. – М.: ОАО «Концерн «Системпром», 2013. – С. 7-9.

273. Шептура В. Н. Архитектура перспективной системы связи группировки войск (сил) для обеспечения управления адаптивными действиями войск (сил) [Доклад] // Мат. всероссийской научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения». Том 4: «Телекоммуникации и связь в информационно-управляющих системах» / Под ред. Ю.В. Бородакия. – М.: ОАО «Концерн «Системпром», 2013. – С. 16-20.

274. Связь в Вооруженных силах Российской Федерации – 2013: Тематический сборник / Под ред. А.В. Абрамовича, А.В. Герасимова, С.В. Цибина, К.С. Ометова, Ю.А. Быстрова. – М.: ООО «Компания «Информационный мост», 2013. – 216 с.

275. Оружие и технологии России. Энциклопедия. XXI век. Системы управления, связи и радиоэлектронной борьбы / Под общ. ред. С. Иванова. – М.: Изд. дом «Оружие и технологии», 2006. – 695 с.

276. Osborn Kr. Adaptive electronic warfare // Army AL&T. 2013. № 1. pp. 44-48.

277. Додонов А. Г. Живучесть информационных систем. – Киев: Наук. думка, 2011. – 256 с.

278. Громов Ю. Ю., Драчев В О., Набатов К. А., Иванова О. Г. Синтез и анализ живучести сетевых систем: монография. – М.: Издательство Машиностроение-1, 2007. – 152 с.

279. Стекольников Ю. И. Живучесть систем. – СПб.: Политехника, 2002. – 155 с.

280. Попков В. К. Математические модели связности. – Новосибирск: ИВМиМГ СО РАН, 2006. – 490 с.

281. Тулин С. Органы управления ВС США боевыми действиями в кибернетическом пространстве // Зарубежное военное обозрение. 2012. № 2. С. 3-10. – URL: http://pentagonus.ru/publ/materialy_posvjashheny/2000_nastojashhij_moment/organy_upravlenija_vs_ssha_boevymi_dejstvijami_v_kiberneticheskom_prostranstve_2012/122-1-0-2083 (дата обращения 23.01.2017).

282. Димлевич Н. Информационные войны в киберпространстве – США // Pentagonus [Электронный ресурс]. 2010. – URL: http://pentagonus.ru/publ/informacionnye_vojny_v_kiberprostranstve_ssha_i/80-1-0-1610 (дата обращения 23.01.2017).

283. Колга М. НАТО: Краткий справочник / М. Колга и д.р. – Таллин: Eesti Entsüklopeediakirjastus, 2007. – 543 с.

284. Очередной успешный тест усовершенствованной противоракеты GBI // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/90207-mda-ocherednoy-uspeshnyy-test-gm-ctv-02-usovershenstvovannoy-protivorakety-gbi.html (дата доступа 06.02.2016).

285. Подберезкин А. И. Сценарий развития системы ПРО как глобальной стратегии США // СМИ-Online [Электронный ресурс]. 04.060.2015 – URL: http://topwar.ru/85355-rossiyskie-eksperty-ne-veryat-v-kitayskiy-giperzvukovoy-samolet.html (дата доступа 03.03.2016).

286. Курушкин С. М. Противоракетный щит США // Воздушно-космическая оборона [Электронный ресурс]. – URL: http://old1.vko.ru/DesktopModules/Articles/ArticlesView.aspx?tabID=320&ItemID=460&mid=2892&wversion=Staging (дата доступа 03.03.2016).

287. Козин В. «Иджис» – прямая угроза России // Национальная оборона. 2012. № 4. С. 39-44.

288. Щербинин Р. Разработка и летные испытания экспериментальных ГЛА // Зарубежное военное обозрение. 2003. № 7. С. 50-56.

289. Военная стратегия / Под ред. В.Д. Соколовского. – М.: Воениздат, 1963. – 504 с.

290. Ивлев А. А. Основы теории Бойда. Направления развития, применения и реализации: Монография. – М., 2008. – 64 с.

291. Ермишян А. Г., Сызранцев Г. В., Дыков В. В. Теоретические и научно-практические основы построения систем связи в локальных войнах и вооруженных конфликтах: учебное пособие / Под ред. А. Г. Ермишяна. – СПб.: ВАС, 2006. – 220 с.

292. Шеховцеов Н. П., Кулешов Ю. Е. Информационное оружие: теория и практика применения в информационном противоборстве // Вестник Академии военных наук. 2012. № 1 (38). С. 35-40.

293. Юферев С. Российские эксперты не верят в китайский гиперзвуковой самолет // Военное обозрение [Электронный ресурс]. – URL: http://topwar.ru/85355-rossiyskie-eksperty-ne-veryat-v-kitayskiy-giperzvukovoy-samolet.html (дата доступа 03.03.2016).

294. Кременчуцкий А. Л., Дворянов Е. Я., Волков В. Ф. Международный терроризм - главная угроза XXI века: Учеб. пособие. – СПб.: ВАС, 2005. – 256 с.

295. Березкин Г. А. и др. Уроки и выводы из войны в Ираке // Военная мысль. 2003. № 7. С. 58-78.

296. Гареев М. А., Цыганок А. Д. Уроки и выводы из войны в Ираке // Военная мысль. 2003. № 8. С. 68-80.

297. Корабельников А. А., Чебан В. В. Уроки и выводы из войны в Ираке // Военная мысль. 2003. № 9. С. 75-80.

298. Батюшкин С. А., Дульнев П. А. Война в Ираке: анализ событий, уроки и выводы // Вестник Академии военных наук. 2004. № 2 (7). С. 43-47.

299. Свиридов А. Некоторые особенности операции «Свободу Ираку» // Зарубежное военное обозрение. 2003. № 4. С. 2-6.

300. Владимиров В. А., Лебедев А. В. Анализ состояния и тенденций развития современных видов оружия // Стратегия гражданской защиты: проблемы и исследования. 2012. № 2. С. 61-80. – URL: http://cyberleninka.ru/article/n/analiz-sostoyaniya-i-tendentsiy-razvitiya-sovremennyh-vidov-oruzhiya (дата обращения 23.01.2017).

301. Дрожжин А. И., Алтухов Е. В. Воздушные войны в Ираке и Югославии. – М.: Техника молодежи, 2002. – 80 с.

302. Ямпольский Л. С. Обобщенный анализ применения средств воздушного нападения ОВС НАТО при проведении военной операции в Югославии «Решительная сила» и в других локальных войнах в 90-х годах: Учебное пособие. – Ульяновск: УлГТУ, 2000. – 80 с.

303. Ермишян А. Г. Теоретические основы построения систем военной связи в объединениях и соединениях: Учебник. Ч. 1: Методологические основы построения организационно-технических систем военной связи. – СПб.: ВАС, 2005.

304. Китай приводит армию в боевую готовность // Expert Online [Электронный ресурс]. – URL: http://expert.ru/2015/11/27/kitaj/ (дата доступа 27.11.2015).

305. Цыганок А. Д. Война в Ливии: циничная ложь НАТО (часть 1) // Оружие России [Электронный ресурс]. 21.10.2012. – URL: http://www.arms-expo.ru/news/archive/voyna-v-livii-cinichnaya-lozh-nato-chast-1-21-10-2012-19-44-00/?sphrase_id=10574728 (дата обращения 13.11.2015).

306. Цыганок А. Д. Война в Ливии: циничная ложь НАТО (Часть 2) // Оружие России [Электронный ресурс]. 11.11.2012. – URL: http://www.arms-expo.ru/news/archive/voyna-v-livii-cinichnaya-lozh-nato-chast-2-11-11-2012-12-05-00/ (дата обращения 13.11.2015).

307. Быстров А. А. Некоторые итоги военной операции Франции в Ливии // Институт Ближнего Востока [Электронный ресурс]. – URL: http://www.iimes.ru/rus/stat/2011/16-10-11.htm (дата доступа 13.11.2015).

308. Война в Ливии. США применили новейший самолет радиоэлектронной борьбы // Оружие России [Электронный ресурс]. 03.04.2011. – URL: http://www.armsexpo.ru/news/weapons_in_the_world/voyna-v-livii-ssha-primenili-noveyshiy-samolet-radioelektronnoy-bor-by03-04-2011-00-04-00/ (дата обращения 13.11.2015).

309. Гушер А. И. Военные и политические итоги четырех месяцев войны НАТО против Ливии // Материк [Электронный ресурс]. 21.07.2011. – URL: http://www.materik.ru/rubric/detail.php?ID=13491&print=Y (дата обращения 13.11.2015).

310. Троян А. Основные итоги и уроки военной компании в Ливии // Зарубежное военное обозрение. 2012. № 4. С. 1-8. – URL: http://factmil.com/publ/strana/nato/osnovnye_itogi_voennoj_kompanii_zapada_v_livii_2012/61-1-0-98 (дата обращения 26.01.2016).

311. Цыганок А. Д. Война в Ливии: итоги и уроки // Арсенал Отечества. 2012. № 2. – URL: http://arsenal-otechestva.ru/article/139 (дата обращения 26.01.2016).

312. Кузнецов А. Ю. Ливия год спустя: печальные итоги // Российский академический журнал. 2012. Т. 20. № 2. С. 16-20.

313. Цыганок А. Д. Чему научило НАТО ливийское небо // Военный обозреватель [Электронный ресурс]. – URL: http://warsonline.info/liviya/chemu-nauchilo-nato-liviyskoe-nebo.html (дата доступа 13.11.2015).

314. Цыганок А. Д. В чем уникальность 240-дневной Ливийской войны // Искусство войны [Электронный ресурс]. 03.03.2012. – URL: http://navoine.info/lybia-war-unique.html (дата обращения 13.11.2015).

315. Хазматов В. В. Влияние концепции сетецентрической войны на характер современных операций // Военная мысль. 2006. № 7. С. 13-17.

316. Мяснико В. Лазерные амбиции Пентагона остыли до киловаттного уровня // Независимое военное обозрение [Электронный ресурс]. 05.08.2011. – URL: http://nvo.ng.ru/armament/2011-08-05/8_pentagon.html (дата обращения 28.01.2016).

317. Армия США провела испытания наземного боевого лазера против воздушных целей // Независимое военное обозрение [Электронный ресурс]. 13.12.2013. – URL: http://nvo.ng.ru/news/452359.html (дата обращения 28.01.2016).

318. Гаврилов А. Автоматизированная система сбора, обработки и распределения разведывательной информации СВ США DCGS-A // Зарубежное военное обозрение. 2010. № 7. С. 32-40.

319. Паршин С., Кожанов Ю. Современные тенденции в совершенствовании системы управления вооруженными силами ведущих зарубежных стран в информационную эпоху // Зарубежное военное обозрение. 2009. № 7. С. 3-9.

320. Крылов А. Космические системы военной связи США: анализ состояния и развития // Военное обозрение [Электронный ресурс]. – URL: http://topwar.ru/34992-kosmicheskie-sistemy-voennoy-svyazi-ssha-analiz-sostoyaniya-i-razvitiya.html (дата доступа 03.03.2015).

321. Шнепс-Шнеппе М. А. «Красный телефон» на DISN сети как родимое пятно в среде AS-SIP // International Journal of Open Information Technologies. 2015. Т. 3. № 6. С. 7-12.

322. Шнепс-Шнеппе М. А. Об эволюции телекоммуникационных сервисов на примере GIG // International Journal of Open Information Technologies. 2015. Т. 3. № 1. С. 1-13.

323. Шнепс-Шнеппе М. А., Намиот Д. Е., Цикунов Ю. В. Телекоммуникации для военных нужд: сеть GIG-3 по требованиям кибервойны // International Journal of Open Information Technologies. 2014. Т. 2. № 10. С. 3-13.

324. Военная сеть США будет построена на маршрутизаторах Juniper Networks // Poplar Systems [Электронный ресурс]. – URL: http://www.poplar.ru/view.php3?cls=news&vguid=1256&guid=1256&parent=1255 (дата доступа 03.03.2015).

325. Янов О., Ширяев В. Участие Министерства обороны США в федеральной программе создания «Среды совместного использования информации» // Зарубежное военное обозрение. 2011. № 12. С. 15-21.

326. Попов И. М. Военные конфликты: взгляд за горизонт // Независимое военное обозрение [Электронный ресурс]. – URL: http://nvo.ng.ru/concepts/2013-04-12/1_conflicts.html (дата доступа 28.01.2016).

327. Сетевые Тактические Информационные Системы коалиционных сил // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/65261-setevye-takticheskie-informacionnye-sistemy-koalicionnyh-sil.html (дата доступа 03.03.2015 г.).

328. Богданов С. Военные конфликты (Особенности и закономерности в их подготовке и проведении) // Армейский сборник. 2013. № 9. С. 34-37.

329. Cebrowski A. K., Garstka J. J. Network-Centric Warfare: Its Origin and Future // U.S. Naval Institute Proceedings. – Annapolis (Maryland), 1998.

330. Alberts D. S., Garstka J. J., Stein F. P. Network Centric Warfare: Developing and Leveraging Information Superiority. 2-nd Edition (Revised). – US Department of Defense C4ISR Cooperative Research Program Publications Series, 2001. – 292 p. – URL: http://www.dodccrp.org/files/Alberts_NCW.pdf (дата обращения 19.01.2016).

331. Alberts D. S., Garstka J. J., Hayes R. E., Signori D. A. Understanding Information Age Warfare. – Washington: CCRP, 2001. – 319 p.

332. Smith E. A. Effects Based Operations. Applying Network Centric Warfare in Peace, Crisis, and War). – Washington: CCRP, 2006. – 602 p.

333. Dombrowski P. J., Gholz E. Ross A. L. Military Transformation and the Defense Industry After Next: The Defense Inductrial Implications of Network-Centric Warfare. – Newport: Naval War College, 2002. – 127 p.

334. Управление высокоточным оружием: учебное пособие / В.Ф. Волков, Н.В. Груздев, А.И. Колдунов, М.П. Шилин. – СПб.: ВКА имени А.Ф. Можайского, 2006. – 96 с.

335. Вильданов М., Резяпов Н. Оснащение ПЛАРБ ВМС США неядерными средствами поражения // Зарубежное военное обозрение. 2007. № 5.

336. Чириков А.Г., Бойко А.В., Василишин И.И., Крылов С.Е., Кубиков Н.Н., Кузьмин А.И., Осипов Д.М., Письменский Н.В., Чумаченко А.П., Кашарный В.В. Организация гражданской обороны в субъекте Российской Федерации (муниципальном образовании): Учебное пособие / Под общ. ред. А.Г. Чирикова. – Химки: ФГБОУ ВПО АГЗ МЧС России, 2012. – 216 с.

337. Подберезкин А.И. Евразийская ВКО: роль стратегических неядерных вооружений // Вестник МГИМО-Университета. 2013. № 1. С. 29-37.

338. Щербинин Р. Перспективные боевые части высокоточного оружия США // Зарубежное военное обозрение. 2010. № 4. С. 58-63.

339. Дьяков А. С. «Быстрый глобальный удар» в планах развития стратегических сил США. Доклад центра по изучению проблем разоружения, энергетики и экологии при МФТИ. – М.: МФТИ, 2007.

340. Ягольников С., Храмичев А., Панин В. Войны высокоточных технологий // Армейский вестник [Электронный ресурс]. – URL: http://army-news.ru/2011/08/vojny-vysokotochnyx-texnologij/ (дата доступа 03.03.2015).

341. Усачев В. А., Голов Н. А., Кудрявцев Н. В. Перспективные технические решения и тенденции развития радиоэлектронных систем наведения для высокоточного оружия класса «воздух-поверхность» // Наука и образование. 2011. № 10. С. 1-5.

342. Американская автоматизированная система управления войсками тактического уровня FBCB2 (Часть 1) // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/32374-amerikanskaya-avtomatizirovannaya-sistema-upravleniya-voyskami-takticheskogo-urovnya-fbcb2-chast-1.html (дата доступа 03.03.2015).

343. Янов О. Система боевого управления Сухопутных войск США в звене «Бригада и ниже» // Зарубежное военное обозрение. 2012. № 2. С. 43-50.

344. Алексеев А. Системы управления боем американской армии. Текущее положение и ориентированная на будущее стратегия модернизации // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/64190-sistemy-upravleniya-boem-amerikanskoy-armii-tekuschee-polozhenie-i-orientirovannaya-na-buduschee-strategiya-modernizacii.html (дата доступа 03.03.2015).

345. Затуливетер Ю. С. Компьютерный базис сетецентрического управления // Труды Второй Российской конференции с международным участием «Технические и программные средства систем управления, контроля и измерения» УКИ-2010. – М.: ИПУ РАН, 2010. – С. 492-511.

346. Фоличев О. На пороге гиперзвукового прорыва // Военные новости [Электронный ресурс]. – URL: http://dokwar.ru/publ/vooruzhenie/aviacija_i_flot/na_poroge_giperzvukovogo_proryva/15-1-0-1000 (дата доступа 03.03.2016).

347. Душенов К. Военный гиперзвук: Россия и США – наперегонки со смертью [Электронный ресурс]. – URL: http://www.liveinternet.ru/users/raduga_podruga/post347255994/ (дата доступа 03.03.2015).

348. Капцов О. Демоны трех стихий. «Калибр» против «Томагавка» // Военное обозрение [Электронный ресурс]. – URL: https://topwar.ru/84614-demony-treh-stihiy-kalibr-protiv-tomagavka.html (дата доступа 03.03.2015).

349. Манойло А. В. Объекты и субъекты информационного противоборства // Пси-фактор [Электронный ресурс]. 2003. – URL: http://psyfactor.org/lib/psywar24.htm (дата обращения 20.09.2016).

350. Joint Publication 3-13.1. Electronic Warfare. US Joint Chiefs of Staff. – URL: https://fas.org/irp/doddir/dod/jp3-13-1.pdf (дата доступа 20.09.2016).

351. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. – Washington D.C.: The White House, 2009.

352. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. – Washington D.C.: The White House, 2011.

353. Department of Defense Strategy for Operating in Cyberspace. – Washington D.C.: U.S. Department of Defense, 2011.

354. AFDD 3-12. Cyberspace Operations. – USAF, 2010. – 60 p.

355. AFDD 3-13. Information Operations. –USAF, 2011. – 65 p.

356. AFPD 10-7. Information Operations. – USAF, 2006. – 29 p.

357. DoDD 3600.1. Information Operations. – US DoD, 2013. – 12 p.

358. Information Operations Primer: Fundamentals of Information Operations. – U.S. Army War College, 2011. – 204 p.

359. JP 3-13. Information Operations. – US Joint Chiefs of Staff, 2012. – 69 p.

360. Стандарт ISO/IEC 27032:2012. Информационные технологии. Методы обеспечения безопасности: Руководящие указания по обеспечению кибербезопасности. 2012.

361. Греков В. Автоматизированные системы обработки и анализа разведывательных данных ASAS // Зарубежное военное обозрение. 1990. № 12. С. 27-35. – URL: http://pentagonus.ru/publ/80-1-0-797 (дата обращения 10.03.2013).

362. Стандарт ITU-T X.1205:2008. Обзор кибербезопасности. 2008. – Женева: МСЭ-Т, 2008. – 162 с. – URL: www.itu.int/ITU-T (дата обращения 20.01.2014).

363. Безопасность в электросвязи и информационных технологиях. Обзор содержания и применения действующих Рекомендаций МСЭ-Т для обеспечения защищенной электросвязи. – Женева: МСЭ-Т, 2009. – 162 с. – URL: www.itu.int/ITU-T (дата обращения 20.01.2014).

364. Почепцов Г. Г. Информационные войны. – М.: Рефл-бук, Киев: Ваклер, 2000. – 576 с.

365. Расторгуев С. П. Информационная война. – М: Радио и связь, 1999. – 416 с.

366. Антонович П. И. Изменение взглядов на информационное противоборство на современном этапе // Вестник Академии военных наук. 2011. № 1 (34). С. 43-47.

367. Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1 (1). С. 2-9.

368. Буянов В. П., Ерофеев Е. А., Жогла Н. Л., Зайцев О. А., Курбатов Г. Л., Петренко А. И., Уфимцев Ю. С., Федотов Н. В. Информационная безопасность России – М.: Экзамен, 2003. – 560 с.

369. Прокофьев В. Ф. Тайное оружие информационной войны. Воздействие на подсознание. – М.: Синтег, 2003. – 430 с.

370. Колин К. К. Социальная информатика. – М.: Академический проект, 2003. – 432 с.

371. Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны – реальная угроза национальной безопасности. – М.: КРАСАНД. – 2011. – 96 с.

372. Проблемы безопасности программного обеспечения / Под ред. П.Д. Зегжды. – СПб.: ГТУ, 1995. – 200 с.

373. Медведовский И. Д., Семьянов П. В., Платонов В. В. Атака через Интернет / Под ред. П.Д. Зегжды. – СПб.: Издательство НПО «Мир и семья-95», 1997с.

374. Макаренко С. И. Информационная безопасность: Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

375. DoS-атака // Wikipedia [Электронный ресурс]. 19.05.2016. – URL: https://ru.wikipedia.org/wiki/DoS%D0%B0%D1%82%D0%B0%D0%BA%D0%B0 (дата обращения 19.05.2016).

376. Марков А. С., Фадин А. А. Организационно-технические проблемы защиты от целевых вредоносных программ // Вопросы кибербезопасности. 2013. № 1 (1). С. 28-36.

377. Куприянов А. И., Сахаров А. В. Радиоэлектронные системы в информационном конфликте. – М.: Вузовская книга, 2003. – 528 с.

378. Duqu: A Stuxnet-like malware found in the wild, technical report. Laboratory of Cryptography of Systems Security (CrySyS). – Budapest: Budapest University of Technology and Economics Department of Telecommunications, 2011. – 60 p. – URL: http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf (дата обращения 20.08.2016).

379. Вирус Regin // Security Lab [Электронный ресурс]. 28.05.2015. – URL: http://www.securitylab.ru/analytics/473080.php (дата обращения 14.08.2016).

380. Киви Б. Кивино гнездо: Государственный троянец // Компьютера [Электронный ресурс]. 21.10.2011. – URL: http://www.computerra.ru/641530/ (дата обращения 10.03.2013).

381. «Лаборатория Касперского» раскрыла новый виток кампании кибершпионажа // PC Week [Электронный ресурс]. 04.07.2014. – URL: http://www.pcweek.ru/security/news-company/detail_print.php?ID=164797&print=Y (дата обращения 04.07.2014).

382. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2007. – 11 с. – URL: http://docs.cntd.ru/document/gost-r-51275-2006 (дата обращения 14.08.2016).

383. Шабанов А. Программные закладки в бизнес-приложениях // Anti-Malware [Электронный ресурс]. 13.01.2011. – URL: http://www.anti-malware.ru/software_backdoors# (дата обращения 14.08.2016).

384. Марков А. С., Цирлов В. Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42-48.

385. "Любопытные" браузеры шпионят за пользователями // Security Lab [Электронный ресурс]. 24.04.2009. – URL: http://www.securitylab.ru/news/378304.php (дата обращения 14.08.2016).

386. В смартфонах с Windows Mobile есть черный ход для спецслужб // Security Lab [Электронный ресурс]. 08.11.2007. – URL: http://www.securitylab.ru/news/307144.php (дата обращения 14.08.2016).

387. О скрытых возможностях «Windows 10» // Безопасность пользователей в сети Интернет [Электронный ресурс]. 18.11.2015. – URL: http://www.safe-surf.ru/users-of/article/205578/ (дата обращения 14.08.2016).

388. Did the FBI Lean On Microsoft for Access to Its Encryption Software? // Mashable [Электронный ресурс]. 11.09.2013. – URL: http://mashable.com/2013/09/11/fbi-microsoft-bitlocker-backdoor/#QHqC4M1Tn8qo (дата обращения 14.08.2016).

389. Каталог АНБ США. 48 с. [Электронный ресурс]. – URL: http://s3r.ru/13/01/2014/novosti/raskryit-spisok-apparatnyih-zakladok-anb-ssha-dlya-tehniki-cisco-huawei-i-juniper-katalog/attachment/48-stranits-kataloga-abn-ssha/ (дата обращения 14.08.2016).

390. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2 (3). С. 60-65.

391. Дождиков В. Г., Салтан М. И. Краткий энциклопедический словарь по информационной безопасности. – М.: ИАЦ «Энергия», 2010. – 240 с.

392. Зайцев О. Современные клавиатурные шпионы // Компьютер-пресс. 2006. № 5. – URL: http://www.compress.ru/Archive/CP/2006/5/23/ (дата обращения 14.08.2016).

393. Виноградов А. А. Функциональность, надежность, кибер-устойчивость в системах автоматизации критических инфраструктур [Доклад] // Конференция «Региональная информатика-2012». – СПб.: ОАО «НПО «Импульс», 2012.

394. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 2: Рабочее место оператора // Вопросы кибербезопасности. 2014. № 4 (7). С. 60-68.

395. Китайские закладки. Голый король // Security Lab [Электронный ресурс]. 30.09.2012. – URL: http://www.securitylab.ru/contest/430512.php? pagen=7&el_id=430512 (дата обращения 14.08.2016).

396. Евграфов В. Перспективы использования зарубежными вооруженными силами беспилотных летательных аппаратов для решения задач РЭБ // Зарубежное военное обозрение. 2009. № 10. С. 53-58. – URL: http://pentagonus.ru/publ/perspektivy_ispolzovanija_zarubezhnymi_vooruzhjonnymi_silami_bespilotnykh_letatelnykh_apparatov_dlja_reshenija_zadach_rehb/17-1-0-1407 (дата обращения 10.01.2017).

397. Тихонов А. Ю., Аветисян А. И. Развитие taint-анализа для решения задачи поиска программных закладок // Труды Института системного программирования РАН. 2011. Т. 20. С. 9-24.

398. Чукляев И. И. Анализ уязвимостей в исходных кодах программного обеспечения статическими и динамическими методами // XII Всероссийское совещание по проблемам управления ВСПУ-2014, 16-19 июня 2014 г. – М., 2014. – С. 9232- 9242.

399. Шурдак М. О., Лубкин И. А. Методика и программное средство защиты кода от несанкционированного анализа // Программные продукты и системы. 2012. № 4. С. 176-180.

400. Гайсарян С. С., Чернов А. В., Белеванцев А. А., Маликов О. Р., Мельник Д. М., Меньшикова А. В. О некоторых задачах анализа и трансформации программ // Труды Института системного программирования РАН. 2004. Т. 5. С. 7-40.

401. AN/ALQ-151A Quickfix // Global Security [Электронный ресурс]. 28.07.2011. – URL: http://www.globalsecurity.org/intell/systems/quickfix.htm (дата обращения 19.07.2016).

402. Язов Ю. К., Сердечный А. Л., Шаров И. А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 55-60.

403. Сердечный А. Л. Инновационный подход к защите информации в виртуальных вычислительных сетях, основанный на стратегии обмана // Информация и безопасность. 2013. № 3. С. 399-403.

404. Булойчик В. М., Берикбаев В. М., Герцев А. В., Русак И. Л . Булойчик А. В., Герцев В. А., Зайцев С. И. Разработка и реализация комплекса имитационных моделей боевых действий на мультипроцессорной вычислительной системе // Наука и военная безопасность. 2009. № 4. С. 32-37. – URL: http://militaryarticle.ru/nauka-i-voennaya-bezopasnost/2009/12076-razrabotka-i-realizacija-kompleksa-imitacionnyh (дата обращения 30.07.2014).

405. Резяпов Н. Развитие систем компьютерного моделирования в вооруженных силах США // Зарубежное военное обозрение. 2007. № 6. С. 17-23. – URL: http://pentagonus.ru/publ/11-1-0-222 (дата обращения 18.08.2016).

406. Резяпов Н. Развитие систем компьютерного моделирования в вооруженных силах США // Зарубежное военное обозрение. 2007. № 6. С. 17-23. – URL: http://pentagonus.ru/publ/11-1-0-222 (дата обращения 18.08.2016).

407. Новиков Д. А. Иерархические модели военных действий // Управление большими системами. 2012. № 37. С. 25-62.

408. Sikorsky EH-60A Quick Fix II // Авиа Стар [Электронный ресурс]. 28.07.2011. – URL: http://www.aviastar.org/helicopters_rus/sik_quickfix-r.html (дата обращения 19.07.2016).

409. Мединн А. Имитационная система JTLS. Часть 1 // Зарубежное военное обозрение. 2010. № 2. С. 31-34. – URL: http://pentagonus.ru/publ/imitacionnaja_sistema_jtls/19-1-0-1672 (дата обращения 18.08.2016).

410. Мединн А. Имитационная система JTLS. Часть 2 // Зарубежное военное обозрение. 2010. № 3. С. 26-31. – URL: http://pentagonus.ru/publ/imitacionnaja_sistema_jtls_ch2/9-1-0-1699 (дата обращения 18.08.2016).

411. Мединн А. Имитационная система JTLS. Часть 3 // Зарубежное военное обозрение. 2010. № 4. С. 35-37. – URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2010-zvo/7897-imitacionnaja-sistema-jtls (дата обращения 30.07.2014).

412. Меньшаков Ю. К. Теоретические основы технических разведок: Учеб. пособие / Под ред. Ю.Н. Лаврухина. – М.: МГТУ им. Н.Э. Баумана, 2008. – 536 с.

413. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – Киев: Юниор, 2003. – 504 с.

414. Чукляев И. И., Морозов А. В., Болотин И. Б. Теоретические основы оптимального построения адаптивных систем комплексной защиты информационных ресурсов распределенных вычислительных систем: Монография. – Смоленск: ВА ВПВО ВС РФ, 2011. – 227 с.

415. Емельянов С. Л. Техническая разведка и технические каналы утечки информации // Системи обробки інформації. 2010. № 3 (84). С. 20-23.

416. Варламов О. О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ЮФУ. Технические науки. 2006. № 7 (62). С. 216-223.

417. Пахомова А. С., Пахомов А. П., Разинкин К. А. К вопросу о разработке структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Том 16. № 1. С. 115-118.

418. Пахомова А. С., Пахомов А. П., Юрасов В. Г. Об использовании классификации известных компьютерных атак в интересах разработки структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Т. 16. № 1. С. 81-86.

419. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description // Cigital Inc. 2008. Vol. 3.

420. O'Neill J. Echelon: Somebody's Listening. – Tarentum: Word Association Publishers, 2005. – 347 с. – URL: http://books.google.com/books?id=1x6Akzkxv5IC&printsec=frontcover&source=gbs_summary_r&cad=0 (дата обращения 30.11.2016).

421. PRISM (surveillance program) // Wikipedia [Электронный ресурс]. 2016. – URL: https://en.wikipedia.org/wiki/PRISM_(surveillance_program) (дата обращения 30.11.2016).

422. Stellar Wind // Wikipedia [Электронный ресурс]. 2016. – URL: https://en.wikipedia.org/wiki/Stellar_Wind (дата обращения 30.11.2016).

423. Meet CO-TRAVELER: The NSA's Cell Phone Location Tracking Program // Electronic Frontier Foundation [Электронный ресурс]. 5.12.2013. – URL: https://www.eff.org/ru/deeplinks/2013/12/meet-co-traveler-nsas-cell-phone-location-tracking-program (дата обращения 30.11.2016).

424. Dropmire // Wikipedia [Электронный ресурс]. 2016. – URL: https://en.wikipedia.org/wiki/Dropmire (дата обращения 30.11.2016).

425. X-Keyscore // Wikipedia [Электронный ресурс]. 2016. – URL: https://en.wikipedia.org/wiki/Dropmire (дата обращения 30.11.2016).

426. Tempora [Электронный ресурс]. 2017. – URL: https://en.wikipedia.org/wiki/Tempora (дата обращения 23.01.2017).

427. Зенин А. Разведка в сухопутных войсках США на основе анализа открытых источников информации // Зарубежное военное обозрение. 2009. № 5 С. 32-38. URL: http://pentagonus.ru/publ/80-1-0-1183 (дата обращения 17.08.2016).

428. Кондратьев А. Разведка с использованием открытых источников информации в США // Зарубежное военное обозрение. 2010. № 9. С. 28-32. URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2010-zvo/7969-razvedka-s-ispolzovaniem-otkrytyh-istochnikov (дата обращения 30.08.2014).

429. Разведка средствами Интернет // IT-сектор [Электронный ресурс]. – URL: http://it-sektor.ru/razvedka-sredstvami-internet.html (дата обращения 17.08.2016).

430. Ларина Е. С., Овчинский В. С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014. – 352 с.

431. Thaler R. H., Sunstein C. R. Nudge: Improving decisions about health, wealth, and happiness. – Yale: Yale University Press, New Haven, CT, 2008. – 293 p.

432. Микрюков В. Победа в войне должна быть достигнута еще до первого выстрела // Независимое военное обозрение [Электронный ресурс]. 15.01.2016. – URL: http://nvo.ng.ru/concepts/2016-01-15/10_infowar.html (дата обращения 30.06.2016).

433. Караяни А. Г. Информационно-психологическое противоборство в современной войне // ArmyRus. Военно-информационный портал [Электронный ресурс]. 16.08.2014. – URL: http://armyrus.ru/index.php?option=com_content&task=view&id=739 (дата обращения 30.06.2016).

434. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт). – Минск: Харвест, 1999. – 448 с. – URL: http://www.e-reading.club/bookreader.php/1005378/Vladimir_-_Sekrety_psihologicheskoy_voyny.html (дата обращения 30.06.2016).

435. Баришполец В. А. Информационно-психологическая безопасность: основные положения // Информационные технологии. 2003. Т. 3. № 2. С. 69-104.

436. Назаров Д. В., Ахмедзянов В. Р. Психотронное оружие. Воздействие скрытых команд на подсознание человека // Вестник РУДН. Серия: Экология и безопасность жизнедеятельности. 2008. № 4 С. 49-54. – URL: http://cyberleninka.ru/article/n/psihotronnoe-oruzhie-vozdeystvie-skrytyh-komand-na-podsoznanie-cheloveka (дата обращения 23.01.2017).

437. Васильева М. М. Информационное оружие как средство управления общественно-политическими процессами // Вестник МГЛУ. 2012. № 25 (658). С. 30-38. – URL: http://cyberleninka.ru/article/n/informatsionnoe-oruzhie-kak-sredstvo-upravleniya-obschestvenno-politicheskimi-protsessami (дата обращения 23.01.2017).

438. Чуйков Д. А. Совершенствование защиты личного состава подразделения от информационно-психологического воздействия противника // VII Международная студенческая электронная научная конференция «Студенческий научный форум». 2015. – URL: https://www.scienceforum.ru/2015/1301/15166# (дата обращения 23.01.2017).

439. Паршакова Е. Д. Информационные войны: Учебное пособие – Краматорск: ДГМА, 2012. – 92 с.

440. Семенкович В. Н. Роль и место глобальной сети Интернет в ведении современного информационного противоборства // Наука и военная безопасность. 2009. № 4. С. 60-64. – URL: http://militaryarticle.ru/nauka-i-voennaya-bezopasnost/2009/12078-rol-i-mesto-globalnoj-seti-internet-v-vedenii (дата обращения 30.06.2016).

441. Машкин К. Современные способы и средства распространения материалов информационно-психологического воздействия в ВС США. Часть 1 // Зарубежное военное обозрение. 2009. № 10. С. 31-36. – URL: http://pentagonus.ru/publ/sovremennye_sposoby_i_sredstva_rasprostranenija_materialov_informacionno_psikhologicheskogo_vozdejstvija_v_vs_ssha_ch1/11-1-0-1403 (дата обращения 17.08.2016).

442. Машкин К. Современные способы и средства распространения материалов информационно-психологического воздействия в ВС США. Часть 2 // Зарубежное военное обозрение. 2009. № 12. С. 25-28. – URL: http://pentagonus.ru/publ/sovremennye_sposoby_i_sredstva_rasprostranenija_materialov_informacionno_psikhologicheskogo_vozdejstvija_v_vs_ssha/105-1-0-1438 (дата обращения 17.08.2016).

443. Командо соло – самолет психологической войны // Zabort.ru [Электронный ресурс]. 24.07.2010. – URL: http://zabort.ru/blog/poznavatelno/9918.html (дата обращения 17.08.2016).

444. Савельев А. Информационное обеспечение применения вооруженных сил США // Зарубежное военное обозрение. 2015. № 12. С. 56-62. – URL: http://pentagonus.ru/publ/informacionnoe_obespechenie_primenenija_vooruzhjonnykh_sil_ssha_2015/109-1-0-2666 (дата обращения 17.08.2016).

445. Пиунов О. Самолеты типа С-130 "Геркулес" сил специальных операций ВВС США // Зарубежное военное обозрение. 2011. № 12. С. 52-54. – URL: http://pentagonus.ru/publ/samoljoty_tipa_c_130_quot_gerkules_quot_sil_specialnykh_operacij_vvs_ssha_2011/17-1-0-1990 (дата обращения 17.08.2016).

446. Китов П. Совершенствование способов и средств ведения психологических операций вооруженных сил США // Зарубежное военное обозрение. 2013. №3. С. 19-20. – URL: http://pentagonus.ru/publ/sovershenstvovanie_sposobov_i_sredstv_vedenija_psikhologicheskikh_operacij_vooruzhjonnykh_sil_ssha_2013/22-1-0-2393 (дата обращения 17.08.2016).

447. Петров А. Участие ВВС США в психологических операциях ВС НАТО в Афганистане // Зарубежное военное обозрение. 2010. № 4. С. 50-57. – URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2010-zvo/8003-uchastie-vvs-ssha-v-psihologicheskih-operacijah-vs (дата обращения 30.06.2016).

448. Петровский А. Информационное противоборство в ходе конфликта в Секторе Газа // Зарубежное военное обозрение. 2009. № 5. С. 29-31. – URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2009-zvo/7742-informacionnoe-protivoborstvo-v-hode-konflikta-v (дата обращения 30.06.2014).

449. Колесов П. Информационная война Грузии против Южной Осетии и Абхазии // Зарубежное военное обозрение. 2008. № 10. С. 18-21. – URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2008-zvo/7600-informacionnaja-vojna-gruzii-protiv-juzhnoj-osetii (дата обращения 30.06.2014).

450. Яшин С. Бортовые радиоэлектронные средства защиты летательных аппаратов // Зарубежное военное обозрение. 2016. № 6. С. 71-75. – URL: http://pentagonus.ru/publ/bortovye_radioehlektronnye_sredstva_zashhity_letatelnykh_apparatov_2016/18-1-0-2712 (дата обращения 19.07.2016).

451. Intelligence and Electronic Warfare (IEW) System Fact Sheets. – Fort Huachuca, Arizona: U.S. Army Intelligence Center, 1994. 39 p. – URL: http://www.dtic.mil/dtic/tr/fulltext/u2/a390663.pdf (дата обращения 19.07.2016).

452. Кондратьев А. Перспективный комплекс РРТР и РЭВ сухопутных войск США Профет // Зарубежное военное обозрение. 2008. № 7. С. 37-41. – URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2008-zvo/7632-perspektivnyj-kompleks-rrtr-i-rjev-suhoputnyh (дата обращения 30.07.2014).

453. AN/MLQ-40 Prophet // Global Security [Электронный ресурс]. 28.07.2011. – URL: http://www.globalsecurity.org/intell/systems/prophet.htm (дата обращения 19.07.2016).

454. Стрелецкий А. Американский перспективный наземный комплекс ведения радиоэлектронной войны "Вулфпак" // Зарубежное военное обозрение. 2002. № 10. С. 27-28. – URL: http://pentagonus.ru/publ/11-1-0-155 (дата обращения 19.07.2016).

455. Judson J. Will Russian Aggression Ramp Up US Army Focus on Electronic Warfare Needs? // Defense News. 07.03.2016. – URL: http://www.defensenews.com/story/defense/show-daily/ausa-global-

force/2016/03/07/russian-aggression-ramp-up-us-army-focus-electronic-warfare-needs/81249312/ (дата обращения 19.07.2016).

456. FY 2015 budget request funds Electronic Warfare Development. PE 0604270A: Electronic Warfare Development Army. – U.S. Army, 2014. – 31 p. – URL: http://www.globalsecurity.org/military/library/budget/fy2015/army-peds/0604270a_5_pb_2015.pdf (дата обращения 19.07.2016).

457. Electronic Warfare Planning and Management Tool (EWPMT) // United States Army Acquisition Support Center [Электронный ресурс]. 2016. – URL: http://asc.army.mil/web/portfolio-item/iews-electronic-warfare-planning-and-management-tool-ewpmt/ (дата обращения 19.07.2016).

458. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь. 2011. № 3. С. 41-47.

459. Макаренко С. И. Использование космического пространства в военных целях: современное состояние и перспективы развития систем информационно-космического обеспечения и средств вооружения // Системы управления, связи и безопасности. 2016. № 4. С. 161-213. – URL: http://sccs.intelgr.com/archive/2016-04/09-Makarenko.pdf (дата обращения 25.01.2017).

460. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (дата обращения 24.03.2018).

461. Попов И. М., Хамзатов М. М. Война будущего: концептуальные основы и практические выводы. Очерки стратегической мысли. – М.: Кучково поле, 2016. – 836 с.

462. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.

463. Макаренко С. И. Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями // Системы управления, связи и безопасности. 2017. № 4. С. 15-59. – URL: http://sccs.intelgr.com/archive/2017-04/02-Makarenko.pdf (дата обращения 27.02.2018).

Макаренко Сергей Иванович
Иванов Максим Сергеевич

Сетецентрическая война – принципы, технологии,
примеры и перспективы

Монография

Научное издание

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел групп»
197372, Санкт-Петербург,
пр. Богатырский, дом 32, к. 1 лит. А, пом. 6Н.
http://publishing.intelgr.com
Тел.: +7 (812) 945-50-63
E-mail: publishing@intelgr.com

Отпечатано:
Типография «Скифия-Принт»
Санкт-Петербург, ул. Б. Пушкарская, д.10.
http://www.skifia-print.ru
Тел.: +7 (812) 644-41-63
E-mail: skifia-print@mail.ru

ISBN 978-5-6040965-3-6

Гарнитура «TimesNewRoman». 45 п.л.
Тираж 600 экз. Подписано в печать 10.06.2018.

Материалы изданы в авторской редакции

«В монографии сосредоточены аналитические и информационные материалы, которые характеризуют практически все появившиеся в последние годы и ожидаемые в недалеком будущем новации в военном деле… По широте и глубине изложенного в этом труде материала данную работу можно оценить как уникальное, наиболее обширное системное издание, которое дает представление обо всех заметных тенденциях в развитии технических средств и технологий силового противоборства…»

Президент РАРАН, д.т.н. проф. В.М. Буренок

Макаренко Сергей Иванович – кандидат технических наук, доцент. Профессор Академии военных наук.

В 2002 году окончил Военный авиационный технический университет имени проф. Н. Е. Жуковского (филиал в г. Ставрополь) по специальности «Автоматизированные системы управления и обработки информации». В 2007 году защитил диссертацию на соискание ученой степени кандидата технических наук по специальности «Вооружение и военная техника. Комплексы и системы военного назначения». В период с 2007 по 2017 годы проходил службу в Ставропольском высшем военном авиационном инженером училище, в ВУНЦ ВВС «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина», в Военно-космической академии им. А.Ф. Можайского. С 2017 года – работает на предприятиях оборонно-промышленного комплекса России.

Иванов Максим Сергеевич – кандидат технических наук.

В 2002 году окончил Военный авиационный технический университет имени проф. Н.Е. Жуковского (филиал в г. Ставрополь) по специальности «Техническая эксплуатация транспортного радиооборудования». В 2011 году защитил диссертацию на соискание ученой степени кандидата технических наук по специальности «Военные системы управления, связи и навигации».

В период с 2004 по 2009 годы проходил военную службу в Ставропольском высшем военном авиационном инженером училище, с 2009 года проходит военную службу в ВУНЦ ВВС «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина».