Макаренко С.И.

Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века

Монография

С.И. Макаренко

Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века

Санкт-Петербург
Наукоемкие технологии
2017

УДК 623.624
ББК 68.8
М15

Рецензенты:

Сотрудник Воронежского института правительственной связи (филиала) Академии Федеральной службы охраны России, доктор технических наук, профессор ***Гречишников Евгений Владимирович****;*

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

Профессор кафедры радиоэлектронной борьбы ВУНЦ ВВС «Военно-воздушная академия имени проф. Н.Е. Жуковского и Ю.А. Гагарина», доктор технических наук, профессор ***Козирацкий Юрий Леонтьевич****;*

Профессор кафедры «Радиосистемы передачи информации и управления» Московского авиационного института (национального исследовательского университета), доктор технических наук, профессор ***Куприянов Александр Ильич****;*

Генеральный конструктор систем радиоэлектронной борьбы СССР, доктор технических наук, профессор ***Перунов Юрий Митрофанович****.*

Макаренко С.И.

М15 Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. — СПб.: Наукоемкие технологии, 2017. — 546 с.

ISBN 978-5-9909412-1-2

УДК 623.624
ББК 68.8

Монография является результатом работы автора по обобщению исследований в областях радиоэлектронной борьбы и информационного противоборства в условиях произошедшей в начале XXI века информационно-технической революции и внедрения в практику войск концепции сетецентрических войн. В монографии проведен анализ основ концепции сетецентрической войны, выявлены фундаментальные взаимосвязи этой концепции с возрастающей ролью средств воздействия на информацию, циркулирующую в системах управления войсками и оружием. Проведен анализ средств радиоэлектронной борьбы, средств информационного противоборства в технической и в психологических сферах, а также способов их применения в современных сетецентрических войнах. На примерах войн начала XXI века, которые велись в соответствии с сетецентрической концепцией, показан вклад радиоэлектронной борьбы, а также информационного противоборства в технической и в психологических сферах в обеспечение достижения военного и информационного превосходства. Представлены основные тенденции развития средств радиоэлектронной борьбы, а также средств и способов информационного противоборства в технической и психологической сферах.

ISBN 978-5-9909412-1-2

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

С чувством глубокой благодарности посвящаю свою работу моим учителям, которые определили мой путь в науке и предвосхитили полученные результаты:

учителю математики гимназии № 25
г. Ставрополя
Юлии Марковне Кудриной;

кандидату технических наук доценту
Александру Васильевичу Кихтенко;

кандидату технических наук профессору
Анатолию Вячеславовичу Баженову;

доктору технических наук профессору
Владимиру Ильичу Владимирову;

доктору технических наук профессору
Юрию Ивановичу Стародубцеву;

доктору технических наук профессору
Александру Григорьевичу Ломако.

С.И. Макаренко

Оглавление

Введение

«Кто владеет информацией, тот владеет миром».

Н.М. Ротшильд

«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 это всему миру — информация является ключом к современной войне в стратегическом, оперативном, тактическом и техническом отношении…»

Начальник штаба армии США
генерал-майор Г. Отис

Конец XX — начало XXI в. ознаменовались информационно-технической революцией. Она характеризуется факторами всемирного доступа к глобальному информационному пространству и широкого распространения электронных средств обработки информации. 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 армии. Это, в свою очередь, обусловило и изменение подходов к ведению войны. Анализ военно-прикладных эффектов от использования достижений информационно-технической революции свидетельствует о том, что развитие информационных систем сбора, передачи и обработки информации, способов представления и подачи информации определяет прорывной скачок в характеристиках средств вооруженной борьбы. 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. Вместе с тем данная концепция, будучи основанной на эффектах тотальной информатизации систем управления войсками и оружием, является асимметрично уязвимой для средств информационного воздействия — систем радиоэлектронной борьбы, систем и способов информационного противоборства. Именно эти системы и способы могут обеспечить решительный перевес в будущей сетецентрической войне и нивелировать преимущество технологически более развитого противника. Таким образом, концепция сетецентрических войн выводит на новый качественный

уровень как новую среду ведения военного противоборства — информационное пространство, так и новый вид вооружения — информационное оружие.

Целью монографии являются выявление роли и места радиоэлектронной борьбы и информационного противоборства, анализ тенденций развития их систем и средств, а также типовых способов их применения в сетецентрических войнах на основе анализа вооруженных конфликтов в Югославии, Ираке и Ливии.

Исследования в области развития методов ведения боевых действий и управления войсками с учетом использования новых информационных технологий, а также использования концепции сетецентрических войн, велись следующими отечественными учеными: Н.В. Огарковым, М.А. Гареевым [1], В.М. Буренком [13, 14, 38–42], А.А. Ивлевым [13, 290], В.И. Слипченко [17, 18], И.М. Поповым [23, 313], С.Я. Лавреновым [21], В.Ю. Микрюковым [22], В.В. Хазматовым [23, 24], Ю.Я. Бобковым, Н.Н. Тютюнниковым [29], А.Е. Кондратьевым [43–51], А.А. Рахмановым [58–60], Г.А. Налетовым [61], М.П. Фархадовым, Д.Н. Душкиным [69], С.В. Кругликовым, А.А. Липатовым [70], А.В. Копыловым [82, 94], Р.В. Арзуманяном [71, 84], А.Н. Сидориным, В.М. Прищеповым, В.П. Акуленко [95], И.М. Капитанцом [173], Л.В. Савиным [239]. При анализе концепции сетецентрических войн широко использовался материал открытых работ американских экспертов: A.K. Cebrowski [152], J.J. Garstka [112, 152, 331], D.S. Alberts [112, 331], F.P. Stein [112], P.J. Dombrowski, E. Gholz, A.L. Ross [333], J.W Bodnar [113], J. Arquilla, D.F. Ronfeldt [148, 206, 207], D.R. Hersprin [153], R.E. Hayes, D.A. Signori [331], E.A. Smith [332], которые лежали в основе создания и развития концепции сетецентрических войн в США. Кроме того, отдельные аспекты сетецентрических войн обобщенно рассмотрены в предыдущих работах автора [36, 197].

Изменение роли информации в процессе функционирования систем управления войсками и оружием привело к разработке концепции информационного противоборства в военной сфере. **Исследования военных аспектов информационного противоборства** вели следующие ученые: С.Н. Гриняев [2, 3], В.С. Пирумов [4, 5], Н.А. Костин [6, 7, 8], С.А. Комов [9, 30, 31, 55–57], В.И. Цымбал [10], А.А. Прохожев, Н.И. Турко [11], С.А. Модестов [12], Т.В. Гуржеянц, Е.А. Дербин, Г.О. Крылов, А.Н. Кубанков [15], А.В. Бедрицкий [16], С.В. Коротков, И.Н. Дылевский, А.Н. Петрунин [31, 55, 56, 57], Ю.И. Стародубцев, В.В. Бухарин [62, 63], С.С. Семенов [62, 63, 97], П.И. Антонович [283-286]. Кроме того, отдельным вопросам информационного противоборства в военной сфере посвящены более ранние работы автора [36, 270].

Развитие теории информационного противоборства привело к декомпозиции ее по сферам применения — психологической и технической. В настоящее время, на взгляд автора, теория информационного противоборства в психологической сфере является в большей степени развитой, нежели теория противоборства в технической сфере. Возможно, это объясняется общей гуманитарной направленностью данных исследований, а также существенным научным заделом в теории психологии, в поведенческих, а также в когнитив-

ных науках. К концу XX века исследования в области этих теорий, с одной стороны, получили широкое финансирование от западных государственных фондов, а с другой стороны — эти исследования из фазы фундаментальных перешли в стадию прикладных разработок, направленных на получение эффективных технологий анализа поведения, а также политических, экономических и социальных процессов в обществе.

Исследования информационного противоборства в психологической сфере, а также его влияния на политические, экономические и социальные процессы вели следующие отечественные ученые: С.Г. Кара-Мурза [20], Г.В. Грачёв [26, 33], В.М. Щекотихин [32], С.Н. Бухарин, В.В. Цыганов [34, 35], С.А. Модестов [37], И.Н. Панарин [52, 53], В.А. Лисичкин, Л.А. Шелепин [54], А.В. Манойло [72, 318], Г.Г. Почепцов [73, 74, 272], С.П. Расторгуев [75, 76, 79, 277], Д.А. Новиков, А.Г. Чхартишвили [77, 78], Д.А. Губанов [77], А.Г. Караяни [80, 400], Д.А. Волкогонов [81], Н.Л. Волковский [83], В.А. Минаев, А.С. Овчинский, С.В. Скрыль, С.Н. Тростянский [85, 419], В.Ф. Прокофьев [303], В. П. Шейнов [315], В.А. Баришполец [390], Л.В. Воронцова, Д.Б. Фролов [402], В.Г. Крысько [405], И.А. Шеремет [419, 420], К.В. Семашко [420]. Результатом этих исследований явилась подробная разработка научно-методических основ влияния информационных воздействий на индивидуальное и массовое сознание, а также на психические процессы. Выявлены механизмы отображения такого влияния на социальные, политические и экономические процессы. Предложены и обоснованы технологии формирования поведения отдельных лиц и групп населения, а также «подталкивание» их к принятию требуемых решений. Таким образом, можно констатировать, что теория информационного противоборства в психологической сфере уже сформировалась как самостоятельная часть науки о манипуляции поведением отдельных личностей и социальных групп. Ее дальнейшее развитие идет по пути конкретизации использования выявленных эффектов информационно-психологического воздействия в социальной, политической и экономической сферах.

Однако такого вывода нельзя сделать о теории информационного противоборства в технической сфере, которая в настоящее время только находится в стадии становления и развития. Терминологический аппарат в этой области отличается противоречивостью и неоднозначностью, а для ее методов зачастую характерен эмпирический, а не системный подход.

В качестве примера этого можно привести работы С.Н. Гриняева [2, 131], А.В. Бедрицкого [16], В.К. Новикова [86], С.А. Петренко [87], Н.П. Шеховцова, Ю.Е. Кулешова [292], Е.Д. Паршаковой [399], Л.В. Воронцовой, Д.Б. Фролова [402]. Представленные в этих работах варианты классификации информационного оружия в технической сфере и информационно-технических воздействий не обладают высокой степенью систематизации и зачастую ведутся без учета методов системного подхода.

По мнению автора, такое «запаздывание» в развитии теории информационного противоборства в технической сфере объясняется рядом факторов.

Во-первых, запаздыванием начала системных исследований в этой области на 40–50 лет по сравнению с информационно-психологическими

исследованиями. Первые широкомасштабные системные исследования в области информационного влияния на психику отдельных людей и масс можно отнести к 1940-м гг. А исследования в области информационного противоборства в технической сфере — только к 1980-м.

Во-вторых, динамическим развитием объекта исследования. Исследования человеческой психики являются актуальными независимо от времени получения научных результатов. В то время как технические системы постоянно совершенствуются и усложняются, что приводит к стремительному устареванию результатов, полученных для информационных систем предыдущего поколения.

В-третьих, отсутствием системного подхода к выработке эволюционного пути развития основ теории информационного противоборства в технической сфере. На первый взгляд, революционное развитие информационно-технических систем требует подобного революционного развития от теории, как минимум в способах осуществления информационно-технических воздействий и защиты от них. Вместе с тем, на взгляд автора, это принципиально неверно. Необходимо сосредоточиться на выявлении общесистемных тенденций, эффектов, свойствах систем, методах воздействий и защиты, которые являются инвариантными к конкретным типам и уровням развития информационно-технических систем. И при революционном развитии информационно-технических систем эволюционно совершенствовать указанные основные элементы теории информационного противоборства.

Исследования отдельных аспектов информационного противоборства в технической сфере велись следующими учеными: С.Н. Гриняевым [2, 96, 131], С.А. Петренко [25, 87], Д.Д. Ступиным [25], Ю.И. Стародубцевым [64–67], Е.В. Гречишниковым [64–68], С.П. Расторгуевым [75, 76, 277], А.Е. Давыдовым [88], М.А. Коцыняком, О.С. Лаутой [89, 90], О.И. Шелухиным [93], В.И. Емелиным [98], Г.А. Остапенко [99, 100], М.А. Еремеевым [127], А.Г. Ломако, Д.Н. Бирюковым [127, 128], А.А. Тарасовым [129], С.А. Будниковым [130], И.И. Чукляевым [137, 349, 360], Н.Н. Толстых [139, 140, 141], А.Г. Алферовым [140, 141], В.Ю. Храмовым, А.А. Бойко [144], Ю.Л. Козирацким [145, 146, 254], И.В. Котенко [147, 149, 150, 151], И.Б. Саенко [147, 149], А.В. Улановым [150, 151], А.А. Хоревым [154, 155], Ю.В. Бородакием [287], П.Д. Зегждой [320, 380], А.И. Куприяновым, А.В. Сахаровым, В.А. Шевцовым [321], Ю.К. Язовым [350], А.Л. Сердечным [350, 351], Ю.К. Меньшаковым [359], А.В. Морозовым, И.Б. Болотиным [360], А.С. Пахомовой [364, 365], С.А. Паршиным, Ю.Е. Горбачёвым, Ю.А. Кожановым [381], И.Д. Медведовским, П.В. Семьяновым, В.В. Платоновым [380], Е.С. Лариной, В.С. Овчинским [378], И.А. Шереметом [417, 418], С.М. Климовым [91, 92, 421–426], М.П. Сычёвым [92, 421, 422], А.Ф. Белым [424, 425], Е.Б. Дроботуном [429]. Кроме того, отдельным вопросам информационного противоборства в технической сфере посвящены более ранние работы автора [193–196, 198, 199–202, 204, 205, 270, 371]. Часть этих исследований велось в рамках развития теории информационной безопасности, часть — как развитие теории систем, часть — как развитие теории информационного конфликта.

Вместе с тем, по глубокому убеждению автора, развитие теории информационного противоборства в технической сфере должно быть основано на научно-методическом заделе в области радиоэлектронной борьбы. Именно теория радиоэлектронной борьбы за более чем вековую историю своего активного развития содержит многократно апробированные и высокоэффективные способы воздействия на информационно-технические системы, основанные на дестабилизации информационного обмена. Формирование базиса информационного противоборства в технической сфере должно основываться на переносе принципов, методов и способов радиоэлектронной борьбы в новую сферу — информационное (кибернетическое) пространство. Актуальность такого направления развития теории радиоэлектронной борьбы подтверждается работами [194, 195, 201, 371, 409, 410].

В настоящее время теория радиоэлектронной борьбы довольно многогранна и включает в себя комплекс специфичных методов, которые ориентированы на различные объекты поражения и защиты. К основным объектам поражения можно отнести: системы управления войсками и оружием, радиолокационные системы, системы радио- и оптической связи, системы радионавигации, оптико-электронные системы, системы радио- и оптико-электронной разведки. При этом подавляющая часть методологии радиоэлектронной борьбы ориентирована на системы управления оружием, основанные на радиолокационных системах обнаружения, наведения и целеуказания.

Исследования отдельных аспектов радиоэлектронной борьбы велись следующими учеными: С.А. Вакиным [156], Л.Н. Шустовым [156, 157, 245, 251], М.В. Максимовым [157], В.В. Дружининым, Д.С. Конторовым [158], А.И. Палием [159], В.В. Цветновым, В.П. Дёминым [160, 161], А.И. Куприяновым [160, 161, 162, 245, 251], А.В. Сахаровым [162], Ю.Л. Козирацким [164], Б.А. Никольским [166], В.Г. Радзиевским [167], В.И. Владимировым, В.П. Лихачёвым, В.М. Шляхиным [168], В.И. Меркуловым [169], В.И. Борисовым, В.М. Зинчуком, А.Е. Лимаревым [170], А.М. Чудновым [172], В.И. Кузнецовым [175], А.П. Дятловым, П.А. Дятловым, Б.Х. Кульбикаяном [176], С.М. Одоевским, В.И. Калюкой [186], Р.Л. Михайловым [188, 189], В.Д. Добыкиным [251], В.Г. Пономарёвым [251], Е.Е. Исаковым [224], Ю.М. Перуновым [247, 250], А.В. Леньшиным [248], В.Ю. Осиповым, А.П. Ильиным, В.П. Фроловым, А.П. Кондратюком [255], Ю.И. Маевским [238], С.В. Козловым, В.И. Карпухиным, С.М. Лазаренковым [241]. Кроме того, отдельным вопросам радиоэлектронной борьбы посвящены более ранние работы автора [190, 191, 192, 195, 194, 196, 276, 371].

Исследования в области радио- и радиотехнической разведки, в части их использования в интересах применения средств радиоэлектронной борьбы, велись следующими учеными: В.А. Вартанесяном [177], С.А. Вакиным, Л.Н. Шустовым [156], В.В. Цветновым, В.П. Дёминым, А.И. Куприяновым [160], Л.А. Марчуком [178], Ю.А. Смирновым [179], В.Г. Радзиевским, А.А. Сиротой [180], Ю.П. Мельниковым [181], А.П. Дятловым, Б.Х. Кульбикаяном [182], С.В. Дворниковым, Ю.К. Меньшаковым [184], А.И. Рембовским, А.В. Ашихминым, В.А. Козьминым [185]. В этих исследованиях глубоко

проработаны вопросы методологии построения и обоснования способов применения средств радиоэлектронной борьбы и радиотехнической разведки. Вместе с тем при глубокой проработке этих методологических вопросов зачастую остаются нераскрытыми вопросы о технических характеристиках конкретных систем и средств, а также о способах и тактике их применения в реальных войнах. Эти сведения являются необходимыми и чрезвычайно актуальными для всех, кто ведет исследования в этой области, и могут служить существенным дополнением к известным теоретически-методологическим исследованиям.

Данная монография в части анализа средств радиоэлектронной борьбы и способов их применения в своевременных войнах развивает и дополняет работы Ю.К. Меньшакова [184], Н.А. Колесова, И.Г. Насенкова [187], Ю.М. Перунова, В.В. Мацукевича, А.А. Васильева [250], носящие описательный характер. В части информационного противоборства монография содержит оригинальный авторский подход к терминологии информационного противоборства, классификации средств и способов информационного воздействия. При этом основной упор сделан на информационное противоборство в технической сфере. Это обусловлено тем, что оно является основной областью научных интересов автора.

В первой главе монографии — «Концепция сетецентрической войны» — проведен анализ этой концепции. Показано, что она 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 в. информационно-технической революции. Выявлены основные особенности «бесконтактных» войн шестого поколения, а именно — существенное возрастание роли информационных средств при ведении войны. Выявлены факторы, предопределившие разработку концепции сетецентрической войны. 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. 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, за счет использования средств радиоэлектронной борьбы и способов информационного противоборства.

Во второй главе — «Радиоэлектронная борьба» — проведен анализ роли радиоэлектронной борьбы в условиях перехода к концепции сетецентрической войны. Проведен сравнительный анализ подходов к основам теории радиоэлектронной борьбы, а именно: терминологии, классификации средств и способов, основных тактических приемов, принятых как в Вооруженных силах США, так

и в отечественной методологии. На основе анализа изменений организационно-штатной структуры Вооруженных сил США проведен анализ совершенствования как организационной структуры, так и вооружения подразделений радиоэлектронной борьбы в сетецентрической войне. Рассмотрен типовой сценарий использования сил и средств радиоэлектронной борьбы в сетецентрической войне. Рассмотрены основные особенности объектов радиоэлектронного поражения: системы управления оружием, радиолокационные системы, системы радиосвязи. Особое внимание уделено подробному рассмотрению систем радиосвязи как объектов радиоэлектронного подавления, что обусловлено областью научных интересов автора. Рассмотрены общие принципы построения систем и средств радиоэлектронной борьбы, осуществляющих подавление и поражение радио- и оптико-электронного оборудования за счет: постановки радиоэлектронных помех; воздействия СВЧ-излучения; воздействия лазерного излучения. На основе систем и средств, используемых в Вооруженных силах США, подробно рассмотрены системы и средства РЭБ для индивидуальной защиты авиации; специализированные авиационные комплексы РЭБ; наземные средства РЭБ; средства и боеприпасы функционального поражения СВЧ-излучением; средства функционального поражения лазерным излучением. В заключении главы представлен анализ перспективных путей развития систем и средств РЭБ.

В частности, в разделе 2.8.4 — «Перспективы развития систем РЭБ, ориентированных на нарушение функционирования сетецентрических систем военного управления» — представлены перспективные подходы к радиоэлектронным воздействиям, основанным на оригинальных научных исследованиях автора. Эти радиоэлектронные воздействия ориентированы на нарушение функционирования сетецентрических систем военного управления. При этом предполагается, что такие воздействия будут менее энергоемкими и более бескомпроматными, а также — что они могут быть реализованы существующими «традиционными» комплексами РЭБ только за счет изменения логики их функционирования. В основу данного материала были положены обзорные работы автора по общим военно-прикладным принципам нарушения функционирования сетецентрических систем военного управления [195, 371], а также работы автора [190–192, 194, 196, 198–201, 204, 205] с теоретическим обоснованием новых способов и технологий радиоэлектронного подавления, ориентированных против объединенных сетей связи, являющихся основой сетецентрической системы управления.

В третьей главе монографии — «Информационное противоборство» — проведен анализ актуальности развития информационных средств и способов воздействия в современных сетецентрических войнах. Рассмотрено ретроспективное изменение подходов к месту и роли информационного противоборства в современных сетецентрических войнах. На основе анализа руководящих документов Вооруженных сил США и открытых работ западных и отечественных экспертов представлен подробный анализ терминологического аппарата теории информационного противоборства. Подробно рассмотрены понятия: информационное пространство, киберпространство и кибербезопасность, информацион-

ная война, информационные операции, информационное воздействие. Проведен анализ как общих аспектов, так и принципиальных различий в ведении информационного противоборства в технической и психологической сферах. Сформулировано понятие информационного оружия, представлен авторский подход к его классификации. Проведен анализ технологий информационного противоборства, обеспечивающих разработку и применение информационного оружия.

В четвертой главе — «Информационное противоборство в технической сфере» — проведен анализ взглядов различных стран к разработке принципов, доктрин и способов комплектования сил информационного противоборства в технической сфере. Этот анализ основан на данных о Вооруженных силах США, стран НАТО, Китая и некоторых других государств. Рассмотрено понятие информационно-технического оружия, дан авторский подход к его классификации. Кроме того, рассмотрены типовые сценарии его использования для борьбы с системами военного управления. Рассмотрены понятия информационно-технических воздействий, предложен авторский подход к их классификации, а также к классификации средств информационно-технических воздействий. Подробно рассмотрены следующие средства и способы информационно-технических воздействий, а также примеры их реализации: удаленные сетевые атаки, компьютерные вирусы, аппаратные и программные закладки, нейтрализаторы тестовых программ, средства создания ложных объектов информационного пространства, средства моделирования боевых действий, средства технической и компьютерной разведки, а также средства разведки по открытым источникам. В заключении главы представлены перспективные пути развития систем и средств информационного противоборства в технической сфере, основанные на проведенном анализе проектов DARPA за 2015 г., ведущихся в интересах совершенствования вооружения и военной техники в Вооруженных силах США.

В пятой главе — «Информационное противоборство в психологической сфере» — проведен анализ понятий информационной и психологической войны, психологической операции, информационно-психологического противоборства, информационно-психологического воздействия. Установлены принципиальные различия между воздействиями, производимыми психологическим и информационно-психологическим оружием. Рассмотрены основные типы психологического оружия, их принципы функционирования, средства реализации и способы применения. К рассмотренным типам психологического оружия относятся: лингвистическое, психотронное, психофизическое, сомато-психологическое. Рассмотрены основные типы информационно-психологического оружия: средства массовой информации, средства на основе интернет-ресурсов и социальных сетей, когнитивное оружие. На примере сил психологических операций Вооруженных сил США рассмотрены принципы комплектования, цели и задачи данных подразделений. На примере средств и систем, стоящих на вооружении в Вооруженных силах США, рассмотрены средства информационно-психологического воздействия, а также способы их применения в военных конфликтах. В заключении главы представлен анализ перспективных

путей развития средств информационного противоборства в психологической сфере, основанный на анализе проектов DARPA за 2015 г.

В шестой главе — «Примеры ведения информационного противоборства и радиоэлектронной борьбы в сетецентрических войнах начала XXI века» — на основе военных конфликтов конца XX — начала XXI века выявлены основные особенности современных операций, проводимых в соответствии с концепцией сетецентрических войн. Рассмотрены: 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, а также применение в них информационного противоборства и радиоэлектронной борьбы. Показано, что в современных сетецентрических войнах массированное применение средств радиоэлектронной борьбы и информационно-технических воздействий обеспечивает достижение тотального информационного превосходства, способствующего быстрому достижению целей войны. Применение сил и средств радиоэлектронной борьбы обеспечивают: нанесение первого удара высокоточным оружием, блокировку систем противовоздушной обороны, нарушение систем государственного и военного управления, защиту авиации при ее боевом применении. Применение сил и средств информационных операций в технической сфере обеспечивают: блокировку информационного обмена в интернет-сегменте страны, блокировку финансовых транзакций, нанесение удара по важным объектам критической информационной инфраструктуры, обеспечение точечного информационного воздействия на лиц, принимающих решения, за счет рассылки e-mail или sms-сообщений. Применение сил и средств психологических операций обеспечивают: формирование позитивного восприятия агрессоров в сознании мирового общественного мнения и гражданского населения страны, втянутой в конфликт.

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, радиоэлектронной борьбы и информационного противоборства.

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 частно-

сти, в монографии при рассмотрении концепции сетецентрических войн, тенденций и перспектив развития радиоэлектронной борьбы и информационного противоборства автор сознательно ориентируется 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.

При подготовке монографии автор использовал только открытые материалы, на которые в списке литературы приведены соответствующие ссылки. Там, где это было возможно, указаны ссылки на расположение этих материалов в сети Интернет, чтобы особо заинтересованные читатели могли с легкостью обратиться к первоисточникам. При этом автор стремился к тому, чтобы монография по своему содержанию могла бы выступить своеобразным справочным пособием. Некоторые повторы и пояснения приведены для облегчения понимания материала неспециалистами, которые стремятся ознакомиться лишь с отдельными проблемами радиоэлектронной борьбы или информационного противоборства.

Автор не претендует на всеобъемлющее изложение всей затронутой проблематики в военной и технической области. Да это и невозможно — ведь прикладные области радиоэлектронной борьбы и информационного противоборства являются молодыми, многообразными и бурно развивающимися отраслями научного знания и использования технических возможностей. Кроме того, не все затронутые в монографии темы рассмотрены с одинаковой степенью подробности, что обусловлено стремлением автора глубже рассмотреть те вопросы, которые соответствуют области его научных интересов. Хочется надеяться, что читатель найдет эти обстоятельства извинительными и не будет сурово осуждать представленную работу за определенную неполноту и непоследовательность.

Благодарности

Автор выражает благодарность рецензентам: доктору технических наук профессору Е.В. Гречишникову, доктору технических наук старшему научному сотруднику С.Н. Гриняеву, доктору технических наук профессору Ю.Л. Козирацкому, доктору технических наук профессору А.И. Куприянову, доктору технических наук профессору Ю.М. Перунову, за поиск ошибок и неточностей при рецензировании монографии.

Автор благодарит кандидата технических наук профессора А.В. Баженова, кандидата технических наук доцента А.В. Кихтенко, доктора технических наук профессора В.И. Владимирова, доктора технических наук профессора Ю.И. Стародубцева, доктора технических наук профессора А.Г. Ломако, за то, что именно они способствовали становлению автора как ученого, и я безмерно горжусь тем, что имел возможность работать рядом с такими людьми, и особенно — учиться у них.

Также хочется отметить, что эпатажная критика исследований автора в их начальный период доктором технических наук профессором И.И. Снытким способствовала росту научного кругозора автора, его творческого потенциала,

а также способности вести научные дискуссии, отстаивать свою точку зрения и просто волю к победе.

Кроме того, выражаю свою благодарность доктору технических наук профессору К.Ю. Цветкову за то, что в период многократных организационно-штатных мероприятий, проходивших в «смутное время оптимизации» российских Вооруженных сил, он поддержал автора и дал ему возможность продолжить службу на возглавляемой им кафедре.

Отправной точкой в формировании направления исследований автора в областях радиоэлектронной борьбы и информационного противоборства послужили кандидатская диссертация С.И. Бабусенко и научные работы доктора технических наук профессора В.И. Владимирова. Автор всегда восхищался научной дальновидностью и огромным потенциалом их работ, которые он взял смелость продолжить и развить в своих исследованиях.

Плодотворные исследования в областях радиоэлектронной борьбы и информационного противоборства стали возможными благодаря тем людям, которые помогали, поддерживали, направляли, критиковали и всячески способствовали автору в его исследованиях. Автор выражает благодарность за доброжелательную критику, научную и организационную поддержку, а также за плодотворное общение всем тем, с кем он обсуждал вопросы радиоэлектронной борьбы и информационного противоборства на встречах, семинарах, конференциях, а также в процессе выполнения совместных НИОКР. Кроме того, автор считает своим долгом поблагодарить всех тех специалистов, которые внесли свой научный и исторический вклад в развитие теорий радиоэлектронной борьбы и информационного противоборства.

Особую признательность хочется выразить коллективам: кафедры эксплуатации и ремонта бортового авиационного радиоэлектронного оборудования (радионавигации и радиосвязи) Ставропольского ВВАИУ, кафедры радионавигации и радиолокации ВУНЦ ВВС «ВВА имени проф. Н.Е. Жуковского и Ю.А. Гагарина», кафедры сетей и систем связи космических комплексов ВКА имени А.Ф. Можайского, на которых автору посчастливилось проходить службу. Их творческая атмосфера всегда способствовала плодотворной деятельности и определила области научных интересов и направления исследований автора.

При подготовке монографии к изданию весьма ценными были замечания и предложения кандидатов технических наук Р.Л. Михайлова, К.В. Ушанева, В.Е. Федосеева, Е.С. Абазиной и А.А. Ковальского. Именно они помогли сделать материал монографии лучше и доступнее. Кроме того, автор глубоко признателен В.В. Вересияновой за кропотливый редакторский труд при подготовке рукописи.

Автор будет рад сотрудничеству в рассматриваемой области исследований, а также конструктивным замечаниям и предложениям. Замечания и предложения прошу направлять по адресу: mak-serg@yandex.ru

С.И. Макаренко

1. Концепция сетецентрической войны

1.1. Трансформация способов и форм военных действий под влиянием информационно-технической революции

1.1.1. 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:

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

В СССР автором советской версии концепции «революция в военном деле» считается начальник Генерального штаба вооруженных сил (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, объединяющей 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 ВС, то сейчас передовые улучшения затрагивают в первую очередь системы управления и разведки. Техническая сторона современной революции в военном деле основана прежде всего 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.

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 ВС.

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].

Таблица 1.1 — 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

В американской армии «информационно-техническая революция в военном деле» получила развитие в виде концепции «системы систем», предложенной заместителем председателя комитета начальников штабов (КНШ) министерства обороны (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 замене 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 ВС в конфликтах, которые в иных условиях могли бы повлечь

неоправданные по политическим и другим причинам жертвы среди мирного населения [16].

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, ВС США должны перенести центр тяжести в системе оборонного планирования с модели, ключевым моментом которой являются 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, ВС 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, необходимо предвидеть появление новых и разнообразных противников, которые будут полагаться на фактор внезапности, обмана и на применение асимметричного оружия для достижения своих целей [2].

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 концепции ведения противоборства, получивших наименование «сетецентрическое противоборство» или «сетецентрическая война» NCW (Network-Centric Warfare) [2].

1.1.2. Основные особенности «бесконтактных» войн нового поколения

На рубеже XX–XXI вв. мир вступил в полосу региональных вооруженных конфликтов и политической нестабильности. Число крупномасштабных военных акций глобального, регионального и национального характера резко увеличилось. Оценка военно-стратегической обстановки показывает, что начавшаяся более двадцати лет назад трансформация форм и способов ведения боевых действий под влиянием концепции сетецентрической войны в последние годы приобретает всё более актуальный характер [3].

При этом всё чаще для достижения геополитических или экономических целей используется скрытое или «латентное» противоборство, а также интенсифицируется применение невоенных форм борьбы [3, 121].

Ключевым способом такой невоенной формы 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 — сформировать требуемую «информационно-виртуальную реальность», что обеспе-

чит управление общественным мнением в подтверждение необходимости, «законности» и эффективности применения силы. Мощное информационно-психологическое воздействие на личный состав ВС 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 необходимы разработка и реализация принципиально новых алгоритмов принятия решений и защищенных технических средств управления [3].

В сфере прямого военного столкновения доминирующее значение приобретают воздушно-космические средства вооружения, а также высокоточное оружие (ВТО), что приводит к тому, что борьба за господство в воздухе и космосе во многом определяет развитие операций на суше и море [3, 121]. 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. При этом 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 они не прекратят сопротивляться его сокращению и ликвидации до тех пор, пока не накопят достаточные запасы ВТО, а также пока не разовьют средства ведения «бесконтактных» войн нового поколения [173].

Войны нового поколения будут вестись, как правило, с применением обычного оружия и, главным образом, ВТО, 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 нового 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 нового поколения решающая роль отводится уже не большому количеству сухопутных войск и ядерному оружию, а высокоточному, обычному ударному и оборонительному оружию, а также информационному оружию. 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 [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 обеспечиваются управление, связь, метеообеспечение, навигация, радиоэлектронная борьба (РЭБ) 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 применение 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, он не сможет захватить инициативу, планировать действия своих войск и эффективно ими управлять. «Бесконтактный» 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 нового 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 нового поколения отражены в работах В.И. Слипченко. К числу наиболее важных характеристик бесконтактных войн следует отнести [17, 29]:

- универсальную для бесконтактных войн единую глобальную разведывательно-информационную систему 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;
- единую систему 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 информационно-психологических операций на всех этапах ведения войны.

Несмотря на то, что войны нового поколения являются «бесконтактными», в угрожаемый период или с началом такой войны будет осуществляться стратегическое развертывание ВС (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 всё 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 государств отстающих в военно-техническом отношении стратегическое развертывание будет сводиться в основном к мобилизации значительной части населения. Успех ее проведения будет зависеть прежде всего от моралъ-

ного 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 и 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 (КР) по объектам систем управления вооруженными силами противника и его противовоздушной обороне (ПВО). При этом в первую очередь удары будут наноситься по зенитным ракетным комплексам большой и средней дальности. 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 оборонно-промышленного комплекса (ОПК), нарушена система управления государством и ВС, выведены из 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 полно-

стью 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. При этом нет никаких гарантий, что не придется решать подобные задачи и в будущем [1].

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].

Слабая 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 вооружения и военной техники (ВВТ) (авиация, зенитные ракетные комплексы, тактические ракеты, бронетехника, боевые корабли и катера) слабая сторона постарается рассредоточить, замаскировать, применять постепенно и внезапно для поддержания у противника 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.

Поле будущего дистанционного боя условно можно разделить на пять функциональных зон [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, раздробленное 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 исчезнут 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 ВТО, элементы противоракетной обороны (ПРО), десантные силы, средства разведки и наблюдения. В результате количество средств поражения стратеги-

ческой 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 средствами массовой информации (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. Всё 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].

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 незащищаемых 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].

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 радиоэлектронного подавления (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), на 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].

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 мероприятия и

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

В целом, на перспективу после 2030 г. ожидается окончательное утверждение новых форм применения войск, таких как массированный удар ВТО, совместное применение средств РЭБ, огневого поражения и т. п.

Основными характерными чертами войн нового поколения являются [17]:

- появление и массовое применение нового главного оружия военных действий — ВТО в обычном оснащении;
- 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;
- возможно, асимметричный характер 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.

Ведущей и устойчивой тенденцией в изменении способов боевых действий можно считать стремление к одновременному разгрому противника на всю глубину его оперативного построения при сосредоточении боевой мощи против основных объектов, определяющих оперативную устойчивость группировки противостоящей стороны [29, 50].

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 театре военных действий (ТВД), а также 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;
- возрастают роль и значение не только мобильности войск (сил) на тактическом и оперативном уровнях, но и стратегической мобильности вооруженных сил в целом.

1.1.3. Современные тенденции по повышению роли 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 войнах и вооруженных конфликтах XXI века будут максимально широко использоваться силы и средства воздушного и космического нападения, дальнего огневого, информационного и радиоэлектронного поражения [269].

В современных вооруженных конфликтах одной из особенностей ведения боевых действий является безусловный приоритет разведки, автоматизированных систем управления (АСУ) войсками и оружием, а также 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 ему удары на всю оперативно-тактическую глубину [17, 29].

Внедрение «неядерных» систем ВТО 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 и антитеррористических операций особое значение приобретают социально-политические, религиозно-этнические и психологические аспекты. Поэтому для разрешения конфликта 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].

С точки зрения способов и стратегии ведения военных действий в войнах нового 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 предыдущих 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 связанна 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 ВС [5, 29].

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

- вначале осуществляется завоевание 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 управле-

ния 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 ресурсов;
- после достижения целей воздушно-наступательной операции (кампании) могут быть начаты операции наземными группировками войск.

Естественным следствием изменений в характере вооруженной борьбы является зарождение новых форм вооруженной борьбы, например таких как информационно-ударная операция [269].

Информационно-ударная операция представляет собой совокупность взаимосвязанных и согласованных по цели, задачам, месту, времени и способам ведения информационно-ударных сражений, информационно-огневых боев и информационных ударов, проводимых с целью дезорганизации системы управления войсками и оружием (СУВО) противника и уничтожения его информационных ресурсов [269].

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 РЭБ 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, систем ПВО и РЭБ [269].

Информационное противоборство станет неотъемлемой частью военных действий. Без преимущества в этой сфере даже более сильная в военном плане сторона столкнется с серьезными трудностями при организации 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 (РЭО) не позволят противостоящей стороне организованно вести боевые действия. Массированному психологическому воздействию подвергнутся военно-политическое руководство, военнослужащие и гражданское население противника в целях 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 войне нового поколения свойственны следующие основополагающие аспекты:

- во-первых, это системная война;
- во-вторых, это война, где основные сценарии определяются на основе сложных эффектов всей системы;
- в-третьих, это война за обладание решающим потенциалом глобального управления.

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 высокую актуальность получат другие сферы: информационная, экономическая и психологическая. Поэтому содержание конкретных военных событий вооруженной борьбы будущего будет тесно взаимосвязано с другими видами противоборства — экономическим, информационным, психологическим [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 — скоординированные по времени психологические и информационно-технические операции 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.

Таким образом, 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.

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

1.2.1. 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 ВС 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, ВС технически развитых государств, имея средства ВТО 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» ВС 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 и др.

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

- противником 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;
- в войне широко использовались новейшие информационные технологии и современные системы 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 ВС 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, получившими 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 ВС придется действовать в среде, характеризующейся всё 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 ВС и системы государственного управления. В будущем ведение военных 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 потенциально

получить как за счет использования внутреннего ресурса самих ВС, так и задействования других госструктур и т. п. Необходимо уменьшить внутренние формальные процедуры согласования в интересах повышения адаптированности подразделений ВС 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 ВС в вооруженной борьбе. В большей степени акцент будет делаться на проведение невоенных операций, что требует повышения значимости сферы информационного противоборства, а также тесного взаимодействия с негосударственными организациями и структурами.

Для организации деятельности ВС 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.

1.2.2. Основные 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 ВС США.

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) [148, 152, 153].

Анализ концепции сетецентрической войны на основе работ [2, 29, 53, 112, 148, 152, 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].

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 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 более 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 ВС основывается главным образом на использовании жестких иерархических структур в звеньях ниже штабов отдельных видов и родов войск. В такой иерархической структуре отдельные и в основном автономные 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 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 дос-

тупные 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 ВС по обмену информацией. Это ведет к появлению новых принципов ведения боевых действий и в целом — к повышению боевой эффективности ВС. При этом под взаимодействием понимается 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 ВС. Такое изменение должно быть поддержано гарантией того, что компоненты ВС будут иметь технические возможности по использованию информационных сетей, независимо от их географической или организационной принадлежности. Таким образом, необходимость обеспечения гибкости действий ВС 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 (Net-Centric Environment Joint Functional Concept — NCE JFC) описывает возможности, вытекающие из использования единого информационного пространства и технической совместимости всех компонентов ВС, 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 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 синхронизации и интеграции компонентов сил, в том числе и на самых низших уровнях. В данной концепции тер-

мины «сеть» и «сетевой» используются как синонимы понятия «сетецентричности» [112].

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 ВС, 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 информационных технологий. В конечном итоге ВС 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 ВС и союзникам при выполнении задач действовать более эффективно (быстрее и качественнее). Важно, что эти новые возможности позволят применять ВС 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 апробирована 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» [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].

1.2.3. Понятие сетецентрической среды

Сетецентрическая среда, оперирующая возможностями и условиями (атрибутами), может рассматриваться в виде модели, состоящей из двух областей (рис. 1.1) [112].

1. Области знаний.
2. Технической области.

Область знаний включает в себя [112]:

- когнитивную область;
- социальную область.

Техническая область включает в себя [112]:

- физическую область;
- информационную среду.

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 областей 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].

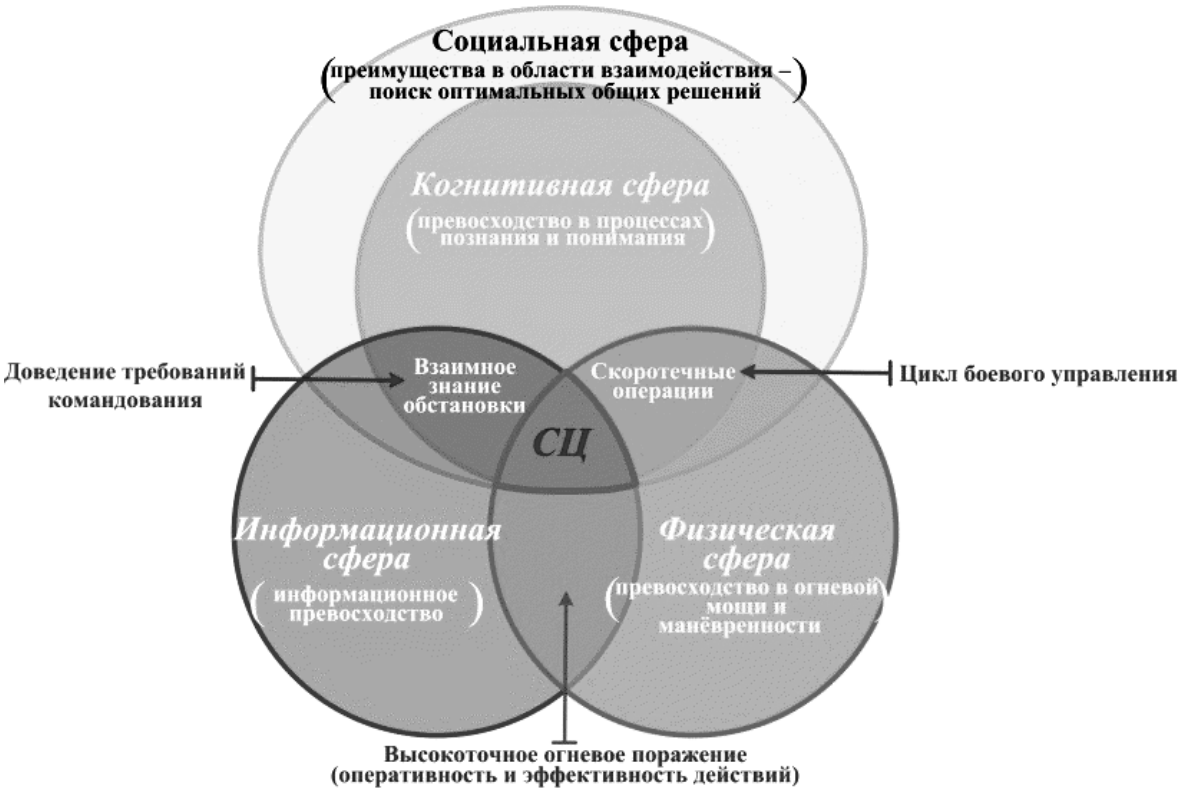


Рис. 1.1. Сетецентрическая среда [112]

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

Физическая область — это традиционная область войны, в которой происходит столкновение средств ВС во времени и в пространстве. Эта область включает в себя среды ведения боевых действий (море, суша, воздух, космическое пространство), средства (комплексы) ВВТ, 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 их способности вести боевые действия. В эпоху сетецентрических 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.

Именно 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 [112].

Когнитивная область. Когнитивной областью является 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 [112].

Социальная область. 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 [112].

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 областей 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, а процесс принятия решения становится коллективным [112].

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

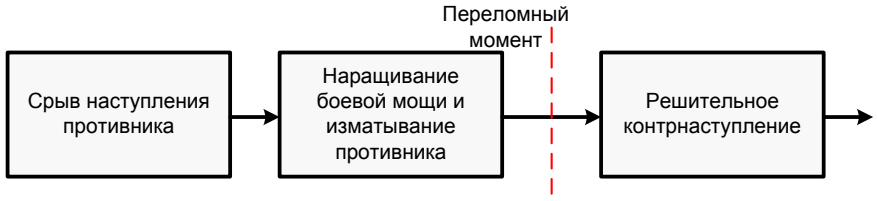
Сетецентрическая среда, интегрированная из коммуникационных сетей и сетей датчиков, программного обеспечения и организационных структур, обеспечит [2, 121]:

- 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;

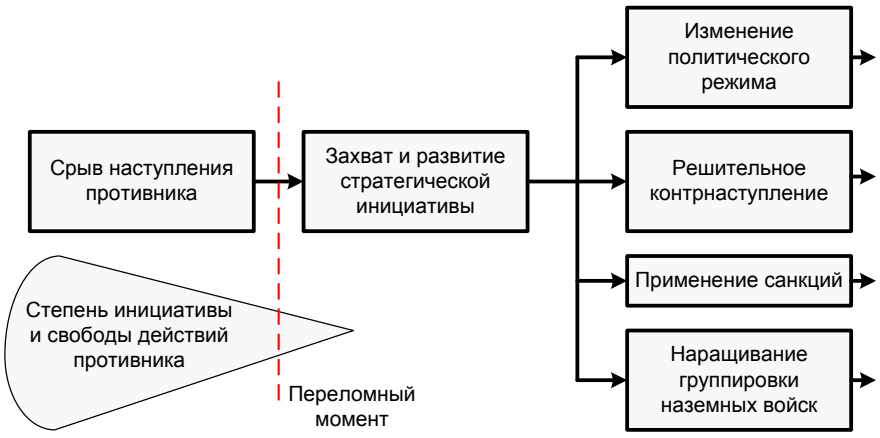
- единое информационное пространство для информационного обмена участников операций и доступа к информационным услугам, основанное на устойчивых и высокоскоростных средствах связи и телекоммуникации;
- оперативное доведение информации (в масштабе близком к реальному времени) о ходе проведения операций, точные и своевременные разведывательные данные о местоположении и действиях, как противника, так и своих войск;
- способность одновременно проводить взаимоувязанный комплекс операций на всём 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.

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. 1.2).



а.



б.

Рис. 1.2. Этапы вооруженного конфликта:
а. — традиционный конфликт; б. — конфликт в соответствии с концепцией сетецентрической войны

Коллективное распределение и обработка информации в сетецентрической среде приведет к необходимости развития организационных принципов управления. Вооруженные 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 ВС 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].

1.3. Критические аспекты концепции сетецентрической войны

Первоначально подходы к сетецентрической войне были предложены еще в конце прошлого века вице-адмиралом ВМС США А.К. Себровски (A. K. Cebrowski) и экспертом Министерства обороны Дж. Гарсткой (J. Garstka) в работе [152], 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 поделилось на серьезно сомневающихся сторонников и противников этой инновационной концепции.

Начиная с 2000 г. Министерство обороны США осуществляет масштабные мероприятия по реализации концепции сетецентрической войны в ВС. Положения о необходимости «сетецентричности» и выгодах, которые она представляет, занимают значительное место в доктринальных документах по ведению боевых действий объединенными группировками войск и применению видов ВС, а также в других руководящих документах. США планируют завершить создание глобальной информационно-управленческой сети к 2020 г. Совет по функциональным сетецентрическим возможностям в ходе разработки требований к ВВТ оценивает будущие системы оружия с точки зрения возможности их встраивания в общую информационную сеть. Министерство обороны США затратило и продолжает расходовать миллиарды долларов для создания «сетецентрических вооруженных сил». На сегодняшний день только в сухопутных войсках на эти цели уже потрачено 230 млрд долларов [82, 94].

Однако в последнее время в американской печати значительно уменьшилось количество публикаций по вопросам высокой 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 считалось раньше [82, 94].

Тот факт, что среди американских военных экспертов есть не только сторонники, но и 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 относящейся к военно-политическому доминированию США. Заместитель редактора международного издания Eurasia Critic К. Курдж в работе [243] отмечал, что «эта концепция используется в качестве политического дискурса для оправдания войны, презентуя вóйны 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 и военному аппарату бороться эффективнее при условии, что доктрина и организация или ВС выстроены в соответствии с оценкой угрозы».

1.3.1. Информационные ограничения на реализуемость концепции сетецентрической войны

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, 94].

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 сетецентри-

ческой 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 сетецентрической 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 до такой степени, когда скорость принятия решений человеком, является «слабым звеном» процесса управления войсками»;
- уязвимость технических средств и программного обеспечения в системах военного назначения к воздействию средств РЭБ и информационно-технического оружия.

В настоящее время практическое внедрение на пунктах управления технических решений для управления сетецентрической войной привело к информационной перегрузке лиц, принимающих решения. 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].

Анализ, проведенный в работах А.В. Копылова [82, 94], позволил сформировать следующие критические аспекты концепции сетецентрических войн.

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 посылом нельзя не согласиться. «Однако скорость принятия решений не должна приобретать господствующую роль в ущерб человеческим факторам, лежащим в основе процесса управления войсками», — указывают их оппоненты. Поддержание высокой скорости управления может привести к поспешным и непродуманным решениям.

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 ВС были

чрезмерно сфокусированы на преимуществах, которые дает информация, и что виды ВС, 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 систем 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 всё 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 кодов 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 [82].

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, концепция 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 применять свои силы и средства вооруженной борьбы и обеспечить достижение целей операций объединенных группировок войск [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 ВС потенциального противника будут развивать контртехнологии и становиться более подготовленными в вопросах организации защиты, оборудования укрытий, обмана и применения систем РЭБ. 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].

1.3.2. Возможности асимметричного противодействия в сетецентрической войне

1.3.2.1. Сущность асимметричного противодействия

Глобальное лидерство в экономической, технологической и военной сферах и широкое внедрение в практику ВС 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 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.

Как показал анализ, проведенный в работе [16], большинство прорывных военных технологий последнего времени, которые используются для модернизации ВС ведущих зарубежных стран, являются коммерческими разработками, а не результатами военных исследований.

К числу этих основных факторов, определяющих широкое внедрение технологии 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;
- высокую конкуренцию на рынке вооружений, обуславливающую необходимость снижения стоимости конечного продукта без потери его функциональности.

Однако эффективность использования двойных и коммерческих технологий создает ряд 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 того, что потенциальный противник также получит заблаговременный 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 благоприят-

ных 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.

В настоящее время в ВС ведущих зарубежных стран «второго эшелона» (Китай, Индия, Пакистан, Иран) резко активизированы исследования, посвященные возможным асимметричным действиям против современных высокотехнологических армий (прежде всего США, а также 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) актуален, также и для самих США, занимающих позицию бесспорного лидера. Это связано с необходимостью превентивного поиска мер, направленных на устранение уязвимостей сетецентрической концепции, и недопущению использования против своих сил и средств асимметричных способов противоборства. 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 условиях, в которых сложно реализовать свое техническое преимущество, расширение географических границ и длительности конфликта, выбор объектов нападения с учетом не их военного значения, а воздействия на моральное состояние личного состава и гражданского населения противника, провоцирование несоразмерного применения силы, активное ведение 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 высококвалифицированного 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 достаточного количества ресурсов — производственных, интеллектуальных, научных, технологических и т. п.) от прямого противоборства 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 в определенном смысле 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 краткосрочными 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 относятся [95]:

- угроза 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.

1.3.2.2. Асимметричное противодействие в сетецентрических войнах за счет использования специализированных информационных технологий и средств РЭБ

Анализ, проведенный в работах А.В. Копылова [82, 94], позволил сформировать следующие критические аспекты концепции сетецентрических войн, делающие возможным асимметричное противодействие за счет использования двойных информационных технологий и средств РЭБ.

Недооценка противника. Успех сетецентрической войны в значительной степени зависит от развертывания сети датчиков разведывательной системы для обнаружения действий и местоположения своих войск и войск противника. Однако в результате исследований, проведенных в 2002 г., сотрудники корпорации RAND пришли к выводу, что, если ВС потенциального противника будут эффективно развивать контртехнологии и становиться более подготовленными в вопросах организации маскировки, информационно-технических воздействий и ведения РЭБ, то эффекты от применения принципов сетецентрического ведения боевых действий могут быть полностью нивелированы.

По мнению специалистов из корпорации RAND, другими высокоэффективными способами борьбы с противником, ведущим сетецентрическую войну, могут быть:

- использование мощных средств РЭП и устройств направленной энергии для подавления информационно-космических систем связи, навигации и разведки;
- применение малогабаритных средств РЭП устройств и направленной энергии для того, чтобы на расстоянии вывести из строя элементы схем РЭС;
- массовое применение информационно-технического оружия с целью нарушить работу компьютеризированных систем управления войсками и оружием.

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 ложное видение обстановки и в конечном итоге навяжут противнику свою стратегию действий или полностью перехватят управление его силами и средствами.

В значительной мере росту угроз асимметричного противодействия высокоразвитым ВС, ведущим сетецентрическую войну, способствуют широкое распространение и доступность уже готовых технологий двойного назначения, которые можно использовать в военных целях.

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 ВС 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.

Еще одной доступной технологией двойного назначения является информационно-техническое оружие, ориентированное на деструктивное воздействие на телекоммуникационную инфраструктуру, на АСУ и на информационные потоки, циркулирующие в них.

Быстрое внедрение перспективных информационных технологий делает возможным неожиданное появление мощного асимметричного информационно-технического 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].

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 и для «отсталых стран», не имеющих современной научно-технической и производственной базы, а также для 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].

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 получили официальное признание «полная зависимость инфраструктуры США от информационных систем и сетей» и уязвимость последних [95].

Сделав ставку на высокую компьютеризацию ВС США и ведение сетецентрических войн, Пентагон стал испытывать всё 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 кибератак на свои компьютерные сети и серверы, руководство Пентагона, оказавшись перед новой угрозой, поручило Стратегическому командованию разработать 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 нём 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 ВС 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 США Р. Гейтс объявил о создании (в соответствии с указанием президента) в ВС принципиально новой структуры — Объединенного кибернетического командования USCYBERCOM (United States Cyber Command). Оно ориентировано на организацию и проведение масштабных наступательных и оборонительных боевых действий в кибернетическом пространстве [95].

Уязвимость боевой техники от воздействия средств РЭБ. Еще одним эффективным средством асимметричного противодействия системе управления и высокотехнологическому вооружению выступает радиоэлектронная борьба.

Под радиоэлектронной борьбой (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 радиоэлек-

тронной защите своих систем и средств управления войсками и оружием и противодействию техническим средствам разведки противника [29].

Задачами, которые решаются системами 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.

Система РЭБ с методологической точки зрения позволяет практически организовать срыв любой военной операции (при условии наличия технических средств РЭБ и возможностей по ее эффективному применению) [29].

Таким образом, подводя итог, можно сделать вывод, что в рамках подготовки к асимметричному противодействию технологически развитому противнику можно выделить следующие пути [29]:

- недопустимость прямого соперничества в создании и развертывании систем и комплексов вооружения;
- ориентация на асимметричные средства вооруженного противостояния в ответ на дорогостоящие средства потенциального противника;
- 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 нового поколения.

2. Радиоэлектронная борьба

Важным и исторически наиболее развитым направлением информационного противоборства является борьба с системами управления противника за счет использования средств РЭБ.

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

Исходя из этого, рассмотрение современного информационного противоборства необходимо начать с рассмотрения РЭБ как ее исторически наиболее важной и развитой части, которая играет важнейшую роль в современных и будущих сетецентрических войнах.

Ниже представлена терминология радиоэлектронной борьбы, принятая в ВС США и в ВС России. На примере ВС США проведен анализ организационно-штатных изменений структурных подразделений, ведущих радиоэлектронную борьбу при переходе к концепции сетецентрической войны. На примере систем и средств, используемых в ВС США, проведен глубокий анализ средств РЭБ, ориентированных на борьбу как с системами управления оружием, так и с системами связи. Кроме того, обзорно представлены средства РЭБ функционального поражения, основанные на сверхвысокочастотном (СВЧ) и лазерном излучении.

2.1. Роль и способы применения РЭБ в сетецентрической войне

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

Анализ оперативных учений, локальных войн и вооруженных конфликтов последних лет позволяет сделать вывод о том, что радиоэлектронная борьба в

ВС 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 ВС США в вооруженных конфликтах показал, что даже подавляющее превосходство в области средств ВТО не гарантирует благоприятного исхода операции в том случае, если системы управления различного уровня оставались неподавленными [95, 256].

Объектами первоочередного воздействия систем РЭБ в ходе операции являлись [95]:

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

Аналитики Пентагона полагают, что основными причинами повышения роли радиоэлектронной борьбы в современных сетецентрических войнах являются [95, 256]:

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

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

Средства РЭБ могут применяться скрытно и открыто, входить в состав различных многоцелевых функциональных и автоматизированных интегрированных систем многосферного базирования, боевого управления, связи, компьютерного обеспечения разведки, огневого поражения, борьбы с системами управления противника и защиты своих систем, использовать в своих интересах сети ЭВМ противоборствующей стороны и воздействовать на них [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 века. Это привело к изменению характера радиоэлектронной борьбы, ее содержания, состава сил и средств, роли, места, цели и задач в операциях. Эти факторы предопределили создание новых средств РЭБ, в том числе 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, 371].

Развитие сил и средств РЭБ и преобразование их в одну из основных составляющих сил «борьбы с системами боевого управления» вызвало появление новых понятий в стратегии и терминологии информационной войны, таких как «война в сетях» или «сетевая война» (Net War), «кибервойна» (Cyber War), «ведение боевых действий и управление вооруженными силами в едином информационно-коммуникационном пространстве». Все эти термины предполагают организацию управления 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 радиоэлектронная борьба является основой информационного противоборства [95].

Анализ эволюции и развития РЭБ в ВС США и объединенными вооруженными силами (ОВС) НАТО позволил выявить возникшие в последние годы различия между характером, содержанием мероприятий и ролью РЭБ, которые сводятся к следующему [256].

- радиоэлектронная борьба в ВС США и в ОВС НАТО имеет различные объекты воздействия и защиты. Если мероприятия РЭБ в ВС ряда государств связаны только с воздействием на РЭС противника, то в ВС США, а в перспективе — и в ОВС НАТО они направлены как на воздействие, так и на защиту РЭС, а также распространяются на боевую

технику, объекты ВС и системы оружия. В рамках проведения мероприятий РЭБ в ВС США уже сегодня кроме использования источников излучения электромагнитной энергии и противорадиолокационных ракет предусматривается задействование других видов летального и нелетального оружия, базирующегося на излучении направленной энергии. При этом в качестве основной цели радиоэлектронной атаки средств РЭБ в ВС США рассматривается система ПВО противника.

- В мероприятиях РЭБ в ВС США имеется такой самостоятельный элемент, как «радиоэлектронное обеспечение операции» (боевых действий), который отсутствует в подобных мероприятиях ВС ряда других государств НАТО.
- Мероприятия РЭБ в ВС США и в ОВС НАТО являются основой противодействия системам боевого управления, то есть радиоэлектронная борьба стала наиболее важным составным элементом информационного противоборства. В других же странах это лишь один из элементов мероприятий оперативного обеспечения, проводимых при дезорганизации управления войсками противника в операции.

Как отмечается в программе создания сухопутных войск США нового типа, «радиоэлектронное поле боя» (Electromagnetic Field of Battle) претерпит значительные изменения с учетом расширения спектра используемых рабочих радиочастот РЭС, который станет более насыщенным и менее доступным для противника. Возрастут возможности, и станут более гибкими силы и средства РЭБ. Последние будут способны функционировать во всех частотных диапазонах, причем планируется применять различные средства летального и нелетального воздействия не только на РЭС противника, но и на его боевую технику и системы вооружения [95].

Анализ эволюции характера, содержания и роли РЭБ в операциях конца XX — начала XXI в. дает возможность вскрыть и сформулировать основные тенденции развития РЭБ в ВС США и в ОВС НАТО до 2025 г., которые наметились в ходе интеграции сил и средств разведки, РЭБ и борьбы с системами боевого управления. К таким тенденциям развития следует отнести следующие [256].

- Частичная утрата самостоятельной роли РЭБ, которая становится одним из основных элементов информационного противоборства, в основном для борьбы с системами боевого управления при проведении информационных операций.
- Коренное поэтапное изменение характера, содержания и роли РЭБ в операции (бое). Так, на первом этапе она являлась одним из видов поддержки ударных сил в ходе боевых действий, на втором — составной частью ведения боевых действий каждого вида ВС со всеми специфическими особенностями. На третьем этапе РЭБ стала компонентом синергетической системы информационного противоборства — одной из составляющих военного потенциала.

- Использование для ведения РЭБ новых видов направленной энергии, а также создание летального и нелетального оружия, действующего на новых физических принципах.
- Переход от подавляющего воздействия и защиты РЭС к комплексному поражающему и подавляющему информационно-техническому воздействию и защите не только РЭС, но и боевой техники, объектов ВС, систем оружия, а также личного состава 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 радиоэлектронной борьбы.

В настоящее время в ВС США радиоэлектронная борьба рассматривается, с одной стороны, как составная часть вооруженного противоборства и военного потенциала, а с другой — как одна из форм вооруженной борьбы и новый, относительно самостоятельный и специфический вид боевых действий. Отличительной особенностью современных взглядов на ведение РЭБ является признание ее комплексности и тесной связи с другими видами боевой деятельности войск [256].

Мероприятия РЭБ составляют основу новой активно внедряемой в ВС 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].

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 «радиоэлектронного поле боя» в информационной операции с участием сил и средств РЭБ предполагает последовательное выполнение четырех основных задач [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 следующие мероприятия [95]:

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

Доктринальными документами ВС США определены следующие основные задачи РЭБ в информационной операции [95]:

- дезорганизация системы управления противника, лишение его возможности использовать информацию о своих войсках и действиях противника;

- разрушение, искажение или создание неадекватной реальной обстановке информации, провоцирующей противника на неверные действия;
- повышение эффективности ведения боевых действий ВС США и их союзников;
- снижение людских и материальных потерь и завершение информационной операции в кратчайшие сроки.

В перечне задач выделяется воздействие не только на РЭС, но и на боевую технику, системы оружия и личный состав органов управления и обслуживания противника [95].

Радиоэлектронная борьба в ВС США подразделяется на следующие мероприятия (рис. 2.1) [95, 187, 250, 253, 256]:

- радиоэлектронная атака (EA — Electronic Attack);
- радиоэлектронная защита (EP — Electronic Protect);
- радиоэлектронное обеспечение (EWS — Electronic Warfare Support).

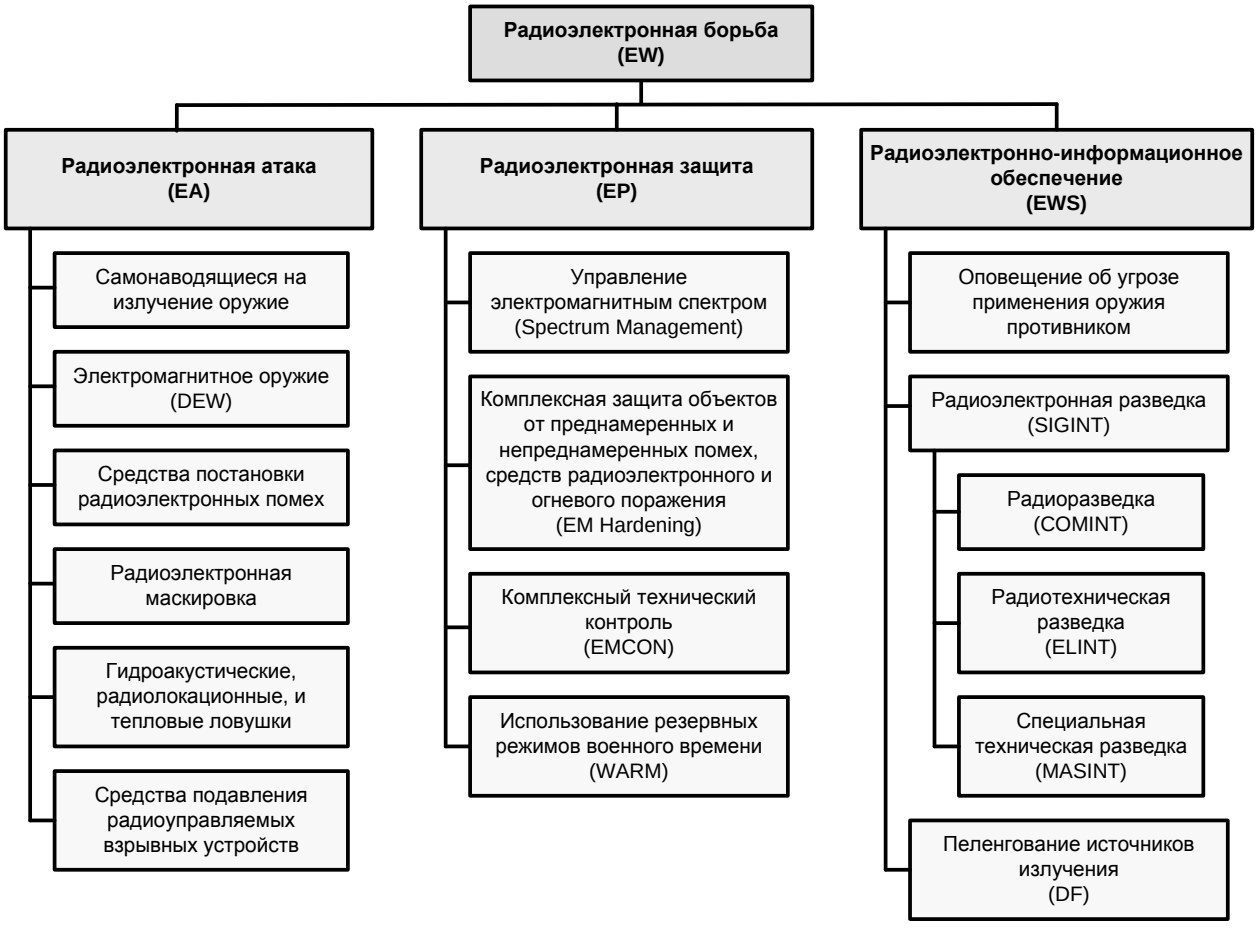


Рис. 2.1. Классификация РЭБ в ВС США [187]

Радиоэлектронная атака — действия наступательного характера, предусматривающие использование электромагнитной и других видов направленной энергии и (или) самонаводящегося на электромагнитное излучение оружия для целенаправленного воздействия на системы управления, личный состав, объекты и боевую технику с целью дезорганизовать, нейтрализовать или снизить

возможности противника по эффективному использованию им радиоэлектронных систем в различных звеньях управления ВС [95, 253].

Радиоэлектронная атака проводится с использованием [95]:

- средств РЭП и радиоэлектронной дезинформации;
- огневых средств, самонаводящихся на излучение различных радиоэлектронных устройств (например, излучение РЭС, систем пуска автомобилей, бронетранспортеров, танков, электропривода орудий и др.);
- управления режимами излучения электромагнитной и направленной энергии;
- управления ложной работой РЭС, имитацией их работы и обеспечения демонстративных действий;
- управляемого оружия с радио- и радиолокационными, инфракрасными, лазерными, гидроакустическими и другими головками самонаведения (ГСН);
- инфразвукового, радиочастотного, лазерного, пучкового и других типов оружия направленной энергии.

Для воздействия на информационные ресурсы противника в мероприятиях РЭБ в ВС США помимо использования источников излучения электромагнитной энергии и иных средств предусматривается применение ложных целей, летального и нелетального оружия, базирующегося на излучении других видов направленной энергии, в том числе действующих на новых физических принципах (инфразвуковое, лазерное, пучковое и др.) [95].

К объектам (целям) радиоэлектронных атак командование ВС США относит [235]:

- личный состав, боевую технику и системы оружия, а также различную радиоэлектронную аппаратуру;
- пункты управления, узлы связи и радиотехнического обеспечения;
- системы и средства боевого управления, связи, разведки, радиолокации, радионавигации.

Согласно наставлениям и уставам ВС США выбор конкретных способов и средств радиоэлектронной атаки, так же, как и электронной защиты, а также обеспечения ведения электронной войны, зависит от задач проводимой операции, возможностей противника и, собственно, имеющихся на вооружении или уже задействованных в операции соответствующих сил и средств. Кроме того, учитываются видовая принадлежность этих сил и средств, платформы размещения, тактико-технические характеристики и т. п. [235].

Разновидностями форм проведения радиоэлектронной атаки, по взглядам военных аналитиков США, являются [95]:

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

Таким образом, мероприятия радиоэлектронной атаки в зависимости от применяемых средств подразделяются на [95]:

- непоражающие;
- поражающие.

К непоражающим (нелетальным) средствам воздействия относятся [95]:

- средства радиоэлектронных помех;
- средства радиоэлектронной дезинформации.

Поражающими средствами воздействия являются [95]:

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

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

Задачами непоражающих средств при проведении радиоэлектронной атаки являются [95, 256]:

- срыв, подавление или вывод из строя радиоэлектронных и оптико-электронных систем, а также средств разведки, наблюдения, наведения, связи, навигации, управления войсками и оружием;
- изменение режима излучения РЭС;
- имитация и ложная работа РЭС, объектов и оружия своих войск и войск противника;
- имитация демонстративных действий войск;
- дезорганизация систем связи и управления противника;
- введение противника в заблуждение относительно намерений своих войск;
- воздействие на личный состав противника, обслуживающий РЭС, системы разведки, наблюдения, средства связи, навигации и управления войсками и оружием, а также участвующий в анализе добытой разведкой информации, подготовке и принятии решений, планировании операции или боя.

Задачами поражающих средств при радиоэлектронной атаке могут быть следующие [95, 256]:

- наведение на цель средств ВТО и оружия направленной энергии;
- уничтожение, разрушение и вывод из строя средств разведки, навигации, наблюдения;
- уничтожение, разрушение и вывод из строя средств, узлов, центров и органов связи, управления войсками и оружием противника, а также его объектов, боевой техники и систем оружия;
- поражение и вывод из строя личного состава противника, участвующего в подготовке, принятии оперативных (боевых) решений и планировании операции (боя).

Опыт локальных войн показал, что применение средств РЭБ ведется одновременно с применением средств ВТО и оказывается для противника кратковременным и неожиданным. В связи с этим было бы логично выделить отдельную форму радиоэлектронной атаки — «радиоэлектронный удар» [95].

При этом, в зависимости от состава привлекаемых сил и средств, «радиоэлектронные удары» могут быть [95]:

- одиночными;
- массированными.

С учетом пространственного размаха «радиоэлектронные удары» могут быть [95]:

- сосредоточенными;
- рассредоточенными.

Комбинированное применение средств РЭП и огневого воздействия в целях нарушения функционирования РЭС противника можно определить как «радиоэлектронно-огневой удар». В подобных ударах огневые средства поражения могут использовать как обычные боеприпасы, так и боеприпасы с радиолокационными ГСН. Учитывая широкомасштабные научно-исследовательские и опытно-конструкторские работы в области создания военной робототехники, его разновидностью может быть «роботизированный радиоэлектронно-огневой удар». Ответные радиоэлектронные и радиоэлектронно-огневые удары, возможно, приведут к новому виду формы боя — «радиоэлектронно-огневому бою» [95].

Радиоэлектронная защита включает в себя разносторонние пассивные и активные мероприятия и специальные средства, обеспечивающие защиту от любого воздействия противника и его средств РЭБ своих группировок войск, личного состава, боевой техники, систем оружия, объектов и отдельных радиоэлектронных средств. Кроме того, этот вид защиты предусматривает необходимые мероприятия и способы противодействия техническим средствам разведки противника, контроль за излучением своих РЭС, обеспечение управления их режимами и электромагнитной совместимости [256].

Средства и методы радиоэлектронной защиты можно условно разделить на три типа [256]:

- непосредственной защиты РЭС;
- обеспечения электромагнитной совместимости РЭС на пунктах управления и в боевых порядках войск;
- радиоэлектронной защиты при проведении информационных операций.

Задачами средств и методов непосредственной защиты РЭС в операции могут быть [256]:

- защита РЭС своих войск от преднамеренных радиоэлектронных и оптико-электронных помех противника;
- защита РЭС своих войск от случайных атмосферных, промышленных помех, непреднамеренных помех от РЭС гражданских ведомств и союзных войск;
- защита РЭС, боевой техники, систем оружия и личного состава своих войск от радиоэлектронной дезинформации противника;
- защита боевой техники, объектов, пунктов управления (ПУ), РЭС, систем оружия, боеприпасов от самонаводящегося на радиоэлектронные излучения оружия противника;

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

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

Задачами средств обеспечения электромагнитной совместимости РЭС на пунктах управления и в боевых порядках войск являются [256]:

- отслеживание и выдача рекомендаций на использование радиочастот и режимов работы различных РЭС в интересах исключения их взаимных помех;
- оценка нанесенного ущерба используемому спектру радиочастот и текущей радиоэлектронной обстановки;
- ведение радиоэлектронной разведки (РЭР).

К задачам сил и средств радиоэлектронной защиты при проведении информационных операций следует отнести [256]:

- информационную и радиоэлектронную защиту средств разведки, средств РЭП;
- радиоэлектронную защиту подразделений и средств РЭБ;
- информационную защиту сил и средств психологических операций;
- информационную защиту сил и средств, — ведущих сбор, передачу и обработку собственной информации.

Радиоэлектронное обеспечение информационной операции включает в себя мероприятия и средства, своевременно обеспечивающие разведывательные потребности штабов войск по выявлению и оповещению об угрозах, их немедленному распознаванию, оценке оперативной и радиоэлектронной обстановки, своевременному принятию оперативных решений, планированию операций, а также выработку данных, необходимых для целеуказания средствам поражения и воздействия в интересах радиоэлектронной атаки и защиты [95].

Фактически радиоэлектронное обеспечение представляет собой действия, направленные на обнаружение, идентификацию и определение местоположения РЭС противника, которые могут являться как источниками получения разведданных, так и источниками информационных угроз [249, 253].

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

Контроль за излучениями различных видов электромагнитной энергии предполагает круглосуточное обеспечение строгого выполнения установленных нормативов электромагнитного излучения войсками и техническими средствами в местах их постоянной дислокации, на учениях, а также при подготовке и в ходе проведения операций. При этом обычно контролируются мощность, характер, направленность и виды излучений, а также соблюдение установленных правил радиообмена и скрытного управления войсками (силами) [256].

Целями радиоэлектронной маскировки являются [256]:

- маскировка излучений объектов, боевой техники и РЭС в местах их постоянной дислокации, на учениях, при подготовке операций;
- введение противника в заблуждение относительно истинных режимов излучений электромагнитной энергии;
- выявление демаскирующих радиоэлектронных признаков объектов, боевой техники и войск в местах их постоянной дислокации, на учениях, при подготовке и в ходе проведения операций;
- принятие мер по минимизации и (или) исключению нарушений радиоэлектронной маскировки;
- обучение личного состава ВС методам радиоэлектронной маскировки в местах постоянной дислокации, на учениях, при подготовке и в ходе ведения боевых действий ВС и их союзников.

Задачами перепрограммирования средств РЭБ являются [256]:

- обеспечение своевременной нацеленности средств РЭБ, организации способов радиоэлектронных атак и защиты согласно установленной командованием приоритетности целей и объектов;
- реализация своевременной перестройки указанных средств в соответствии с изменением оперативной (боевой, радиоэлектронной) обстановки;
- достижение максимальной эффективности (по мощности, направлению, виду, типу радиоэлектронного обеспечения) радиоэлектронных атак и радиоэлектронной защиты при изменении формы, вида и характера электромагнитного излучения цели (объекта) и совершении целью (объектом) маневра;
- своевременное резервирование, замена излучающих средств и дублирование их при выходе из строя или уменьшении эффективности средств РЭБ, радиоэлектронных атак и защиты.

Планирование РЭБ, которое подразделяется на долгосрочное и краткосрочное, носит централизованный характер, а ее ведение — децентрализованный [95].

В ходе планирования радиоэлектронных атак, радиоэлектронной защиты и радиоэлектронного обеспечения определяются [95]:

- порядок обеспечения электромагнитной совместимости радиоэлектронных средств и защиты от радиоэлектронных излучений личного состава, объектов и боевой техники;
- способы разрешения конфликтных ситуаций по: устранению случайных и непреднамеренных помех, маскировки и радиоэлектронной разведки, радиоэлектронной безопасности, радиоэлектронного подавления и перепрограммирования средств РЭБ в ходе операции;
- способы контроля излучения РЭС, применения летального и нелетального оружия, разведывательного обеспечения сил и средств РЭБ и их сопряжения со средствами разведки.

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

Средства РЭБ по степени мобильности подразделяются на [95]:

- стационарные;
- подвижные.

При этом стационарные дислоцируются, как правило, на территории США и стран — союзников по блоку НАТО, а подвижные развертываются в ходе боевых действий на минимально возможном расстоянии от подавляемых радиоэлектронных средств [95].

2.1.2. Основные термины, определения и классификация систем, принятые в отечественной теории РЭБ

В отечественной теории радиоэлектронной борьбы принят несколько другой подход к целям, задачам и классификации мероприятий РЭБ. Рассмотрим основные отличия более подробно.

Радиоэлектронная борьба — совокупность взаимосвязанных по цели, задачам, месту и времени мероприятий, действий, направленных на выявление радиоэлектронных средств и систем противника, их подавление, радиоэлектронную защиту своих радиоэлектронных систем и средств от средств РЭП противника, а также на радиоэлектронно-информационное обеспечение [248].

Радиоэлектронная борьба проводится в тесной взаимосвязи с огневым поражением, захватом и выводом из строя РЭС и радиоэлектронного оборудования (РЭО) в системах управления силами и оружием противника [248, 254].

Первичная цель РЭБ — затруднение или исключение функционирования РЭО систем управления противника.

Основными задачами РЭБ выступают [248, 255]:

- вскрытие и анализ радиоэлектронной обстановки;
- дезорганизация управления силами и оружием противника, поражение систем управления войсками и оружием противника, а также его средств разведки и РЭБ;
- уничтожение (разрушение) и/или внесение искажений в программное обеспечение информационных систем противника, его баз данных и АСУ;
- снижение эффективности применения оружия, боевой техники и технических средств разведки противника;
- обеспечение устойчивости работы систем и средств управления своими войсками и оружием в условиях двусторонней РЭБ;
- обеспечение электромагнитной совместимости собственных РЭС.

Главными и конечными целями РЭБ как вида оперативного (боевого) обеспечения являются [248, 255]:

- повышение эффективности применения оружия по объектам противника;
- повышение боевой устойчивости собственных сил при отражении ударов противника.

К общим задачам РЭБ относятся [248]:

- дезорганизация управления силами, снижение эффективности применения оружия и боевой техники противника;
- снижение возможностей технических средств разведки противника;
- срыв или существенное затруднение выдачи целеуказаний силам противника на прицельное применение ими своего оружия;
- отвлечение части ударных сил противника и его оружия на ложные цели;
- обеспечение устойчивой работы систем управления своими силами и оружием.

Возрастание значения фактора времени, сложность и высокая динамичность общей оперативной и радиоэлектронной обстановки при ведении боевых действий в современных сетецентрических войнах, по взглядам отечественных специалистов, позволили определить следующие основные принципы организации и ведения РЭБ, изложенные ниже в соответствии с работой [248].

1. Соответствие организации и ведения РЭБ замыслу боевых действий. Цели, привлекаемые силы и средства РЭБ, время и порядок их применения, организация защиты от радиоэлектронной разведки и радиоэлектронного поражения противника должны быть тесно увязаны с действиями частей и соединений войск на ТВД, рассчитаны и спланированы по выполняемым ими задачам.
2. Массированное и комплексное применение сил и средств РЭБ на главных направлениях при решении войсками наиболее важных задач. Поскольку одновременное поражение всех РЭС противника затруднено и может привести к распылению усилий и невыполнению поставленных задач, то необходимо сосредоточить силы и средства РЭБ на главных направлениях и обеспечить быстрое перенацеливание их с одной задачи на другую. Такой же подход необходим при организации защиты своих РЭС от помех противника.
3. Внезапность применения сил и средств РЭБ, тактических приемов и способов ее ведения, исключение шаблонов в их применении достигается:
    - скрытием от противника планируемых мероприятий и планов их реализации;
    - созданием группировки сил и средств для решения задач РЭБ;
    - прогнозированием изменения радиоэлектронной обстановки и намерений противника, упреждением его в реакции на эти изменения.
4. Обеспечение непрерывного взаимодействия сил и средств РЭБ всех видов вооруженных сил, согласованности радиоэлектронного подавления с огневым поражением, а также между средствами РЭП и другими РЭС с целью обеспечения их электромагнитной совместимости.
5. Обеспечение одновременного комплексного воздействия на все важнейшие элементы систем управления силами и оружием противника.

6. Непрерывное осуществление мероприятий по радиоэлектронной защите своих систем и средств управления частями, подразделениями и оружием, постоянного проведения мероприятий защиты во всех видах деятельности войск и в любых условиях обстановки, а также с учетом действий противника. Для реализации этого принципа необходимы глубокое знание состава, возможностей и характера боевого применения сил и средств РЭБ противника, своих РЭС, а также непрерывная координация организационных и технических мер по радиоэлектронной защите.
7. Активное и комплексное противодействие техническим средствам разведки противника, которое достигается:
    - знанием состава и возможностей технических средств разведки противника;
    - проведением мероприятий по противодействию техническим средствам разведки;
    - организацией и осуществлением эффективного контроля проводимых вышеуказанных мероприятий.

Активность РЭБ, в целом, заключается в способности и готовности органов управления в любых условиях обстановки умело организовывать и настойчиво проводить мероприятия по дезорганизации системы управления противника, а также по сохранению устойчивости своей системы управления и снижению возможностей технических средств разведки противника [248].

Активность РЭБ достигается [248]:

- своевременным добыванием и анализом данных о силах и средствах управления, разведки и РЭБ противника;
- своевременной и скрытной подготовкой сил и средств, выделенных для решения задач РЭБ, к боевому применению, их решительными действиями в ходе боевых действий;
- организацией и поддержанием четкого и непрерывного взаимодействия сил РЭБ с обеспечиваемыми соединениями и частями.

В соответствии с отечественной методологией мероприятия РЭБ классифицируют следующим образом [248]:

- радиоэлектронное поражение (РЭПр);
- радиоэлектронная защита (РЭЗ);
- радиоэлектронно-информационное обеспечение (РИО).

Подробно эта классификация представлена на рис. 2.2.

Далее представлено описание отдельных мероприятий РЭБ по данным из работ [245, 248, 255].

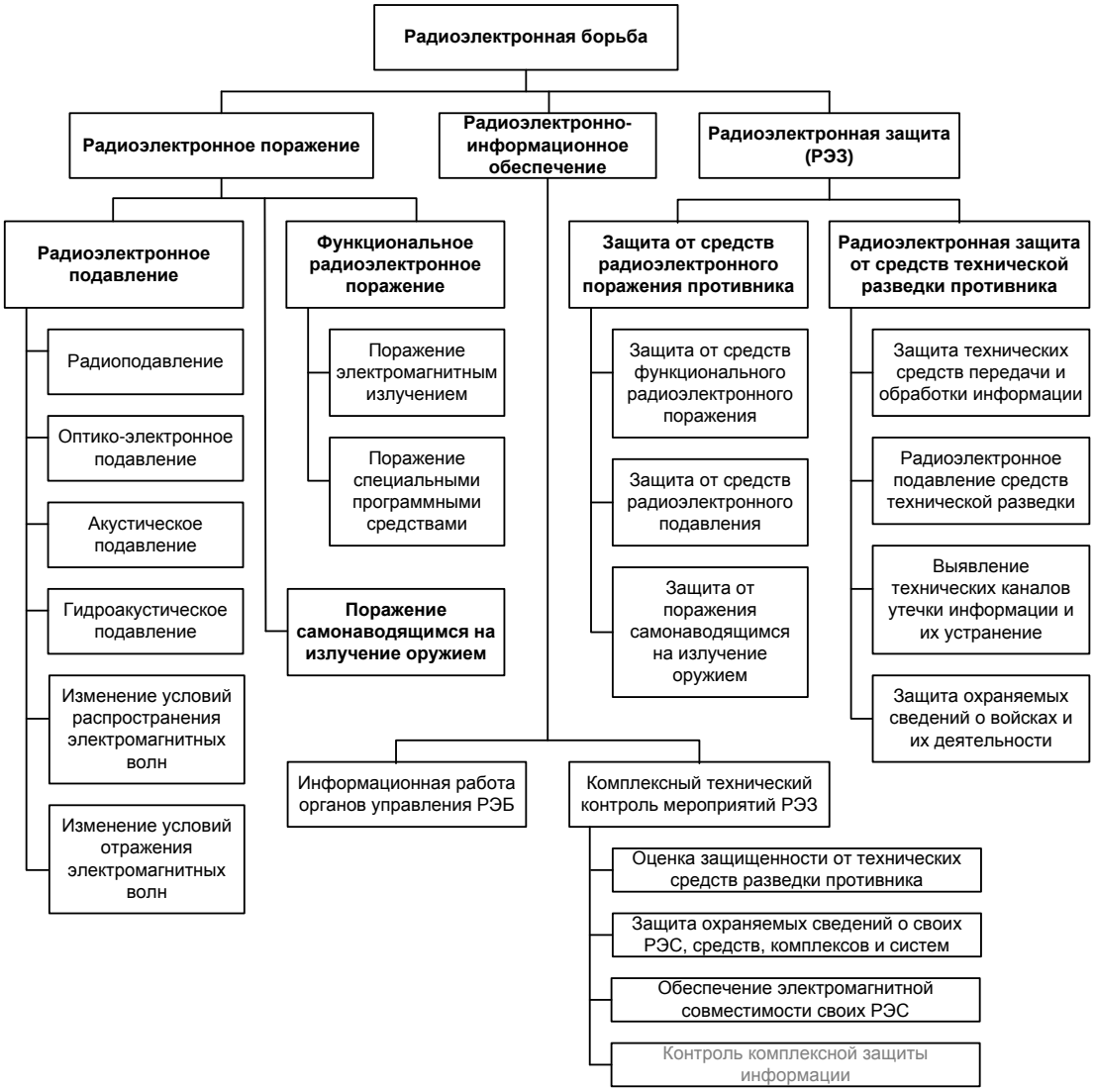


Рис. 2.2. Классификация мероприятий РЭБ [248]

Радиоэлектронное поражение (РЭПр) — совокупность мероприятий и действий по функциональному радиоэлектронному поражению, радиоэлектронному подавлению, поражению самонаводящимся на излучение оружием РЭС противника [248].

Радиоэлектронное подавление (РЭП) — радиоэлектронное поражение, заключающееся в снижении эффективности функционирования РЭС противника путем воздействия на них преднамеренными радиоэлектронными помехами [248].

Радиоэлектронное подавление включает: радио-, оптико-электронное, акустическое и гидроакустическое подавление. Одним из видов радиоэлектронного подавления также является изменение условий распространения и/или отражения электромагнитных волн. При этом различают радиоэлектронное подавление систем управления оружием и подавление систем управления войсками [248].

Более подробно составные части и мероприятия радиоэлектронного подавления рассмотрены далее.

Радиоподавление — радиоэлектронное подавление, ведущееся в диапазоне радиоволн и заключающееся в снижении эффективности функционирования РЭС противника путем воздействия на них преднамеренными радиопомехами [248].

Оптико-электронное подавление — радиоэлектронное подавление, ведущееся в оптическом диапазоне и заключающееся в снижении эффективности функционирования оптико-электронных систем противника путем воздействия на них преднамеренными оптико-электронными помехами. Результатом оптико-электронного подавления может быть нарушение работы тепловых, телевизионных, лазерных и оптико-визуальных систем и средств разведки, наблюдения и связи [248].

Акустическое подавление ведется в диапазоне акустических волн и заключается в снижении эффективности функционирования акустических средств противника путем воздействия на них преднамеренными акустическими помехами [248].

Гидроакустическое подавление — акустическое подавление, ведущееся в водной среде путем применения преднамеренных гидроакустических помех. Гидроакустическое подавление предусматривает создание помех стационарным и авиационным средствам гидроакустического обнаружения и гидроакустическим системам самонаведения оружия противника [248].

Изменение условий распространения электромагнитных (акустических) волн заключается в изменении свойств среды распространения электромагнитных (ЭМ) (акустических) волн путем применения средств постановки пассивных преднамеренных радиоэлектронных помех и/или создания искусственных ионизированных образований [248].

Изменение условий отражения электромагнитных (акустических) волн заключается в изменении величины отражения электромагнитных (акустических) волн путем применения средств постановки пассивных преднамеренных радиоэлектронных помех и/или изменения контраста окружающей среды [248].

Поражение самонаводящимся на источники излучения оружием — радиоэлектронное поражение, заключающееся в уничтожении или повреждении элементов РЭС противника оружием с пассивной системой наведения по излучениям военной техники в диапазонах электромагнитных, оптических и акустических волн [248].

Функциональное радиоэлектронное поражение (ФРЭПр) — радиоэлектронное поражение, заключающееся в разрушении и/или повреждении элементов РЭС противника электромагнитным излучением или в искажении информации противника специальными программными средствами [248].

Поражение электромагнитным излучением — функциональное поражение РЭС противника, заключающееся в разрушении и/или повреждении его элементов средствами поражения электромагнитным излучением. Оно может проводиться путем использования однократных или многократных импульсных воздействий электромагнитными полями, приводящих к необратимым измене-

ниям электрофизических параметров в полупроводниковых или оптико-электронных элементах РЭС в результате их перегрева или пробоя [245, 248, 255].

Поражение специальными программными средствами (СПС) заключается в снижении эффективности функционирования или выводе из строя компонентов систем обработки информации РЭС противника, нарушении конфиденциальности, целостности и доступности информации путем применения специальных программных средств [248].

Радиоэлектронная защита (РЭЗ) — совокупность мероприятий и действий по устранению или ослаблению воздействия на свои РЭС средств радиоэлектронного поражения, защите от технических средств разведки противника и обеспечению электромагнитной совместимости своих РЭС [248].

Защита от средств радиоэлектронного поражения противника заключается в снижении эффективности воздействия на свои РЭС средств функционального поражения, средств РЭП и оружия, самонаводящегося на источники излучения [248].

Радиоэлектронная защита от технической разведки противника заключается в исключении или существенном затруднении добывания противником с помощью технических средств разведки охраняемых сведений о РЭС. Радиоэлектронная защита от технических средств разведки противника ставит целью устранение разведывательных признаков по первичным и вторичным полям военных объектов, защите передаваемой, обрабатываемой и хранимой информации. Важное значение в обеспечении радиоэлектронной защиты от технических средств разведки противника имеет комплексный технический контроль защищаемых объектов [248].

Радиоэлектронно-информационное обеспечение — совокупность мероприятий и действий по выявлению функционирования РЭС противника в целях их радиоэлектронного поражения и контролю функционирования своих РЭС в целях их радиоэлектронной защиты [248].

Комплексный технический контроль мероприятий радиоэлектронной защиты заключается в следующем [248]:

- оценке защищенности своих РЭС от технических средств разведки противника;
- защите охраняемых сведений о своих РЭС, средствах, комплексах и системах;
- обеспечении электромагнитной совместимости своих РЭС.

Организационно в радиоэлектронно-информационное обеспечение также включается **контроль комплексной защиты информации**, задачами которого являются [248]:

- выявление демаскирующих признаков в деятельности войск в ходе боевого применения и использования вооружения, военной техники и военных объектов;
- оперативное пресечение нарушений установленных норм и требований по противодействию разведкам.

Информационная работа органов управления РЭБ заключается в сборе, накоплении, анализе, обобщении, хранении и распределении данных о РЭС

противника и своих РЭС, добываемых техническими средствами разведки, и в комплексном техническом контроле мероприятий радиоэлектронной защиты. Эти данные поступают от средств радиоэлектронной разведки, для чего соответственно оборудованные наземные станции, корабли, самолеты и космические аппараты перехватывают сигналы РЭС и определяют параметры радиосигналов. Кроме того, для получения этой информации могут использоваться шпионаж, аварии военных самолетов, экспорт военной техники, а в военное время — захват РЭС противника [248].

2.1.3. Совершенствование структуры подразделений сил РЭБ в условиях перехода к концепции сетецентрических войн (на примере ВС США)

Постоянное повышение требований к системам разведки и РЭБ, а также появление новой концепции сетецентрической войны стало основой революционного развития РЭБ в конце XX — начале XXI века. Это привело к изменению характера радиоэлектронной борьбы, ее содержания, состава сил и средств, роли, места, цели и задач в операциях. Эти факторы предопределили создание новых средств РЭБ, в том числе скрытного радиоэлектронного подавления, летального и нелетального оружия и средств борьбы с другими видами излучения направленной энергии, средств подавления и поражения, действующих на новых физических принципах, а также информационно-технических воздействий, предназначенных для атаки на компьютерные сети [95].

К настоящему времени аналитиками Пентагона отмечается, что в современных условиях именно радиоэлектронная борьба является основой информационной войны на военном уровне, а развитие теории «информационных операций» является базой для ведения такой войны [95].

Ключевые концепции строительства сухопутных войск США XXI века нового типа и задачи РЭБ по подавлению систем боевого управления противника определены рядом основных документов КНШ 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 2-0, FM 3-0, FM 2-19.301/ST, FM 2-19.401/ST, PM2-40.1/8T и др.

Способы, методы и приемы ведения РЭБ, 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 ВС и органах их управления;
- создаются единые структурно-упорядоченные системы РЭБ соединений и объединений во всех видах ВС, а в перспективе — в масштабе видов;

- развернут обширный круг научно-исследовательских и опытно-конструкторских работ по созданию новых средств РЭБ, а также по 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 РЭБ в операциях 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 по комплексному противодействию техническим средствам разведки противника, огневому и ядерному поражению его РЭС и их захвату диверсионными силами [95].

Мероприятия РЭБ составляют основу активно внедряемой в ВС США концепции «Борьбы 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 радиоэлектронных атак и радиоэлектронной защиты, согласование действий со штабами формирований других видов ВС, разрешение конфликтных ситуаций при использовании радиоэлектронных систем и средств возлагаются на управление (отдел) боевого управления, связи и автоматизации [95].

Все мероприятия РЭБ в информационной операции 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 [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, шт. Виргиния. Общая численность командования к началу 2011 г. составляла приблизительно 12 500 человек личного состава, из них около 3000 — гражданские специалисты [95].

На командование INSCOM 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 ВС вероятных противников для руководства сухопутных войск, оказанием технического содействия и оперативной помощи командованиям 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 РЭБ, была разработана новая доктринальная концепция разведывательного обеспечения операций для ВС США XXI века — Intelligence XXI Concept.

В ней определены основные принципы ведения разведки и РЭБ в операциях сухопутных войск [95]:

- непрерывное руководство организацией и ведением разведки и РЭБ 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 сил РЭБ;

- обеспечение подготовки и проведения информационных операций сухопутных войск и объединенных сил США.

Как показано в работах [258–261], основным воинским формированием, которое решает задачи радиоразведки (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 и 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.

2.1.3.1. Рота РЭБ сухопутных войск США

Рота РЭБ предназначена для ведения воздушной и наземной радиоразведки и создания помех радиосетям (радионаправлениям) тактического звена управления. (Предназначение выделяемых сил и средств из состава батальона разведки и РЭБ дивизии США аналогичное) [258, 259].

В составе роты РЭБ отдельной бригады имеются три взвода [258, 259].

1. Вертолетный взвод, на вооружении которого находятся два вертолетных комплекса РЭП Quick Fix II, включающие 2 станции РЭП для подавления радиосетей (радионаправлений) КВ- и УКВ-диапазонов. Носитель — вертолет ЕН-1Н или ЕН-60А.

2. Взвод радиоразведки (радиоперехвата). На вооружении этого взвода находятся:

- 3 наземные станции радиоразведки AN/TRQ (КВ- и УКВ-диапазонов), включающие 6 постов радиоперехвата (3 — КВ и 3 — УКВ) и 1 пеленгаторную сеть (3 поста). Размещаются станции на 1,25-тонных автомобилях с прицепами;
- 3 носимые станции радиоразведки AN/TRQ (КВ- и УКВ-диапазонов), включающие 6 постов радиоперехвата (3 — КВ и 3 — УКВ).

3. Взвод радиоподавления. На вооружении находятся:

- 2 наземных комплекса радиоэлектронного подавления УКВ-диапазона TACJAM, каждый из которых имеет по 3 передатчика помех. Размещаются на 2 гусеничных БТР М548;
- наземный комплекс радиоэлектронного подавления в КВ- и УКВ-диапазонах Traffic Jam, имеющий один передатчик помех (КВ- или УКВ-диапазона). Размещается на автомобиле с одноосным прицепом.

Таким образом, рота РЭБ имеет возможности развернуть [258, 259]:

- 12 постов радиоперехвата;
- 3 пеленгаторных поста (1 пеленгаторную сеть);
- 9 передатчиков помех.

Эти средства позволяют вести периодическое наблюдение за 35–50 радиосетями (радионаправлениями), определить в течение часа местоположение

60–80 радиостанций, создать помехи 1 КВ и 8 УКВ радиосетям (радионаправлениям).

Усиление роты РЭБ [258, 259]:

- 1 вертолетный комплекс РЭП Quick Fix II;
- 1+2 наземных комплекса РЭП Traffic Jam;
- комплект забрасываемых передатчиков помех.

Время вскрытия системы связи составляет 2–3 ч.

Боевой порядок сил и средств роты РЭБ в полосе действия мотострелкового (танкового) полка строится в один эшелон. Вертолетные комплексы ведут разведку и подавление с высоты 60–180 м на удалении 4–8 км от линии соприкосновения войск. Дальность подавления — до 40 км [258, 259].

Наземные станции радиоразведки развертываются в полосе 10–15 км на удалении 4–6 км от линии соприкосновения войск и обеспечивают пеленгование радиостанций на глубину до 25 км [258, 259].

Станции помех комплексов TACJAM и Traffic Jam развертываются в 3–4 км от линии соприкосновения войск и обеспечивают подавление радиосетей (радионаправлений) на глубину до 25 км [258, 259].

Носимые станции радиоразведки развертываются на удалении до 1,5–2 км от линии соприкосновения войск и ведут радиоразведку на глубину до 5–7 км [258, 259].

2.1.3.2. Батальон РЭБ сухопутных войск США

Батальон РЭБ состоит из штаба и четырех рот [258, 259]:

- оперативно-штабной;
- сбора данных и радиоэлектронного подавления;
- разведки и наблюдения;
- обслуживания.

В тяжелой дивизии США батальон разведки и РЭБ состоит из рот [258, 259]:

- штабной и оперативной маскировки;
- радиоэлектронной борьбы;
- радиоразведки и контроля;
- обслуживания.

Оперативно-штабная рота обеспечивает управление силами и средствами разведки и РЭБ дивизий с центром управления боевыми действиями. Для этого рота выделяет в состав секции РЭБ штаба дивизий силы и средства, занимающиеся планированием РЭБ в боевых действиях, обработкой разведывательной информации, управлением и контролем. Кроме того, из состава роты выделяются силы и средства в состав центра технического анализа и контроля штаба дивизии. Его личный состав по указанию начальников оперативного и разведывательного отделений штаба дивизии разрабатывает задачи подразделениям батальона, обеспечивает контроль за действиями средств разведки и РЭП и нацеливает их на выполнение поставленных задач. Группа контроля безопасности связи роты кроме своего прямого назначения может использоваться для разра-

ботки и проведения по указанию оперативного отделения штаба дивизии мероприятий оперативной маскировки [258, 259].

Рота сбора данных и радиоэлектронного подавления служит для выявления и подавления помехами РЛС и радиосвязи тактического звена на дальности 15–20 км. Ее взводы оснащены средствами радио-, радиотехнической разведки (РТР) и станциями радиопомех. В ее составе имеются [258, 259]:

- комплекс радиоразведки КВ/УКВ радиосвязи TSQ-114A;
- комплекс РТР типа MSQ-103A;
- по 3 наземных станции радиопомех УКВ радиосвязи MLQ-34, КВ/УКВ радиосвязи TLQ-7A и VLQ-4.

Кроме того, в составе роты может быть 3 вертолета EH-60A со станциями помех КВ/УКВ радиосвязи ALQ-151 Quick Fix II и станциями ALQ-143 предназначенными для радиотехнической разведки и постановки помех РЛС. Вертолеты EH-60A имеются также в составе бригад армейской авиации. Так, в тяжелой дивизии США имеется 12 вертолетов РЭБ EH-60A [258, 259].

Комплекс радиоразведки и управления TSQ-114, состоящий из 4 постов радиоперехвата (по 2 радиоприемных устройства в каждом), обеспечивает радиоперехват передач средств КВ/УКВ-радиосвязи в диапазоне 0,5–150 МГц и пеленгование 6–12 радиостанций в минуту в диапазоне 20–80 МГц. Система MSQ-103 Team Pack позволяет за час работы определить местоположение 6–9 РЛС в диапазоне 0,5–40 ГГц [258, 259].

Мобильные станции радиопомех TLQ-17A, MLQ-34 и VLQ-4 и вертолетный комплекс ALQ-151 Quick Fix II предназначены для выявления и подавления КВ/УКВ радиосвязи с амплитудой и частотной модуляцией; комплекс ALQ-143 — для создания помех РЛС войсковой ПВО и наземной артиллерии [258, 259].

Комплекс радиопомех TLQ-17A обеспечивает поиск и подавление КВ/УКВ-радиосвязи дивизий в диапазоне 1,5–80 МГц. Еге приемник (всего в комплексе их 12) при создании помех настраивается на частоту подавляемой станции. Работой передатчика радиопомех управляет микро-ЭВМ. Аппаратура комплекса может размещаться в автомобиле грузоподъемностью 1,25 т с прицепом, или в БТР М-113, или на вертолете EH-1H [258, 259].

Станция радиопомех MLQ-34, установленная на БТР М-113 и прицепе, предназначается для подавления КВ/УКВ-радиосвязи тактического звена в диапазоне 20–150 МГц. Одна станция может подавлять до 3 радиосвязей (радиосетей и радионаправлений) [258, 259].

Вертолетный комплекс ALQ-151 Quick Fix II, действуя совместно с наземной системой радиоразведки и управления TSQ-114, может создавать помехи КВ/УКВ радиосвязи в диапазоне 2–76 МГц на дальности до 60 км. В состав комплекса входят приемопеленгаторная станция и бортовой вариант наземной мобильной станции помех TLQ-17A. Комплекс ALQ-143 позволяет выявлять и подавлять одновременно 4–6 РЛС войсковой ПВО и наземной артиллерии на дальности до 40 км [258, 259].

Всего рота сбора данных и РЭП может развернуть 12 постов радиоперехвата (по 6 для КВ- и УКВ-диапазонов), 6 радиопеленгаторных постов

(по 3 для КВ- и УКВ-диапазонов), 3 поста радиотехнической разведки, 15 комплексов радиопомех КВ/УКВ радиосвязи и наземным РЛС. Этими средствами рота может вести периодическое наблюдение за 24–36 радиосетями, создавать помехи 12 КВ и УКВ радиосетям, 6 РЛС, а также определять характеристики и местоположение 5–10 РЛС на дальности 30 км с точностью 50 м. Взвод радио- и радиотехнической разведки обеспечивает выявление и радиопеленгование средств радиосвязи, а также анализ радиосигналов [258, 259].

Таким образом, технические средства разведки и РЭБ сухопутных войск США обеспечивают ведение радиоразведки и радиоподавления тактической и оперативно-тактической связи в УКВ-диапазонах 1,5–500 МГц и 20–80 МГц соответственно. К наиболее распространенным средствам подавления в этом звене относятся [258, 259]:

- вертолетный комплекс AN/ALQ-151(V)2 Quick Fix II;
- наземная станция AN/TLQ-17A(V)1 Traffic Jam.

Также опыт и практика войск показывают, что на вооружении сухопутных войск США имеются технические средства разведки и постановки помех радиорелейной, тропосферной и космической связи.

2.1.4. Типовой сценарий использования сил и средств РЭБ в сетецентрической войне

На примере операций многонациональных сил в зоне Персидского залива в 1991 и в 2003 гг. рассмотрим, насколько была важна радиоэлектронная борьба 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. 2.3 и 2.4 представлены схемы постановки помех с началом воздушной и воздушно-наземной операций многонациональных сил.

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 защиты 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].

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].

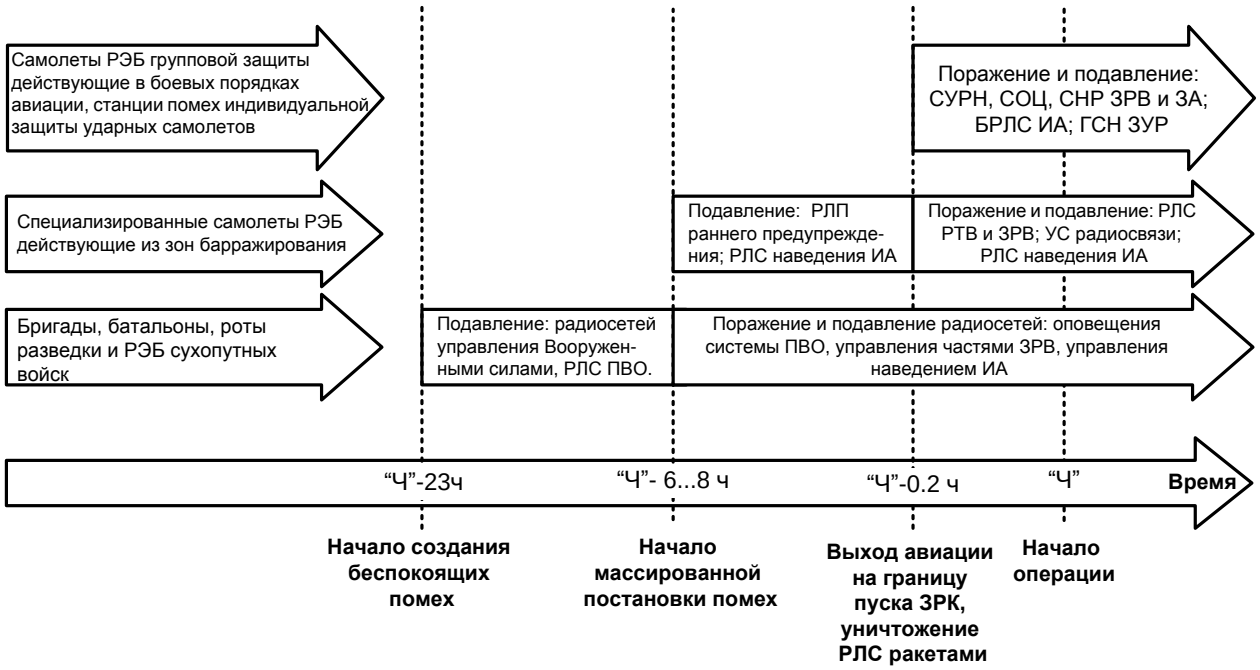


Рис. 2.3. Сценарий применения РЭБ с началом воздушной операции в сетецентрической войне [250]

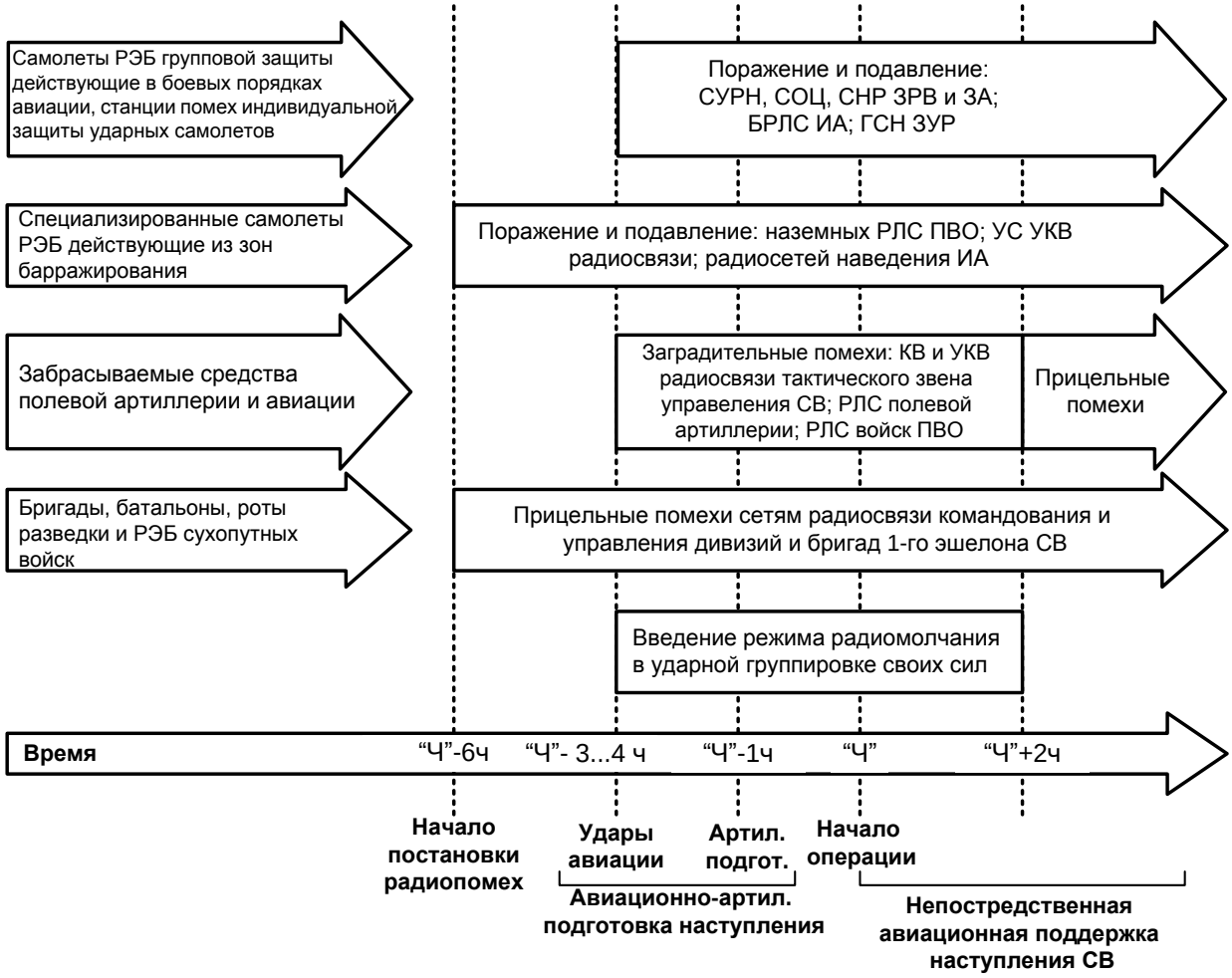


Рис. 2.4. Сценарий применения РЭБ с началом воздушно-наземной операции в сетецентрической войне [250]

Кроме того, в военных операциях широко применялись беспилотные летательные аппараты (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 30–11 000 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].

На рис. 2.5 показано распределение по рабочим частотам средств связи, навигации и некоторых других систем. Из номограммы видно, что наибольшее количество средств связи и навигации сосредоточено в диапазоне частот от 2 до 1215 МГц [250].

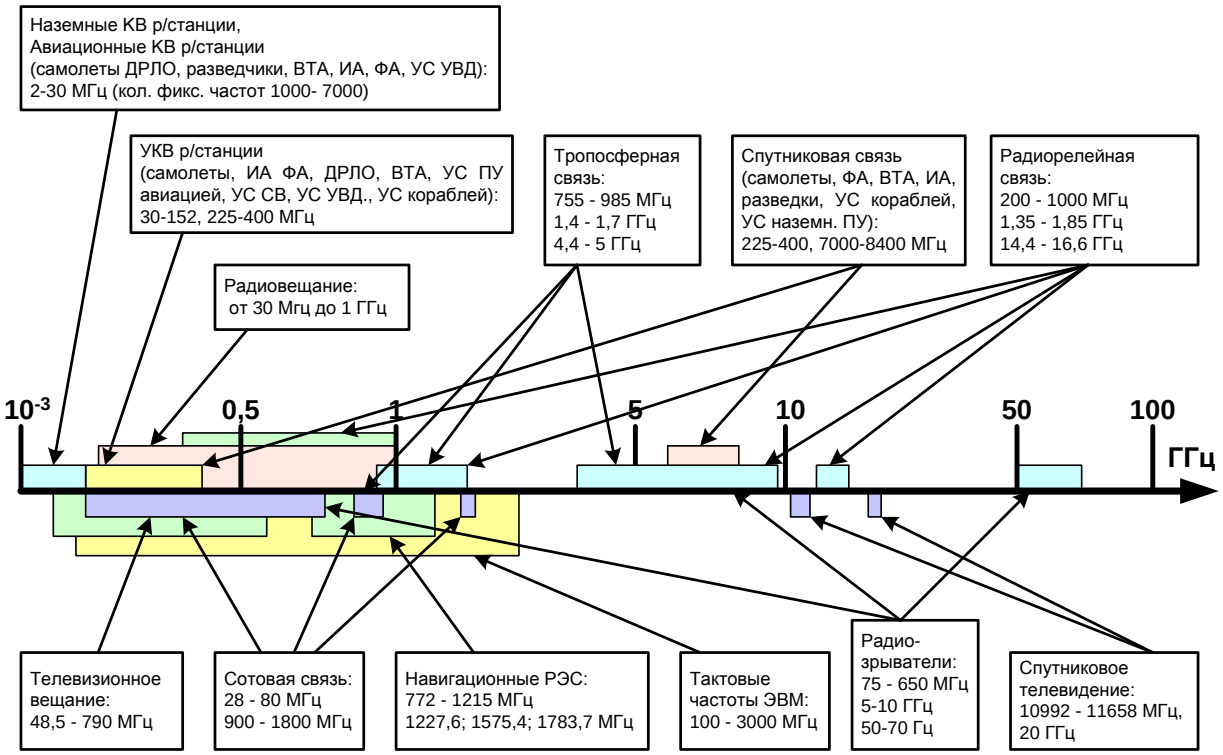


Рис. 2.5. Распределение по рабочим частотам средств связи, навигации и некоторых других систем [250]

На рис. 2.6 показано распределение по рабочим частотам радиолокационных средств наземного и морского базирования. Из номограммы следует, что РЛС обнаружения сосредоточены в основном в диапазоне частот 2–6 ГГц, а РЛС управления оружием — в диапазоне частот 8–12 ГГц [250].

На рис. 2.7 показано распределение по рабочим частотам средств радиолокации, размещаемых на летательных аппаратах различного назначения. Из номограммы видно, что наибольшая плотность РЛС этого класса приходится на частотный диапазон от 8 до 12 ГГц [250].

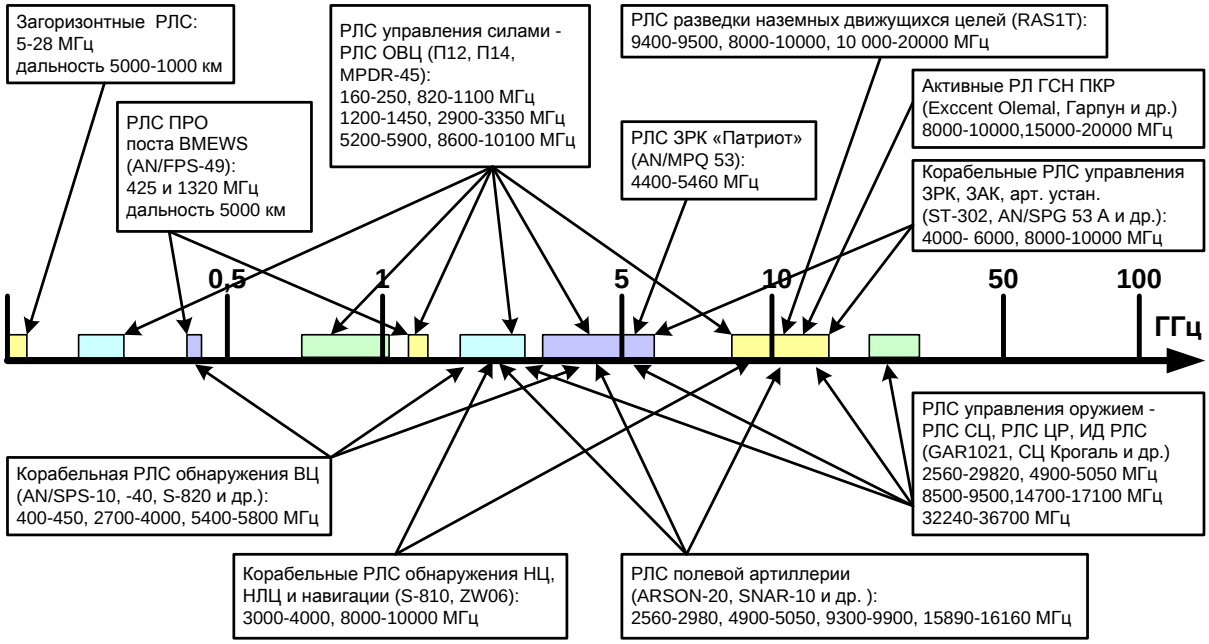


Рис. 2.6. Распределение по рабочим частотам РЛС наземного и морского базирования [250]

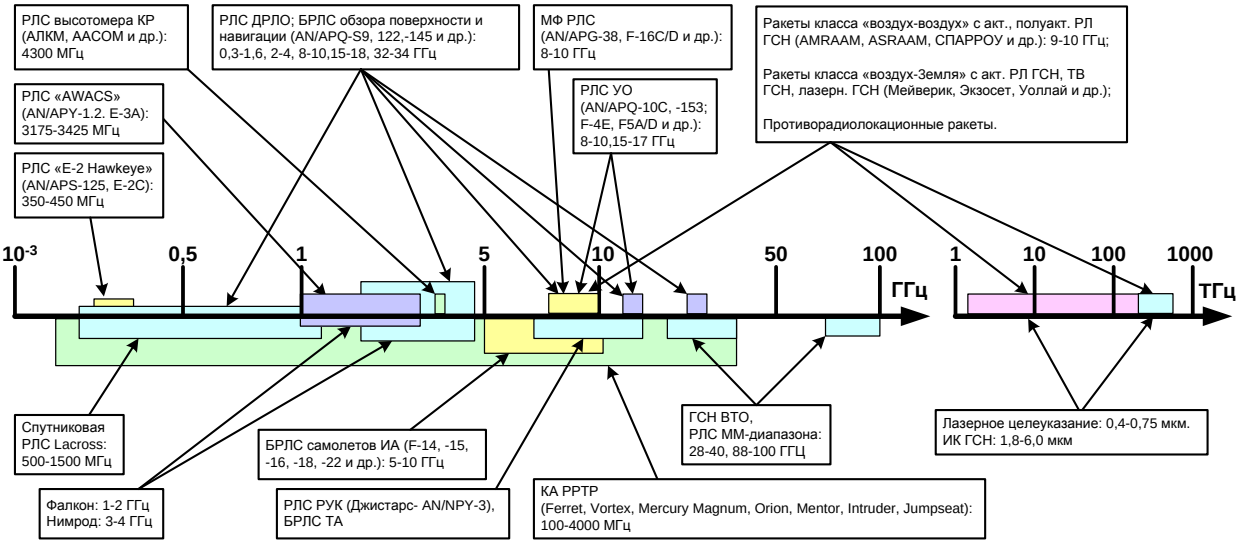


Рис. 2.7. Распределение по рабочим частотам средств радиолокации, размещаемых на летательных аппаратах различного назначения [250]

В соответствии с данными, приведенными на рисунках, для решения задач подавления этих систем выбирались средства РЭБ, обеспечивающие воз-

действие в данных диапазонах. Наиболее часто используемыми средствами РЭБ в последних конфликтах являлись [250]:

- ALR-46 — аппаратура радио- и радиотехнической разведки;
- ALQ-131 — станции активных помех;
- ALE-40 — станция пассивных помех;
- AAR-46 — ИК-аппаратура разведки;
- ALQ-132 — станция оптико-электронного подавления;
- AGM-88 HARM — противорадиолокационная ракета.

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].

2.2. Радиоэлектронное подавление радиолокационных станций систем управления оружием и комплексов ПВО

2.2.1. Системы управления оружием как объекты подавления

В современных сетецентрических войнах радиоэлектронная борьба активно ведется всеми видами ВС, но наиболее интенсивно эти средства задействовываются в интересах ВВС и ПВО. Так, в США до 70% материальных ресурсов, предназначенных для развития и совершенствования систем РЭБ, поступают именно в авиацию. В ходе ряда конфликтов («Буря в пустыне», «Лиса в пустыне», «Шок и трепет», «Рассвет Одиссей») средства РЭБ решали следующие задачи [248]:

- дезорганизация системы государственного и военного управления стран и их ВС;
- деморализация армии и народа;
- нанесение существенного ущерба военно-экономическому потенциалу стран и разрушение их инфраструктуры;
- нанесение значительного урона группировкам ВС и создание условий для гарантированного успеха планируемых операций наземных сил с минимальными потерями.

Опыт локальных войн свидетельствует: вкладывать деньги в развитие средств РЭБ является экономически целесообразным. Анализ показывает, что стоимость техники РЭБ по отношению к стоимости основных видов вооружения составляет 5–8%. При этом в локальных войнах и вооруженных конфликтах были весьма наглядно продемонстрированы роль и значимость РЭБ, когда ее умелое применение приводило к повышению боевого потенциала группировок войск в 1,5 раза и позволяло снизить потери кораблей в 2–3 раза, а авиации — в 4–6 раз [245, 248].

В качестве объектов воздействия средств РЭБ могут рассматриваться различные системы управления силами, войсками и оружием, и прежде всего — входящие в них отдельные РЭС добывания, передачи и обработки информации, а также энергетические системы. В качестве РЭС добывания информации выступают активные и пассивные радио-, оптико-электронные комплексы, станции и устройства. Средства передачи информации как объекты РЭБ — это средства радио-, оптической и кабельной связи. К системам и средствам обработки информации как объектам РЭБ относятся различные электронно-вычислительные сети и устройства: глобальные и локальные вычислительные сети, вычислительные центры, боевые информационно-управляющие системы, отдельные ЭВМ, микропроцессорные устройства. Всем этим системам и средствам свойственны свои сильные и слабые стороны, которые необходимо учитывать при решении задач РЭБ.

К факторам, обуславливающим сильные стороны систем управления оружием, относятся [247, 248]:

- возможность ведения радиоэлектронной и оптической разведки в широком диапазоне с использованием разветвленной сети космических, воздушных, корабельных, наземных подвижных и стационарных сил разведки;
- применение развитой системы космической и наземной связи с высокими показателями оперативности и достоверности передачи информации, значительное резервирование узлов и линий связи;
- широкое использование средств автоматизации при обработке информации и выработке управляющих решений.

Слабыми сторонами систем управления оружием являются [247, 248]:

- уязвимость РЭС от преднамеренных помех и поражающих воздействий;
- высокая наблюдаемость излучений РЭС средствами радиоэлектронной разведки;
- зависимость эффективности комплексов вооружения от успешности функционирования систем разведки, навигации и связи, которые являются недостаточно защищенными от средств поражения и РЭБ.

При организации РЭП на системы управления оружием необходимо учитывать, что РЭС, входящим в состав систем управления, как правило, присущи следующие функции [247]:

- поиск и обнаружение целей;
- опознавание государственной принадлежности «свой — чужой»;

- передача по линии связи информации об обстановке в зоне ответственности и обработка этой информации;
- выработка команд управления и передача их по линиям связи;
- целеуказание, наведение оружия и его применение по цели.

В связи с этим основные усилия при организации радиоэлектронного подавления систем управления оружием, как правило, направлены на [247]:

- ухудшение радиолокационной видимости цели с помощью радиопоглощающих материалов и других мер, снижающих эффективную площадь отражения цели;
- ухудшение условий радиолокационной видимости цели путем создания маскирующих активных или пассивных помех;
- дезинформацию системы опознавания государственной принадлежности цели путем создания ей имитационных помех;
- нарушение работы каналов передачи информации и команд управления путем создания им активных помех;
- перегрузку датчиков систем управления оружием ложными целями с помощью имитационных помех;
- создание ошибок в наведении и ложные срабатывания оружия.

2.2.2. Подавление радиолокационных станций систем управления оружием

В боевых условиях эффективность систем управления оружием различного назначения в значительной степени зависит от успешного функционирования РЛС, позволяющих обнаруживать и распознавать различные объекты (цели), определять их координаты, параметры движения и другие данные методами радиолокации [247].

Как показывает анализ типовых сценариев применения средств РЭБ в военном конфликте, основная часть усилий сосредотачивается на подавлении системы ПВО противника. Таким образом, наиболее актуальной тематикой подавления систем управления оружием является подавление РЛС систем ПВО.

При этом сами РЛС систем ПВО постоянно совершенствуются, что также обусловлено развитием средств воздушного нападения в направлении [248]:

- снижения радиолокационной заметности летательных аппаратов (ЛА);
- повышения маневренности и расширения диапазона скоростей и высот полета, создание мини и микро-ЛА;
- рост возможностей средств РЭП и средств ракетно-бомбового поражения РЛС.

Основными направлениями развития перспективных РЛС являются [248]:

- расширение перечня задач, решаемых РЛС в комплексах вооружения в интеграции их с подсистемами разведки, подавления и навигации для решения задач по предназначению;
- увеличение дальности обнаружения и числа одновременно сопровождаемых целей;
- повышение точности измерения координат и разрешающей способности;

- адаптивный обзор требуемой зоны с заданными параметрами;
- автоматическое распознавание класса и типа цели;
- повышение скрытности излучения за счет использования различных диапазонов электромагнитных волн (3 мм, 8 мм) и сверхширокополосных сигналов, управления мощностью излучения и изменения формы диаграммы направленности антенны;
- групповое применение бистатических систем радиолокации, работа в условиях встречного излучения РЛС противника и помех, обеспечение электромагнитной совместимости.

Реализация указанных направлений будет обеспечиваться за счет [248]:

- применения твердотельных активных фазированных антенных решеток (АФАР) с программным электронным сканированием луча и цифровым преобразованием сигналов в элементах решетки;
- реализации оптимальных (квазиоптимальных) адаптивных алгоритмов цифровой обработки радиолокационной информации в условиях РЭП;
- использования в многофункциональных РЛС режимов навигации, опознавания, наведения оружия и обмена информацией;
- перехода к наземным и авиационным многопозиционным РЛС и системам пассивного и активно-пассивного типа, совместно ведущим радиолокационное сопровождение цели.

Многочисленные попытки совершенствования РЛС на базе традиционной радиолокации наталкиваются на проблемы принципиального характера. Выходом из создавшегося положения является развитие двух принципиально новых радиолокационных технологий [248]:

- MIMO (Multiple Input — Multiple Output («много входов — много выходов») — радиолокационная технология, основанная на многопозиционной радиолокации, а также получении и совместной апостериорной обработке результатов измерений;
- САОРИ — технология радиолокационных систем с апостериорной обработкой результатов измерений (JAPRM technology).

Возможность нарушения работоспособности большинства РЛС является прямым следствием принципа их работы, заключающегося в излучении радиосигналов в пространство и приеме отраженных от объектов сигналов. Излучение сигналов не только демаскирует РЛС и позволяет обнаружить ее местоположение, но и дает возможность определить основные характеристики режима ее работы: рабочую частоту, вид излучения, поляризацию сигнала, вид и параметры модуляции сигнала (АМ, ЧМ, ФМ, ФКМ), ширину спектра, длительность импульса, частоту следования импульсов, излучаемую мощность [248].

Измеренные характеристики дают возможность определить тип облучающей защищаемый объект РЛС, сформировать помеховый сигнал в соответствии с предусмотренным заранее алгоритмом и нарушить нормальную работу РЛС. При этом непосредственная задача РЭП может заключаться в создании условий, при которых отраженный от объекта сигнал будет замаскирован более мощным помеховым сигналом, в результате чего исключается возможность извлечения из него полезной информации, необходимой для системы ПВО, или

создаются сигналы, несущие ложную информацию об объектах и воздушной обстановке в целом. В результате этого в системе ПВО могут вырабатываться неверные решения, снижающие эффективность ее работы [247].

Различные виды помех вызывают в РЛС входящих в состав систем управления оружием следующие эффекты [247]:

- нарушение процесса обнаружения (пропуск цели);
- дезориентацию оператора РЛС или комплекса вооружения;
- задержку обнаружения или задержку начала автосопровождения цели;
- сопровождение ложной цели или перегрузку систем обработки информации их большим количеством;
- нарушение способности измерения радиолокационными средствами дальности, скорости и направления цели;
- создание ошибок в измерении дальности, скорости и направления цели;
- срыв автосопровождения цели или ракеты.

Современные РЛС решают широкий круг задач, связанных с обнаружением целей, определением их местоположения в пространстве и оценкой параметров их движения. Помеховое воздействие на РЛС требует знания конкретных функциональных характеристик ее аппаратуры, а также принципов решения возложенных на комплекс вооружения задач. Наибольшего эффекта радиоэлектронное подавление достигает тогда, когда оно организуется целенаправленно с учетом индивидуальных особенностей подавляемой аппаратуры [247].

Методы создания помехи могут быть самыми различными и определяться типом подавляемых РЛС. В РЛС обнаружения и сопровождения, а также в РЛС управления оружием канал автоматического сопровождения по направлению является основным, так как именно там производятся угловая селекция и измерение угловых координат. По этим каналам обычно ставится организованная помеха для того, чтобы сорвать сопровождение цели по угловым координатам [247].

К основным видам помех, ориентированных на РЛС, относятся [247].

1. Универсальные помехи:
   - шумовая помеха;
   - когерентная помеха;
   - поляризационная помеха;
   - мерцающая помеха;
   - прерывистая помеха;
   - перенацеливающая помеха;
   - помеха с вынесенной точки пространства.
2. Помехи, зависящие от принципа работы подавляемой РЛС:
   - помеха, ориентированная на угломерные РЛС;
   - помеха, ориентированная на РЛС с коническим сканирующим лучом;
   - заградительная по частоте сканирования помеха, модулированная по амплитуде сеткой частот;

- комбинированная помеха по угломерному каналу со скрытым коническим сканированием лучом и по каналу скорости;
- помеха полуактивным доплеровским головкам самонаведения с коническим сканированием лучом;
- адаптивная помеха, ориентированная на подавление РЛС сопровождения.

При этом надо учитывать, что в современных РЛС для противодействия помехам используются следующие способы помехозащиты [248]:

- перестройка несущей частоты от импульса к импульсу в широкой полосе частот по случайному закону;
- моноимпульсный метод измерения угловых координат целей и угловое стробирование отметок;
- применение простых и сложных импульсных зондирующих сигналов, период повторения и длительность которых могут изменяться в широких пределах;
- управление параметрами обзора (временем облучения цели, частотой обращения к цели, периодом просмотра сектора поиска и др.) в соответствии с быстро изменяющейся тактической и радиоэлектронной обстановкой;
- компенсация и бланкирование помех, принимаемых по боковым лепесткам диаграммы направленности;
- селекция движущихся целей на фоне естественных и искусственных пассивных помех;
- применение специальных режимов — пеленгация (пассивное сопровождение), сопровождение по переднему фронту импульса, силовое преодоление преднамеренных помех;
- применение оптимальных и квазиоптимальных алгоритмов обнаружения и селекции целей;
- фильтрация параметров траекторий и управление полетом управляемых ракет;
- структурная адаптация многопозиционной радиолокационной системы, использование ложных излучений;
- различные модификации автоматической регулировки усиления и стабилизация уровней ложных тревог.

2.3. Радиоэлектронное подавление систем управления, связи и навигации

2.3.1. Системы связи как объекты разведки и подавления

Для определения параметров систем связи в различных диапазонах в интересах их подавления используются средства радиоразведки. Основным источником информации для систем радиоразведки сигналов являются самолеты, корабли, наземные станции связи управления сухопутными войсками, а также спутниковые системы связи [250].

Используемые частоты в системах связи распределяются следующим образом [250]:

- 3–30 Гц (КНЧ-диапазон), 30–300 Гц (СНЧ-диапазон) — связь с подводными лодками на большой глубине;
- 0,3–3 кГц (УНЧ-диапазон), 3–30 кГц (ОНЧ-диапазон) — связь с подводными лодками;
- 30–300 кГц (НЧ-диапазон) — связь с использованием отражения от атмосферы (связь в условиях ведения ядерной войны);
- 0,3–3 МГц (СЧ-диапазон) — стратегическая дальняя связь;
- 3–30 МГц (ВЧ-диапазон) — загоризонтная тактическая связь (самолеты, корабли, наземные средства);
- 30–300 МГц (ОВЧ-диапазон) — связь «земля-воздух» и связь в пределах прямой видимости (корабли, самолеты, наземные средства);
- 0,3–3 ГГц (УВЧ-диапазон) — спутниковая и тактическая связь «земля — воздух», бортовая связь самолетов;
- 3–30 ГГц (СВЧ-диапазон), 30–300 ГГц (КВЧ-диапазон) — спутниковые системы связи;
- 0,4–0,75 мкм (видимая часть спектра электромагнитных волн) — лазерные системы связи, связь с подводными лодками в голубой и зеленой частях спектра видимого света.

Радиосвязь в КВ (3–30 МГц) и в нижней части ОВЧ (30–52 МГц) диапазонов по основным показателям (помехозащищенность, надежность) приближается к спутниковым системам связи. Основным направлением ее совершенствования является развитие автоматизированных адаптивных средств связи, способных работать в помехозащищенном режиме [250].

УКВ радиосвязь (в основном используется диапазон 225–400 МГц) активно используется в тактических звеньях управления авиации, кораблей и наземных формирований, о чём свидетельствуют данные радиоразведки при ведении военных действий [250].

При этом дециметровый, сантиметровый и особенно миллиметровый диапазоны волн позволяют аппаратуре связи работать в очень широкой полосе частот, с большой эффективной излучаемой мощностью при небольших размерах антенн [250].

Для выбора типа и диапазона постановки помех средствам РЭП необходимо выдать целеуказание по характеристикам подавляемых РЭС средств связи. Для этого используются средства радио- и радиотехнической разведки.

Основными функциями системы разведки являются [250]:

- непрерывное сканирование диапазона частот;
- дискретное сканирование полосы частот;
- комбинированное сканирование.

Различные диапазоны систем связи характеризуются следующими параметрами, значимыми для средств разведки [250]:

- приоритет;
- скорость сканирования;

- порог обнаружения;
- исключение сигналов, не представляющих интереса.

Вероятность обнаружения РЭС систем связи зависит от скорости сканирования относительно длительности принимаемых сигналов. Например, при продолжительности связи в УКВ-диапазоне, равной нескольким секундам, скорость сканирования, равная 20–50 МГц/с, будет приемлемой [250].

Чувствительность приемных разведывательных устройств в КВ- и УКВ-диапазонах с широкополосными антеннами лежит в пределах 0,5–5 мкВ/м, а разрешающая способность по частоте находится в пределах 20–30 кГц [250].

Сложнее обстоит дело с перехватом сигналов средств связи, которые используют режимы псевдослучайной перестройки рабочей частоты. В этом случае необходимо установить программу, по которой изменяется частота разведываемой связной станции, что является непростой задачей. При этом, как правило, содержание передачи таких средств связи не поддается анализу [120, 250].

Существующие системы связи в большинстве своем являются цифровыми. Для перехвата таких сигналов необходимо иметь полностью цифровое приемное устройство, работающее в режиме радиомониторинга. Современные цифровые приемные устройства, работающие в режиме радиомониторинга в диапазоне частот 1,5–30 МГц, имеют чувствительность 184 дБВт/Гц, динамический диапазон не менее 80 дБ, скорость поиска по частоте 3–50 ГГц/с, разрешение по частоте от 100 Гц до 5 кГц. Они способны вести разведку сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ), сигналов со сжатием, со всеми видами модуляции и кодирования [250].

Дальность разведки для средств связи определяется их типом и используемым диапазоном [250]:

- для средств КВ — 3000 км;
- для средств УКВ — 200 км (при наличии прямой видимости);
- для средств РТР — 100 км для наземных целей, до 300 км для воздушных целей.

Разведка сигналов спутниковой связи представляет собой технически сложную задачу, так как при применении на космическом аппарате (КА) узконаправленных антенн с диаграммой направленности 1° и менее (что возможно в миллиметровом и оптическом диапазонах волн) обеспечивается высокая скрытность связи. При этом прием сигналов по боковым лепесткам диаграмм направленности спутниковой антенны требует высокой чувствительности приемника разведки — 140 дБ/Вт и выше [250].

Информация о разведанных целях в КВ- и УКВ-диапазонах поступает в систему местоопределения, где обеспечивается решение задачи определения местоположения РЭС связи по данным территориально-распределенной сети средств разведки. Современные комплексы радиоразведки и РЭП способны обнаружить несколько сотен источников излучения в КВ-диапазоне и более десятка тысяч источников излучения УКВ-диапазона и подавлять до сотни целей [250].

Станции активных помех в КВ- и УКВ-диапазонах способны поставлять различные типы помеховых сигналов: шум, меандр, ЛЧМ, псевдослучайный код, «электронную музыку». При этом ширина заградительных помех может составлять 5–100 МГц, ширина прицельной помехи — от 50 кГц до 100 МГц при выходной мощности передатчика не менее 1 кВт [250].

2.3.2. Помехозащищенность радиолиний отдельных родов связи

Для оценки помехоустойчивости систем радиосвязи общепринятым является использование так называемого коэффициента защиты ($К_З$) [224], представляющего собой минимально допустимое отношение сигнал/(шум+помеха) (ОСШП), на входе приемника, при котором еще обеспечивается требуемое качество связи (заданная достоверность приема). Обычно значения $К_З$ представляются в виде нескольких сомножителей, учитывающих способы модуляции, быстрые и медленные замирания сигналов на трассах связи, виды помех и др. Реальные значения $К_З$ обычно находятся в рамках от 1 (слуховой прием) до 50–100 (качественная телефонная связь) [224].

Для оценки эффективности подавления (полного нарушения связи) обычно используют коэффициент подавления ($К_П$), представляющий собой минимально возможное значение отношения помеха/сигнал на входе приемника, при котором достигается полное нарушение связи. По аналогии с $К_З$ коэффициент подавления также может представляться в виде сомножителей, учитывающих виды информационных сигналов, типы помех, влияние быстрых и медленных замираний сигналов и помех на трассах связи и др. [224].

По физическому смыслу данные коэффициенты не являются взаимно обратными величинами ($К_З \neq 1/К_П$), поскольку значения $К_П$ соотносятся с воздействиями специально организованных (преднамеренных) помех и с полным прекращением связи.

Отмеченные коэффициенты характеризуют в основном технические характеристики самих приемных устройств с подключенными к их выходам абонентскими комплектами, рассчитанными на определенные виды информационных сигналов (телефония, передача данных и др.). Оценка качества приема здесь зависит только от отношения сигнал/шум (или помеха/сигнал) и не учитывает возможных дополнительных зависимостей от абсолютных значений самих сигналов (т. е. не учитывает энергетических параметров передающих устройств, параметров трасс связи, значений коэффициентов усиления антенн, их пространственной избирательности и др.). Иначе говоря, применение только таких коэффициентов не содержит необходимых данных о возможных свойствах помехозащищенности реальных линий радиосвязи (ЛРС) и их различий по данному показателю.

Для количественной оценки помехозащищенности радиолиний в реальных условиях их развертывания Е.Е. Исаковым в работе [224] было предложено использовать новый показатель — *реальную помехозащищенность*.

Реальную помехозащищенность соответствующего типа радиолинии (РРЛ, ТРЛ, ДКМ, МВ, ЛРС ССС и пр.) Е.Е. Исаков предлагает оценивать через максимально допустимые значения мощности помехи на входе ее приемного

устройства ($P_{\text{П ВХ}}$**)** для близкой к штатной (рис. 2.8) протяженности интервала радиосвязи, при которой в канале радиолинии происходит полное нарушение связи [224]:

$$P_{\text{П ВХ}} = P_{\text{С ВХ}} \cdot K_{\text{П}} \cdot K_{\text{З АНТ}}(\alpha),$$

где $P_{\text{П ВХ}}$ — соответствует мощности сигнала на входе приемника радиолинии для близкой к штатной протяженности ее интервала $P_{\text{С}}$ (км); $K_{\text{П}}$ — коэффициент подавления; $K_{\text{З АНТ}}$ — коэффициент защиты приемной антенны со стороны ее боковых и обратных лепестков ($K_{\text{З АНТ}} \approx 1$ для $\alpha \approx 0^\circ$, $K_{\text{З АНТ}} \geq 10–10^3$ для $\alpha \approx 90^\circ–180^\circ$).

Значения реальной помехозащищенности (рис. 2.8), согласно [224], зависят от мощности информационного сигнала в точке приема (от мощности передатчика, коэффициентов усиления приемной и передающей антенн, протяженности трассы связи и условий прохождения радиоволн), технических значений параметра $K_{\text{П}}$ и направлений прихода в точку приема радиопомех (от защитных свойств антенн). Как показано ниже, с применением данного показателя вполне возможными становятся различного рода энергетические (количественные) оценки при расчетах помехозащищенности реальных наземных радиолиний в условиях применения средств РЭП [224].

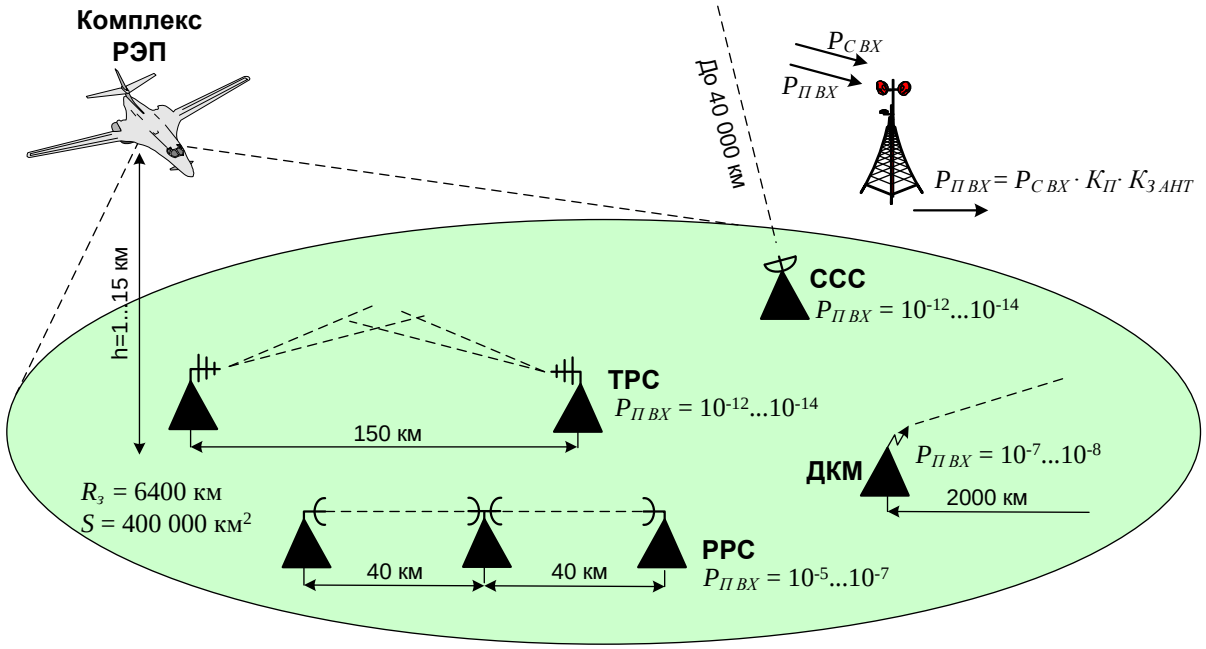


Рис. 2.8. Количественное определение реальной помехозащищенности $P_{\text{П ВХ}}$ для радиолиний различных типов [224]

Проведем оценку вероятных значений коэффициентов подавления линий связи. Для получения объективной количественной оценки необходимо проведение специальных лабораторных, полигонных и полевых испытаний, включая применение передатчиков помех на летно-подъемных средствах. Поскольку данные по результатам подобного рода испытаний в отечественной и в рассмотренной зарубежной литературе отсутствуют, то остается только один способ приближенной количественной оценки ожидаемых (вероятных) верхних (оптимистических) и нижних (пессимистических) значений $K_{\text{П}}$. Данный способ

состоит в использовании известных из теории связи значений «пороговой» мощности сигналов для получения «оптимистической» оценки $K_{П}$ и простейших аналитических соотношений для «пессимистической» оценки нижних граничных значений данного показателя [224].

Что касается оценки верхних значений $K_{П}$ для применяемых в составе сетей многоканальных радиолиний, то для случая шумовой помехи с мощностью $P_{П}=P_{Ш}$ «оптимистические» значения $K_{П}=P_{П}/P_{С\ порог}$ для приемных устройств многоканальных радиолиний реально будут иметь значения порядка 0,1–0,06 [224].

Известно, что заградительные шумовые помехи в энергетическом плане относятся к числу наименее эффективных. Более рациональными с точки зрения экономии выходной мощности передатчиков помех являются импульсные помехи (частотно-сканирующие, дискретно-сканирующие и т. п.), т. е. попадающие в каналы радиосвязи с определенной частотой повторения. Так, если принять во внимание типовые значения полосы каналов радиосвязи многоканальных наземных радиолиний ($\Delta f \approx 0{,}1$–1 МГц), то минимальные значения длительности попадающих в эту полосу частот импульсных помех (при их дискретном сканировании) составят: $\Delta t = 1/\Delta f$, или $\Delta t \approx 10^{-5}$–10^{-6} с [224].

Частота повторения n таких импульсов в канале радиосвязи при постоянном «обслуживании» передатчиком помех, например порядка $N = 100$ частот (что близко к частотному ресурсу значительной части существующих типов наземных радиолиний) может составить: $n=1/(N\cdot\Delta t)$ или $n = 10^{3}$-10^{4} имп. в секунду. При указанных значениях длительности импульсов помех (1–10 мкс) и частот их повторения неизбежно существенное снижение помехозащищенности основных видов многоканальной радиосвязи, вплоть до полной их потери. Вероятные значения коэффициента подавления $K_{П}=K_{П\ max}/N$ для данного примера могут составить значения 10^{-3}–10^{-4} [224].

Однако реальные значения подобных показателей для многоинтервальных радиолиний могут оказаться еще хуже. Связано это не только с процессами ретрансляции, суммирования и размножения помех и искажений, но и с возможным одновременным попаданием преднамеренных помех на несколько участков многоинтервальных линий. В этих случаях сама структура многоинтервальной линии служит дополнительным источником размножения помех на последующих ее участках. С увеличением числа подверженных интенсивным помехам участков многоинтервальной радиолинии или сети радиосвязи в целом процесс размножения таких помех может приобретать лавинообразный характер. Это означает, что для внешних заградительных помех многоинтервальные линии и сети радиосвязи становятся «многовходовыми». Это служит дополнительным источником для повышения эффективности воздействий преднамеренных радиопомех. Многовходовый характер проникновения заградительных помех оказывается особо опасным для сетей радиосвязи, имеющих в своем составе участки сети: с низкими уровнями полезных сигналов на стороне приема; с глубокими медленными замираниями; с полузакрытыми интервалами связи; с дополнительными затуханиями сигналов в передающих фидерных трактах, с неисправными передатчиками, с некачест-

венной юстировкой антенн и пр. В связи с этим вполне резонным может быть заключение, что с ростом структурной сложности и разветвленности сетей связи показатели их помехозащищенности неизбежно снижаются [224].

Таким образом, в качестве нижней границы («пессимистической») оценки значений $K_{\text{П}}$ можно принять значения от 10^{-3} до 10^{-4} [224].

Определение областей вероятных значений $K_{\text{П}}$ позволяет количественно определить значения реальной помехозащищенности основных типов радиолиний из состава сетей связи для условий системного РЭП. Эта количественная оценка на основе предложенного выше показателя «реальной помехозащищенности» радиолинии $P_{\text{П ВХ}}$ и с учетом ряда упрощающих предположений (проведение расчетов для номинальных значений выходной мощности передатчиков, наличия открытых трасс связи, табельной юстировки антенн, штатной протяженности интервалов связи и пр.) представлена в таблицах 2.1 и 2.2 [224].

В таблице 2.1 приведены оценки значений мощности информационных сигналов $P_{\text{С ВХ}}$ на выходе приемной антенны для основных типов линий радиосвязи военного назначения (радиорелейных, тропосферных, коротковолновых, спутниковых и пр.) в соответствии с расчетами, выполненными в работе [224].

Таблица 2.1 — Расчетные значения мощности информационных сигналов $P_{\text{С ВХ}}$ на выходе приемной антенны [224]

Тип радиолинии	Средняя полоса частот радиолинии f ср, ГГц	Мощность передатчика сигнала $P_{C\,ПРД}$, Вт	Коэф. $G_{A\,ПРД}$ усиления передающей антенны	Длина радиолинии R_C, км	Коэф. $W^2_{0\,C}$ затухания свободного пространства на линии радиосвязи	Коэф. $W^2_{C\,МЕДЛ}$ затухания на линии радиосвязи за счет медленных замираний	Коэф. $W^2_{C\,ЗЕМ}$ потерь сигнала в Земле и в рельефе местности	Коэф. $W^2_{C\,ТРОП}$ потерь сигнала в тропосфере	Коэф. $G_{A\,ПРМ}$ усиления приемной антенны	Значения мощности информационных сигналов $P_{C\,ВХ}$ входе приемника при идеальных фидерных трактах, Вт	Среднее значение мощности информационных сигналов $P_{C\,ВХ\,ср}$ входе приемника при идеальных фидерных трактах, Вт
РРЛ стац.	2	10	10^4	40	10^{13}	1	1	1	10^4	10^{-3}–10^{-5}	10^{-5}
РРЛ моб.	2	5	10^3	40	10^{13}	1	5	1	10^3	10^{-6}–10^{-8}	10^{-7}
ТРЛ стац.	4	$5\cdot10^3$	10^4	150	10^{15}	10–30	1	10^7–10^8	10^4	10^{-11}–10^{13}	10^{-12}
ТРЛ моб.	4	10^3	$5\cdot10^3$	150	10^{15}	10–30	1	10^7–10^8	$5\cdot10^3$	10^{-12}–10^{-14}	10^{-13}
КВ ЛРС, стац.	0,01	10^4	15	$2{,}7\cdot10^4$	10^{11}	10–100		1	15	10^{-6}–10^{-7}	10^{-7}
КВ ЛРС, моб.	0,01	10^3	3	$2{,}8\cdot10^3$	10^{11}	10–100	5–10	1	3	10^{-7}–10^{-9}	10^{-8}
Спутниковая ЛРС, стац.	6	10-30	50	$4\cdot10^4$	10^{20}	1	1	1	10^5	$\approx10^{-12}$	10^{-12}
Спутниковая ЛРС, моб.	6	10-30	50	$4\cdot10^4$	10^{20}	1	1	1	10^2–10^3	$\approx10^{-14}$	10^{-14}

В таблице 2.2 в соответствии с расчетами, выполненными в работе [224], приведены оценки реальной помехозащищенности радиолиний $P_{\text{П ВХ}}$ для основных типов ЛРС военного назначения, с учетом значений $P_{\text{С ВХ}}$, с учетом коэффициента подавления $K_{\text{П}}$ и коэффициента защиты приемной антенны со стороны ее боковых и обратных лепестков $K_{\text{З АНТ}}$.

Таблица 2.2 — Расчетные значения $P_{\text{П ВХ}}$ для основных типов радиолиний военного применения, с учетом значений $P_{\text{С ВХ}}$, коэффициента подавления $K_{\text{П}}$ и коэффициента защиты приемной антенны со стороны ее боковых и основных лепестков $K_{\text{З АНТ}}$ [224]

Тип линии радиосвязи	$P_{C\ BX\ CP}$, Вт	$P_{П\ ВХ}$, Вт							
		$K_П \cdot K_{З\ АНТ}$			$K_П \cdot K_{З\ АНТ}$				
		0,001	0,01	0,1	1	10	100	1000	10000
РРЛ стац.	10^{-5}	10^{-8}	10^{-7}	10^{-6}	10^{-5}	10^{-4}	10^{-3}	10^{-2}	10^{-1}
РРЛ моб.	10^{-7}	10^{-10}	10^{-9}	10^{-8}	10^{-7}	10^{-6}	10^{-5}	10^{-4}	10^{-3}
ТРЛ стац.	10^{-12}	10^{-15}	10^{-14}	10^{-13}	10^{-12}	10^{-11}	10^{-10}	10^{-9}	10^{-8}
ТРЛ моб.	10^{-13}	10^{-16}	10^{-15}	10^{-14}	10^{-13}	10^{-12}	10^{-11}	10^{-10}	10^{-9}
КВ (УКВ) ЛРС	10^{-8}	10^{-11}	10^{-10}	10^{-9}	10^{-8}	10^{-7}	10^{-6}	10^{-5}	10^{-4}
Спутниковая ЛРС, стац.	10^{-12}	10^{-15}	10^{-14}	10^{-13}	10^{-12}	10^{-11}	10^{-10}	10^{-9}	10^{-8}
Спутниковая ЛРС, моб.	10^{-14}	10^{-17}	10^{-16}	10^{-15}	10^{-14}	10^{-13}	10^{-12}	10^{-12}	10^{-11}

Из анализа приведенных в таблице 2.2 данных можно сделать следующий основной вывод. При штатных условиях функционирования радиолиний различных типов на входных трактах их приемных устройств ($P_{\text{С ВХ}}$) имеются значительные отличия в значениях мощности полезных сигналов, которые достигают многих порядков [224].

Так, для стационарных РРЛ мощности принимаемых полезных сигналов находятся в области значений $P_{\text{С ВХ}} \approx 10^{-5}$ Вт, а для мобильных (носимых, возимых, военных) станций спутниковой связи они имеют значения $P_{\text{С ВХ}} \approx 10^{-14}$ Вт. Столь большая разница ($\approx 10^9$ раз) означает следующее. В совпадающих частотных диапазонах и при одинаковых значениях сомножителей ($K_{\text{П}} \cdot K_{\text{З АНТ}}$) линии спутниковой связи по критерию реальной помехозащищенности потенциально проигрывают стационарным радиорелейным линиям до 10^9 раз. Причем эти проигрыши обусловлены не какими-то техническими недостатками оборудования линий спутниковой связи, а существенной разницей в протяженностях интервалов связи (разница между 40 км и 40 000 км дает проигрыши в энергетическом потенциале до $\approx 10^6$ раз) и в суммарном коэффициенте усиления передающей и приемной антенн (дополнительные проигрыши в энергетическом потенциале до $\approx 10^3$ раз) [224].

Существенные проигрыши по данному показателю имеют место и у тропосферных линий (до 10^6–10^8 раз) по сравнению с радиорелейными, хотя тропосферные станции используют более мощные (до 10–100 раз) по сравнению с РРС передатчики и антенны с бóльшими коэффициентами усиления (до 5–15 раз). Причины проигрышей здесь связаны с существенно бóльшими протяженностями интервалов связи ТРЛ по сравнению с РРЛ (до 3–5 раз) и с особо большими потерями сигналов на трассах из-за механизмов дальнего тропосферного распространения радиоволн (до 10^6–10^9 раз) [224].

На рис. 2.9 представлены результаты сопоставления реальной помехозащищенности по показателю $P_{\text{П ВХ}}$ различных линий радиосвязи, нормированные по отношению к реальной помехозащищенности стационарных РРЛ, обычно имеющих наивысшие значения мощности информационных сигналов на входах их приемных устройств (значения сомножителя $K_{\text{П}} \cdot K_{\text{З АНТ}}$ для сопоставляемых радиолиний приняты одинаковыми) [224].

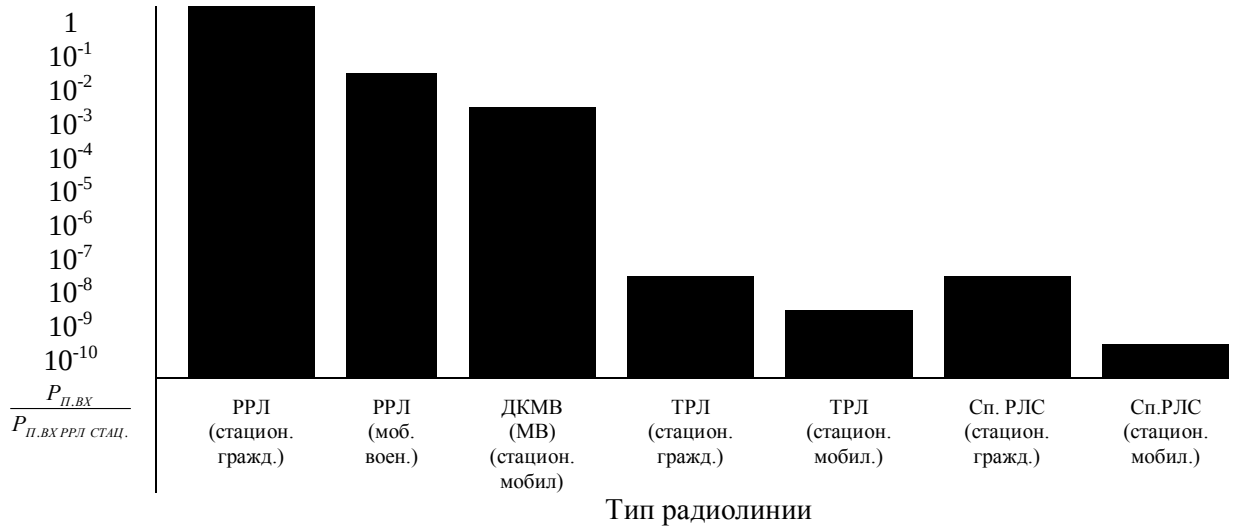


Рис. 2.9. Сравнительные данные по реальной помехозащищенности радиолиний различных типов[224]

Из анализа приведенных расчетных данных и в дополнение к сделанным выше замечаниям в части сопоставительной оценки реальной помехозащищенности РРЛ, ТРЛ и спутниковых радиолиний можно сделать следующие заключения [224]:

- значения реальной помехозащищенности радиолиний (значения $P_{П\,ВХ}$) зависят в первую очередь от реальных значений мощности полезных сигналов ($P_{\text{С ВХ СР}}$) на входах их приемников. Чем они выше, тем бóльшие значения $P_{\text{П ВХ}}$ необходимы для нарушения связи (тем выше реальная помехозащищенность);
- реальная помехозащищенность радиолиний $P_{\text{П ВХ}}$ зависит от направлений прихода радиопомех (значений $K_{\text{З АНТ}}$), их структуры (значений $K_{\text{П}}$) и для одного и того же типа радиолинии, с учетом значений сомножителя $K_{\text{П}} \cdot K_{\text{З АНТ}}$ (таблица 2.2), может отличаться от средних значений до $\pm(10^3 - 10^4)$ раз;
- потенциально наивысшими значениями реальной помехозащищенности располагают станции и линии радиорелейной связи (для стационарных РРЛ $P_{\text{П ВХ}} \approx 10^{-3}$–$10^{-5}$ Вт, для мобильных РРЛ $P_{\text{П ВХ}} \approx 10^{-6}$–$10^{-8}$ Вт);
- потенциально наименьшими значениями реальной помехозащищенности располагают линии спутниковой связи (для стационарных средств ССС $P_{\text{П ВХ}} \approx 10^{-11}$–$10^{-13}$ Вт, для мобильных средств ССС $P_{\text{П ВХ}} \approx 10^{-13}$–$10^{-15}$ Вт);

- значения реальной помехозащищенности линий тропосферной связи оказываются достаточно близкими к соответствующим показателям линий спутниковой связи ($P_{\text{П ВХ}} \approx 10^{-11}$–$10^{-14}$ Вт);
- показатели реальной помехозащищенности ДКМ (МВ) радиолиний занимают промежуточные значения между РРЛ и ТРЛ (для средств связи КВ-диапазона $P_{\text{П ВХ}} \approx 10^{-6}$–$10^{-9}$ Вт, для средств связи УКВ-диапазона $P_{\text{П ВХ}} \approx 10^{-8}$–$10^{-11}$ Вт);
- потенциально наихудшими свойствами в области электромагнитной совместимости располагают радиолинии с наименьшими значениями реальной помехозащищенности ДКМ, ТРЛ, спутниковые ЛРС.

Следует отметить, что приведенные выше соотношения между значениями реальной помехозащищенности для близких к штатным условиям применения рассматриваемых типов радиолиний не могут быть искусственно изменены в пользу любой из них за счет применения каких-то особых, присущих только данному типу радиолиний видов сигналов или способов их обработки [224].

Требуемые для практики количественные данные по оценке энергетической доступности наземных радиолиний передатчикам помех на самолетах РЭБ могут быть получены при пересчете приведенных в таблице 2.2 значений $P_{\text{П ВХ}}$ на выходную мощность передатчиков помех, размещенных на самолетах РЭБ. Результаты подобного пересчета в пределах частотных диапазонов СДВ-ММВ проведены в работе [224] и представлены в таблице 2.3. При расчетах протяженность линии радиопомех принята $R_{\text{П}}$ = 400 км, что соответствует дальности «прямой» радиовидимости при высоте барражирования самолета РЭБ на высоте 10 км. Эти ограничения введены с целью получения верхней граничной оценки для выходной мощности передатчиков помех, достаточных для нарушения связи в соответствующей ЛРС.

Обозначенные в левой части таблицы 2.3 [224] заштрихованные области соответствуют наиболее вероятным отклонениям от нормы в значениях $P_{\text{П ВХ}}$ для соответствующих типов радиолиний в зависимости от возможного изменения значения сомножителя $K_{\text{П}} \cdot K_{\text{З АНТ}}$ (10^{-3}–10^{-4}, таблица 2.2) и возможных отклонений от средних значений $P_{\text{С ВХ СР}}$ (0,1–10 Вт, таблица 2.1).

Показанная в правой части таблицы 2.3 ломаная линия соответствует реально возможным значениям суммарной эффективной мощности бортовых передатчиков помех из расчета на один самолет РЭБ — $P_{\text{П ПРД. ЭФ}\,\Sigma} \approx 100$ кВт (10^5 Вт). Тем самым она делит приведенные расчетные данные на две области: верхнюю (недоступную для средств на самолетах РЭБ с расстояний 400 км в режиме «прицельных» помех) и нижнюю (доступную для средств РЭБ в аналогичном режиме). Разделение таких зон на две является достаточно условным, поскольку относится оно к R_{Π} = 400 км и соответствует значениям сомножителя $K_{\text{П}} \cdot K_{\text{З АНТ}}$ =0,1–1 (таблица 2.2). Создание преднамеренных помех с меньших расстояний, со специальной структурой помех (импульсные, дискретно-сканирующие и пр.), со стороны боковых и обратных лепестков диаграмм направленности антенн и т. д. может быть учтено в приведенных табличных

данных соответствующим изменением их численных значений (масштабного множителя).

Таблица 2.3 — Расчетные значения эффективной мощности передатчиков помех на самолете РЭБ ($P_{\text{П ПРД ЭФ}}$) достаточных для нарушения связи с расстояния прямой видимости в 400 км [224]

$P_{\text{П ВХ}}$ (Вт)	Тип линии связи								$P_{\text{П ПРД ЭФ}}$ (Вт)							
									Длина волны (м)							
									50000	5000	500	50	5	0,5	0,05	0,005
									Частота (МГц)							
	РРЛ Стац.	РРЛ Моб.	КВ (УКВ)	ТРЛ Стац.	ТРЛ Моб.	Спутниковые ЛРС Стац.	Спутниковые ЛРС Моб.	Проводн.	0,006	0,06	0,6	6	60	600	6000	60000
									СДВ	ДВ	СВ	КВ	МВ	ДЦВ	СМВ	ММВ
10^{-4}	■							■	1	10^{2}	10^{4}	10^{6}	10^{8}	10^{10}	10^{12}	10^{14}
10^{-5}	■							■	0,1	10	10^{3}	10^{5}	10^{7}	10^{9}	10^{11}	10^{13}
10^{-6}	■	■							10^{-2}	1	10^{2}	10^{4}	10^{6}	10^{8}	10^{10}	10^{12}
10^{-7}	■	■	■						10^{-3}	0,1	10	10^{3}	10^{5}	10^{7}	10^{9}	10^{11}
10^{-8}	■	■	■						10^{-4}	10^{-2}	1	10^{2}	10^{4}	10^{6}	10^{8}	10^{10}
10^{-9}		■	■						10^{-5}	10^{-3}	0,1	10	10^{3}	10^{5}	10^{7}	10^{9}
10^{-10}		■	■						10^{-6}	10^{-4}	10^{-2}	1	10^{2}	10^{4}	10^{6}	10^{8}
10^{-11}			■	■		■			10^{-7}	10^{-5}	10^{-3}	0,1	10	10^{3}	10^{5}	10^{7}
10^{-12}				■	■	■			10^{-8}	10^{-6}	10^{-4}	10^{-2}	1	10^{2}	10^{4}	10^{6}
10^{-13}				■	■	■	■		10^{-9}	10^{-7}	10^{-5}	10^{-3}	0,1	10	10^{3}	10^{5}
10^{-14}				■	■	■	■		10^{-10}	10^{-8}	10^{-6}	10^{-4}	10^{-2}	1	10^{2}	10^{4}
10^{-15}				■	■	■	■		10^{-11}	10^{-9}	10^{-7}	10^{-5}	10^{-3}	0,1	10	10^{3}
10^{-16}					■		■		10^{-12}	10^{-10}	10^{-8}	10^{-6}	10^{-4}	10^{-2}	1	10^{2}
10^{-17}							■		10^{-13}	10^{-11}	10^{-9}	10^{-7}	10^{-5}	10^{-3}	0,1	10

Из приведенных данных таблицы 2.3, например, следует, что при создании прицельной помехи с самолета РЭБ мобильной ТРС со стороны ее главного лепестка с мощностью $P_{\text{П ВХ}} = 10^{-12}$ Вт, необходимыми и достаточными значениями выходной мощности передатчика помех на самолете РЭБ с расстояния $R_{\text{П}} = 400$ км в частотном диапазоне 600 МГц составят значения всего около $P_{\text{П ПРД. ЭФ}} \approx 1$ Вт. Это вполне согласуется с данными, которые были экспериментально получены еще в 1967 г. путем специально организованных полигонных испытаний подавления наземной ТРЛ преднамеренных помех с авиационного постановщика помех [225].

В случае же применения импульсных помех (обычно $K_{\text{П имп.}} \le (10^{-2} - 10^{-3})$) и учета негативного влияния на связь быстрых и медленных замираний сигналов на интервалах тропосферной связи, необходимая и достаточная мощность передатчика помех для тех же условий может составить $P_{\text{П ПРД. ЭФ}} \approx 1$ мВт! При этом подобного рода результаты не являются неожиданными. Именно они нашли свое подтверждение в специальных испытаниях ТРЛ военного назначения [226].

Полученные расчетные данные, представленные в таблице 2.3, позволяют сделать прогноз в отношении возможных способов подавления наземных сетей связи преднамеренными помехами с передатчиков, размещенных на самолетах РЭБ.

Тропосферная связь. Для данного вида связи наиболее вероятна будет постановка заградительных помех (шумовых, частотно- и дискретно-сканирующих) в рамках рабочих диапазонов ныне существующего парка многоканальных ТРС (с полосами частот каналов радиосвязи 0,1–1 МГц). Подтверждением этому служат данные таблицы 2.3, из которой следует, что с рас-

стояний прямой видимости $R_П$ = 100–400 км потенциальные энергетические запасы одного из бортовых передатчиков помех самолета РЭБ с эффективной выходной мощностью $P_{П\,ПРД\,эф}$=1–10 кВт и с различными значениями коэффициента подавления $K_П$, изменяемого от 0,1 (тепловые шумы) до 10^{-3} (дискретно-сканирующие помехи), могут составлять значения 10^5–10^6 и более раз. Этого вполне достаточно для организации ТРС заградительных помех одновременно на 100–1000 частотах связи со стороны основных и боковых лепестков диаграммы направленности антенн ТРС ($10^2 \le K_{З\,АНТ} \le 10^3$) [224].

Подтверждением этому могут служить расчетные данные, представленные в работе [224], для участка ТРЛ с протяженностью интервала связи $R_С \approx 150$ км и для линий помех с двумя протяженностями — $R_П \approx 150$ км и $R_П \approx 450$ км. Они приведены для двух частотных поддиапазонов (50 и 5 см) с близкими к реальным значениями энергетических потенциалов передатчиков ТРС ($P_{П\,ПРД\,эф}$ = 55–65 дБ/Вт). При расчете использовались ограничения, соответствующие воздействию наземного передатчика помех со значением эффективной мощности ($P_{П\,ПРД\,эф} \approx 10^9$ Вт), и эквивалентного по степени воздействия передатчику помех на летательном аппарате ($P_{П\,ПРД\,эф} \approx 1$ Вт). Полученное значение проигрыша в энергетическом потенциале для наземного передатчика помех по сравнению с передатчиком помех на ЛА (в 10^9 раз) служит достаточно наглядным подтверждением высокой эффективности постановщиков преднамеренных помех на самолетах РЭБ и их реальной значимости для организации радиоподавления систем связи и управления противника.

Спутниковая связь. Как и для линий тропосферной связи, для линий спутниковой связи наиболее вероятна постановка заградительных помех (шумовых, частотно- и дискретно-сканирующих) в рамках рабочих диапазонов станций спутниковой связи. Аналогичные ТРЛ энергетические запасы по мощности передатчиков помех ($P_{П\,ПРД\,эф} \approx 10$ кВт) в отношениях помеха/сигнал $P_{П\,ВХ}/P_{С\,ВХ} \approx 10^5$–$10^9$ (что соответствует изменению коэффициента подавления $K_П$ от 0,1 до 1) обеспечивают возможности для постановки заградительных помех земным (морским) станциям спутниковой связи в выделенном частотном диапазоне с расстояний прямой видимости ($R_П \le 400$ км) [224].

В отличие от тропосферных радиолиний, постановка преднамеренных помех спутниковым линиям возможна и наземными передатчиками помех, воздействующими непосредственно на оборудование связи, размещенное на КА. При этом подразумевается, что КА расположен на геостационарной или на близкой к ней орбите ($R_С \approx R_П \approx 40\,000$ км). Для достижения необходимой эффективности таких передатчиков вполне вероятно применение дискретно-сканирующих помех в сочетании с локационными режимами их работы (импульсными радиосигналами длительностью 10^{-3}–10^{-6} с [224].

ДКМВ линии радиосвязи. Приведенные в таблице 2.2 расчетные значения $P_{П\,ВХ}$, $P_{С\,ВХ}$ и их отношений ($K_П \approx 10^{-2}$–10^3) для ДКМВ радиолиний свидетельствуют о возможности постановки в данном частотном диапазоне с самолетов РЭБ широкополосных заградительных (системных) помех. Как и для тропосферной (спутниковой) связи, здесь наиболее вероятными являются шумовые, частотно-сканирующие и дискретно-сканирующие заградительные помехи

с возможными значениями $K_П$ от 0,3 (голосовая радиосвязь) до 0,1 (телефонные каналы) [224].

Суммарные энергетические запасы при использовании одного бортового передатчика помех ДКМВ-диапазона с выходной мощностью $P_{П\,ПРД\,эф} \approx 10$ кВт (10^4 Вт), при $K_П \approx 0{,}3$–$0{,}1$ и при создании помех с расстояний прямой видимости $R_П = 100$–400 км (таблица 2.3) составляют: $(10^2$–$10^3)/K_П \approx 10^3$–10^4. Это позволяет оценить возможную ширину подавляемых заградительными помехами частотных поддиапазонов [224].

Так, если принять за исходные типовые значения полосы пропускания ДКМВ-линии радиосвязи от $\Delta f_с \approx 1$ кГц (режим телеграфной связи) до $\Delta f_с \approx 3$ кГц (режим телефонной связи), то при сетке частот $\Delta f_1 = 1$ кГц возможная полоса частот заградительных шумовых и дискретно-сканирующих помех составит $\Delta f_П \approx 1$–10 МГц. При длительности импульсов помех $\Delta t_П = \Delta f_1 \approx 10^{-3}$ с частота их повторения за 1 с на каждой из подавляемых частот составит $n \approx 0{,}1$–1. Этого может оказаться вполне достаточно для подавления практически всех видов связи на основе ДКМВ-радиолиний в зоне их электромагнитной доступности со стороны постановщиков помех [224].

МВ-линии радиосвязи. Приведенные в таблице 2.3 данные для МВ-радиолиний (метровые волны) по расчетным значениям $P_{П\,ВХ}$ и $P_{С\,ВХ}$ оказываются достаточно близкими к ДКМВ-радиолиниям, хотя и используют более высокие частоты. Так, для передатчика помех на самолете РЭБ с выходной мощностью $P_{П\,ПРД\,эф} \approx 1$–10 кВт и вероятных значений коэффициента подавления $K_П \approx 10^{-2}$–10^{-3} существует возможность для постановки с самолета РЭБ широкополосных заградительных помех в рамках всего МВ-диапазона [224].

Радиорелейная связь. Существенно более высокие по сравнению с ТРЛ и спутниковыми радиолиниями значения показателей реальной помехозащищенности радиорелейной связи (таблицы 2.1, 2.2, 2.3), которые обеспечивают повышенную защищенность данного рода связи от всех видов помех и особенно со стороны боковых и обратных лепестков диаграмм направленности антенн. Как следует из таблицы 2.3, РРЛ сантиметрового и миллиметрового диапазонов волн оказываются энергетически недоступными как для прицельных, так и для заградительных помех с самолетов РЭБ на дальностях воздействия помех более 100–200 км. Что же касается метрового и дециметрового диапазонов волн, где сейчас сосредоточена бóльшая часть существующего парка РРС, то они остаются энергетически доступными для прицельных и заградительных помех в основном со стороны главных и первых боковых лепестков диаграмм направленности антенн. Возможному эффективному применению таких помех способствуют и особенности организации самой радиорелейной связи. Поскольку протяженности отдельных интервалов при развертывании РРЛ обычно не превышают 30–40 км, то в зоне досягаемости самолета РЭБ с радиусом $R_П \approx 200$–400 км может оказаться одновременно до 5–10 участков многоинтервальных линий. При этом в сторону постановщика помех может быть одновременно развернуто до 5–10 приемных антенн РРС. И при ширине главных лепестков диаграмм направленности антенн $\alpha \approx 5^\circ$–15° периметры их зон на расстояниях 200–400 км от РРС составят 25–100 км. Это означает, что

при барражировании постановщика помех в недоступной зоне для огневых средств поражения противостоящей стороны он постоянно будет находиться в пределах одного или нескольких главных лепестков диаграммы направленности подавляемых радиолиний. Кроме того, дополнительное снижение помехозащищенности РРЛ вполне вероятно и за счет процессов суммирования помех отдельных интервалов многоинтервальных РРЛ.

2.3.3. Особенности подавления спутниковых радионавигационных систем

Задачей подавления тракта приема спутниковых радионавигационных систем (СРНС) является искажение навигационных сигналов, принимаемых потребителями от навигационных КА, входящих в наблюдаемую группировку, по обоим каналам связи. Эти эффекты достигаются за счет [250]:

- значительного увеличения отношения помеха/сигнал;
- существенного повышения веса паразитных составляющих в корреляционном отклике обработанных навигационных сигналов;
- затруднения или полного срыва в течение длительного времени режима захвата и слежения за навигационными сигналами.

В качестве помеховых воздействий могут быть использованы [250]:

- прицельный (по частоте и спектру) шумовой процесс;
- сигнал на рабочей частоте с изменяемой фазой по закону цифровой модулирующей функции — псевдоимитирующий сигнал (однако такая реализация процесса требует знания тактовой частоты в формирователях псевдослучайной последовательности, а также ожидаемых значений доплеровских сдвигов);
- помеховые сигналы, имитирующие навигационные.

Первые два помеховых воздействия требуют повышенных энергетических затрат. Третье помеховое воздействие представляется наиболее эффективным и относительно простым для технической реализации. Реализация имитации осуществляется приемом навигационных сигналов на рабочих несущих частотах, усилении их и ретрансляции на тех же рабочих частотах в сторону бортовой приемной навигационной системы крылатой ракеты, при предварительном обогащении ее рециркуляционными компонентами (заградительная помеха по задержке). Тактика применения помехового воздействия на приемник GPS крылатой ракеты простая и однозначная: оно должно излучаться равномерно по всем направлениям нижней полусферы [250].

Более подробная информация о подавлении спутниковых радионавигационных систем представлена в работе А.П. Дятлова, П.А. Дятлова и Б.Х. Кульбикаяна [176].

2.4. Системы и средства РЭБ для индивидуальной защиты авиации (на примере систем и средств ВС США)

2.4.1. Авиационные бортовые системы предупреждения об облучении радиолокационными станциями комплексов ПВО

В современных условиях воздушное пространство характеризуется большой насыщенностью электромагнитными сигналами, излучаемыми радиоэлектронными системами различного назначения (включая сигналы головок самонаведения ракет и РЛС системы ПВО). При непрерывном совершенствовании этих средств системы предупреждения об облучении становятся важным звеном в бортовых комплексах всех боевых самолетов. По сложности построения и функционирования эти системы приближаются к бортовой аппаратуре РТР. Основной отличительной особенностью систем предупреждения об облучении является то, что они предназначаются в основном для защиты носителя, на котором они установлены. Это означает, что такие системы должны работать в режиме реального времени. В отличие от систем предупреждения об облучении системы, РТР предназначены для решения более широкого круга задач. Они должны обеспечивать высокую точность измерения основных параметров сигнала (несущая частота, длительность и частота повторения импульсов и т. д.), излучающих РЭС, а также отслеживать во времени изменения этих параметров [250].

Системы предупреждения об облучении осуществляют обнаружение и идентификацию принимаемых сигналов путем сравнения их с информацией об известных РЭС вероятного противника и вырабатывают сигналы для предупреждения экипажа о наиболее опасных РЭС. При этом практически все самолеты и вертолеты ВВС США и других стран НАТО оснащены системами подобного рода [250].

Система AN/ALR-56M была разработана фирмой Loral и является наиболее распространенным устройством для обнаружения облучений в ВВС США и ОВС НАТО. Система предназначена для обнаружения сигналов РЛС, работающих в импульсном и непрерывном режимах, а также РЛС с высокой скрытностью работы. Определение типа излучающих средств осуществляется путем сравнения обработанной информации с данными об известных РЭС, хранящихся в запоминающем устройстве. По сравнению со своими аналогами, система имеет на четверть меньшую массу и почти вдвое меньший объем благодаря применению современной технологии функциональных интегральных схем и микропроцессоров. Приемник системы обеспечивает перехват сигналов в диапазоне частот 0,5–18 ГГц [250].

Система AN/ALR-67 предназначена для предупреждения о радиолокационном облучении и была разработана фирмой Itek для установки на самолетах тактической авиации ВМС США. В состав системы входят: тюнеры, супергетеродинный приемник и быстродействующий цифровой процессор. Составление программы работы для системы проводится перед выполнением боевой задачи. В программу могут быть введены изменения в зависимости от конкретной тактической обстановки. Система AN/ALR-67 взаимодействует с пере-

датчиками помех, системами запуска ракет типа HARM и устройствами выброса дипольных отражателей и ИК-вспышек [250].

Система AN/ALR-69 использует приемник с быстрым сканированием разработки фирмы Litton. Скорость перестройки у таких приемников в полосе частот 2–18 ГГц составляет 100 кГц за 50 мкс. Система обеспечивает высокую точность измерения частоты. При разработке системы AN/ALR-69 за основу был принят приемник предупреждения о радиолокационном облучении AN/ALR-46, и дополнительно в систему были введены частотно-избирательная приемная подсистема FSRS (Frequency Selective Receiver System) и узкополосный приемник предупреждения о запуске ракет. Подсистема FSRS предназначена для обнаружения и анализа ВЧ-сигналов РЛС управления и наведения ракет, непрерывных сигналов, излучаемых ГСН ракет, работающих в полуавтоматическом режиме [250].

Система AN/ALR-74 разработана фирмой Litton и является комбинированной системой предупреждения об облучении. В этой системе используется приемник с мгновенным измерением частоты (диапазона 0,5–20 ГГц), работающий параллельно с приемником прямого усиления, и супергетеродинный приемник, обеспечивающий обнаружение непрерывного излучения и импульсных сигналов с высокой частотой повторения, излучаемых доплеровскими РЛС. Приемник с мгновенным измерением частоты определяет частоту каждого импульса. Эти данные затем обобщаются и используются совместно с получаемой от приемника прямого усиления информацией о длительности, частоте повторения импульсов и их амплитуде. Система AN/ALR-74 устанавливается на самолетах ВВС и ВМС США (таких как F-16, A-10 и F-4E) и используется в комплексе с бортовой системой индивидуальной защиты ASPJ [250].

Увеличение сложности радиоэлектронных систем приводит к необходимости постоянно совершенствовать аппаратуру РТР и систем предупреждения об облучении. Если раньше для идентификации излучающих средств было достаточно измерить длительность, частоту повторения и амплитуду импульсов, то теперь требуется измерять такие сложные параметры, как фаза и поляризация сигналов [250].

Начиная с середины 70-х гг. прошлого столетия, в США проводились исследования, направленные на создание приемных систем, в которых сочетаются радиотехнические и оптические устройства. Предполагалось, что с помощью таких систем станет возможным решение проблемы анализа и сортировки радиолокационных сигналов в сложной электромагнитной обстановке. Проведенные исследования показали, что приемные устройства на ячейках Брэгга имеют ограниченный динамический диапазон (30–50 дБ). В дальнейшем динамический диапазон был расширен до 60 дБ. Работы в этом направлении продолжаются. Фирмы Harris, Sunders, Westinghouse, отделение Itek фирмы Litton и отделение электронно-оптических систем фирмы Loral разрабатывают акустооптические процессоры для систем РЭБ [250].

Система PTP SCR-2100 представляет собой набор приемников AN/ALR-75 (V) фирмы Scientific Communication. Система предназначена для

поиска и анализа сигналов в диапазоне частот от 0,1 до 40 ГГц. Вся аппаратура, за исключением дисплея, выполнена на твердотельных компонентах. Набор тюнеров может меняться в соответствии с решаемой задачей. Процессор обрабатывает на промежуточной частоте сигналы, поступающие с любого из 8 тюнеров, и обеспечивает выдачу данных на панорамный дисплей. Применение анализатора импульсов SCP-2160 позволяет восстанавливать первоначальную последовательность принятых сигналов и осуществлять достаточно точное измерение параметров импульсов. Типичная величина подавления по зеркальному каналу на частотах до 18 ГГц равна 80 дБ. Типичная величина подавления паразитного сигнала на промежуточной частоте равна 100 дБ, минимальная — 80 дБ. В качестве других особенностей этой системы отмечаются цифровое управление, оптимизация процессов поиска и приема, идентификация сигналов путем сравнения с информацией, имеющейся в библиотеке источников, и наличие дисплеев с обновлением информации в цифровой форме [250].

Система PTP AN/ALQ-78 производится фирмой Loral, которой оснащаются самолеты противолодочной авиации P-3C, стоящие на вооружении ВМС США. Система осуществляет обнаружение импульсных радиолокационных излучений в определенных участках частотного диапазона, характерных для противолодочной обороны, а также определение основных характеристик принятых сигналов и направления на источники излучения, размещаемые в основном на подводных лодках. В состав этой системы входят: антенна, вращающаяся с высокой скоростью, супергетеродинный приемник с быстрой перестройкой по частоте и управляющий процессор, использующий принятые сигналы для обеспечения пеленгации и сопровождения целей. Измеренные параметры сигналов и данные о направлении на источники излучения передаются в центральный процессор, где производятся их обработка, анализ и регистрация, а также преобразование в цифровую форму, удобную для отображения на экранах многофункциональных дисплеев. Работа системы автоматизирована. Основной режим работы — всенаправленный поиск. После обнаружения и анализа радиолокационных сигналов приемник автоматически начинает работать в режиме пеленгации, осуществляя накопление данных об источниках излучения и определяя их азимуты. Затем система вновь возвращается в режим всенаправленного поиска [250].

Система AN/ALQ-78 прошла несколько модернизаций с целью создания варианта, способного работать в обстановке с высокой плотностью электромагнитных излучений. Система продается и находится на вооружении в ряде западных стран: Австралии, Канаде, Японии и Нидерландах. Стоимость одного комплекта аппаратуры — примерно 170 тыс. долларов США [250].

2.4.2. Авиационные бортовые системы радио- и радиотехнической разведки

Система PTP ES-5000 (США, 1995 г.) имеет диапазон частот 500–40 000 МГц, точность пеленгования источников радиоизлучения 150 м, диапазон измерения длительности импульсов — в пределах 0,1–2,5 мкс.

Система AN/ALQ-61 (США) имеет диапазон частот 80–18 000 МГц, чувствительность — 190дБВт/Гц, точность пеленгования источников радиоизлучения — 2° [250].

Станция WJ-1740 имеет диапазон частот 30–40 000 МГц, чувствительность — 179–195 дБВт/Гц, точность измерения пеленга 1–2° [250].

Система LR-100 (США) имеет диапазон частот 2–18 ГГц, носитель — БПЛА, динамический диапазон 60 дБ, точность измерения частоты 2 МГц, точность пеленга 0,8°, массу 16 кг [250].

Система PTP FASTHAT (Fast High Accuracy Tunable — с быстрой установкой частоты), разработанная фирмами Martin Marietta и Information and Communication System (США), предназначена для систем с быстрым преобразованием Фурье (осуществляемых, например, с помощью ячеек Брэгга). Система обеспечивает перехват сигналов в полосе частот от 0,5 до 18 ГГц при ширине мгновенной полосы пропускания 0,5 ГГц и высокой вероятности перехвата. В приемнике используется прецизионный гетеродин с быстрой перестройкой, созданной на основе перестраиваемого варактором генератора и разработанной фирмой Martin Marietta техники синхронизации частоты. При наличии управляющего процессора, который используется в приемнике FASTHAT, можно успешно осуществлять интенсивную радиотехническую разведку во всём диапазоне частот, слежение за обнаруженным сигналом в процессе сканирования по частоте, а также проверку аппаратуры на электромагнитную совместимость и измерение уровня паразитных излучений. Система имеет следующие технические характеристики: коэффициент шума 18 дБ; скорость перестройки 100 МГц/мкс; точность настойки ±250 кГц; точность повторной установки частоты ±100 кГц; величина случайной частотной модуляции 30 кГц; коэффициент передачи преобразователя (вход/выход) 30 дБ [250].

Система PTP LR-5200 относится к тактическим системам и выпускается фирмой Litto Ateco (США). Диапазон разведки 2–18 ГГц. Приемник может быть запрограммирован на работу в двух режимах [250]:

1. обнаружение, опознавание и определение местоположения;
2. получение информации только об определенных типах источников излучения в соответствии с приоритетом и степенью их опасности.

С помощью установленной на самолете системы LR-5200 обеспечиваются обнаружение, опознавание и определение местоположения источников, расположенных по обе стороны от направления полета. Перед началом полета система может быть запрограммирована на 10 типов, 40 рабочих уровней приоритета и степени опасности источников излучения путем введения в запоминающее устройство системы данных о несущей частоте, длительности и частоте повторения импульсов, виде модуляции и скорости сканирования. Данные об обнаруженных источниках излучения отображаются на дисплее оператора системы, находящегося на борту самолета, и одновременно передаются в тактическое звено управления, а также записываются в запоминающее устройство. Система LR-5200 имеет следующие технические характеристики: полоса частот приемника в режиме поиска — 400 МГц; в режиме сигнала — 25 МГц; перекрытие по азимуту: в режиме поиска — 360°, в режиме пеленга — 180°;

чувствительность системы, обеспечивающей обработку сигнала, — 65 дБ/мВт; отношение сигнал/шум, обеспечивающее обработку сигнала, — 14 дБ; динамический диапазон — 60 дБ; средняя квадратичная погрешность измерения азимута — 5° [250].

В перспективе до 2020 г. ожидается, что средства РТР будут использовать диапазон частот 0,7–160 ГГц для тактических самолетов и 0,25–160 ГГц для стратегических самолетов. Чувствительность приемной части системы может составить до 190 Вт/Гц, динамический диапазон — до 90 дБ, точность пеленга — до 0,02–0,05°, число каналов — более 100, число РЭС, параметры которых хранятся в запоминающем устройстве, может составить несколько тысяч. Масса таких систем может быть порядка 20–30 кг [250].

К этому же сроку ожидается, что системы радиоразведки будут использовать диапазон частот от 0,03 МГц до 100 ГГц, иметь чувствительность 150–180 дБВт/Гц, избирательность — 90–95 дБ, точность пеленга — 0,1–0,5 °, точность определения координат на дальности до 300 км — 10–20 м [250].

2.4.3. Бортовые средства и комплексы РЭБ для индивидуальной защиты авиации от систем ПВО

2.4.3.1. Станции РЭБ для индивидуальной защиты самолетов

Основными станциями для обеспечения индивидуальной защиты самолетов ВВС США считаются [250]:

- AN/ALQ-119;
- AN/ALQ-135;
- AN/ALQ-137;
- AN/ALQ-184;
- AN/ALQ-165;
- AN/ALR-94.

По мере разработки сверхмощных процессоров высокой производительности стало возможным в программе ASPJ частично, а в программе INEWS полностью реализовать объединение всех подсистем РЭО современного тактического истребителя на новом функциональном уровне. На основе корреляционной обработки данных, поступающих от различных РЛС обнаружения, а также от аппаратуры связи, навигации и опознавания, производится оценка тактической обстановки, и пилоту выдаются необходимые рекомендации на задействование средств РЭП или совершение необходимых маневров самолета. При этом задействование средств РЭП возможно в автоматическом режиме [250].

Рассмотрим более подробно отдельные системы и комплексы индивидуальной защиты самолетов и вертолетов. При рассмотрении необходимо обратить внимание, что в настоящее время в США данное направление активно развивается. В результате создаются комплексы РЭБ как для вновь разрабатываемых самолетов (комплекс INEWS для F-22), так и комплексы для уже давно эксплуатируемых самолетов. Примером такого комплекса может служить комплекс индивидуальной защиты IDECM, первоначально разработанный для палубных истребителей-штурмовиков F/A-18E/F ВМС США, а также комплекс

AN/ALQ-211 SIRFC — для вертолетов сухопутных войск США. В целом оснащение самолетов тактической авиации станциями РЭП нового поколения позволяет с высокой эффективностью обеспечить индивидуальную защиту существующего парка самолетов (F-15, F-16, A-10, F-22, F-35 и др.) [223, 227].

2.4.3.2. Авиационные передатчики помех одноразового использования

Передатчики помех одноразового использования (ПОИ) изготавливаются на основе монолитных интегральных схем СВЧ-диапазона. Передатчики помех в виде переизлучателей или ответчики с микропроцессорным управлением могут размещаться в аэродинамическом корпусе стандартного пиропатрона, используемого авиационным автоматом выброса дипольных противорадиолокационных отражателей и ИК-ловушек. Основное их назначение заключается в создании уводящих ответных помех приближающимся к самолету головкам самонаведения управляемых ракет класса «воздух — воздух» и «земля — воздух». В долгосрочном плане в США проводятся поисковые разработки по созданию многоспектральных ПОИ. Необходимость в устройствах, которые могли бы работать в нескольких участках частотного спектра, связана с появлением комбинированных радиолокационных головок самонаведения для управляемых ракет, например сантиметрового и миллиметрового диапазона волн. Такие устройства могут быть созданы на базе развивающейся технологии массового производства дешевых монолитных сверхвысокочастотных (МСВЧ) интегральных схем, являющихся базовыми электронными компонентами ПОИ [250].

2.4.3.3. Комплекс РЭБ индивидуальной защиты AN/AAQ-24(V)13 LAIRCM

Комплекс РЭБ индивидуальной защиты AN/AAQ-24(V)13 LAIRCM устанавливается на воздушных судах и тяжелых вертолетах и предназначен для оптоэлектронного подавления управляемых ракет с тепловой головкой самонаведения. Принцип его функционирования заключается в следующем: при обнаружении факта пуска ракеты он определяет степень ее угрозы и осуществляет ее оптико-электронное подавление. В состав комплекса LAIRCM входят 4 станции: предупреждения об облучении УФ-диапазона; сопровождения управляемой ракеты; оптико-электронного подавления и управления; устройства для обнаружения, сопровождения и постановки помех управляемой ракете с ИК ГСН. Количество поворотных турелей с оптоэлектронным оборудованием зависит от габаритных размеров и предназначения ЛА [218].

Предполагается оснастить этими комплексами самолеты командования воздушных перебросок: C-17A, C-130, C-5M, C-40, C-37, C-130J, новый легкий транспортный (LCA) и транспортно-заправочный самолеты, вертолеты морской пехоты CH-53D и E, CH-46E (156 машин были оснащены в 2013 г.), MV-22 (390 единиц до 2030 г.). Комплексом РЭБ LAIRCM уже оборудованы самолеты E-3 AWACS [218].

2.4.3.4. Система индивидуальной защиты TEWS

Система индивидуальной защиты TEWS в настоящее время установлена на тактических истребителях F-15. Система TEWS имеет модульную структуру и включает в свой состав: системы предупреждения об облучении AN/ALR-56C и AN/ALQ-128; станцию РЭП AN/ALQ-135(V); автомат отстрела дипольных отражателей и ложных тепловых целей AN/ALE-45 [227].

Станция РЭП AN/ALQ-135(V) может одновременно и в соответствии с приоритетами целей осуществлять постановку активных помех непрерывным, импульсным и импульсно-доплеровским РЛС. Она способна генерировать шумовые и имитирующие помехи в диапазоне от 2 до 20 ГГц. В состав станции не входит собственное приемное устройство, сигнал в нее поступает от приемника предупреждения об облучении AN/ALR-56C, а на самолетах F-15E от БРЛС с АФАР AN/APG-82(V)1. Оконечным излучающим устройством станции являются рупорные антенны [227].

2.4.3.5. Система индивидуальной защиты EPAWSS

В период с 2020 по 2030 г. планируется замена системы TEWS на EPAWSS. В начале 2016 г. компания BAE Systems была выбрана ВВС США в качестве основного разработчика этой новой системы. Систему EPAWSS планируется устанавливать на самолеты F-15C/D/E [227, 430].

Система EPAWSS будет включать [227, 430]:

- средства предупреждения о радиолокационном облучении и ракетной атаке;
- средства РЭП ориентированные на противодействие ракетам «воздух — воздух» и «земля — воздух», а также РЛС обнаружения наземного, воздушного и морского базирования;
- расходуемые средства противодействия в радио- и оптическом диапазонах длин волн.

Одной из дополнительных возможностей системы EPAWSS предположительно будут определение местоположения источников радиоизлучения и возможность постановки помех в миллиметровом диапазоне длин волн. Отличительной особенностью данной системы, как предполагается, будет наличие устройств запоминания и воспроизведения сигналов. Такие устройства позволяют осуществлять радиоэлектронное подавление всех видов когерентных РЛС (импульсно-доплеровских и со сложными сигналами), осуществлять одновременный коррелированный ввод в их сигналы ложной информации о дальности и скорости движения, а также осуществлять постановку правдоподобных имитирующих помех [227].

Общая стоимость программы EPAWSS оценивается в 4 млрд долларов. Система защиты EPAWSS, как ожидается, будет установлена примерно на 412 самолетах F-15C/D/E, стоящих на вооружении ВВС США и ее союзников. Поставки систем EPAWSS должны начаться в 2020 г., а ее эксплуатация на самолетах предполагается на период до 2029 г. [430].

2.4.3.6. Подвесная контейнерная система РЭП AN/ALQ-131

Подвесная контейнерная система РЭП AN/ALQ-131 предназначена для оснащения тактических истребителей F-16. В состав системы входят автоматы отстрела дипольных отражателей и ложных тепловых целей AN/ALE-47 и средств предупреждения об облучении AN/ALR-56M. В целях повышения эффективности средств РЭБ на самолетах установлена система управления AN/ALQ-213. Автомат AN/ALE-47 позволяет осуществлять отстрел 30 пиропатронов с ложными тепловыми целями типа MJU-7 или MJU-10, а также снаряженных дипольными отражателями типа RR-170 или RR-180. Масса устройства в комплектации с 4 блоками расходуемых средств РЭБ составляет около 30 кг. Приемник средства предупреждения об облучении AN/ALR-56M позволяет обнаруживать непрерывные и импульсные сигналы в диапазоне частот от 0,3 до 20 ГГц. В его состав входят 4 спиральные антенны и 1 штыревая. При обнаружении РЛС, осуществляющих сопровождение самолета, в автоматическом режиме выдается команда на отстрел ложных целей [227].

С 2013 г. приостановлено финансирование программы модернизации системы РЭП AN/ALQ-131, что подразумевает возможное оснащение самолетов другой системой. В качестве альтернативных вариантов оснащения средствами РЭП самолетов F-16 рассматриваются системы постановки помех индивидуальной защиты ЛА AN/ALQ-214, буксируемых ложных целей AN/ALE-50(55), а также ресурсы БРЛС с АФАР [227].

2.4.3.6. Интегрированная бортовая система РЭБ IDECM

Интегрированная бортовая система РЭБ IDECM предназначена для защиты истребителя-штурмовика F/A-18E/F. В состав системы IDECM входят [227]:

- станция предупреждения об облучении AN/ALR-67(V)3;
- система РЭП AN/ALQ-165 или станция активных помех AN/ALQ-214;
- блок ложных целей AN/ALE-50 или AN/ALE-55 FODT (Fiber Optic Decoy Towed), в зависимости от модификации бортовой системы обороны;
- автоматы выброса расходуемых средств РЭП AN/ALE-47.

Известны четыре модификации системы IDECM. Основным их отличием являются различные системы РЭП и блоки ложных целей. В период до 2020 г. в ВМС США будет осуществлена замена модификаций Block 1 и Block 2 на Block 3 [227].

Станция РЭП AN/ALQ-165, которой оснащаются системы IDECM модификации Block 1, предназначена для создания активных помех в диапазоне от 1 до 35 ГГц. В ее состав входят 5 блоков: НЧ- и ВЧ-приемники и передатчики, а также устройство управления. Передающие антенны размещаются в хвостовой и носовой частях фюзеляжа. Эта станция РЭП обеспечивает автоматическое обнаружение и идентификацию сигналов РЛС противника, определение приоритетности их подавления комбинированными шумовыми и импульсными

помехами. Выходная мощность в импульсе — 1 кВт, время реакции — от 0,1 до 0,25 с [227].

Принцип действия системы IDECM модификаций Block 3 и Block 4 заключается в следующем: сигнал объекта подавления принимается станцией предупреждения об облучении AN/ALR-67(V)3, и на его основе в станции помех AN/ALQ-214 формируется имитирующий помеховый сигнал, который преобразуется в электронном преобразователе частоты и передается по волоконно-оптической линии связи в буксируемую ложную цель, где сигнал усиливается и излучается. Предусмотрена возможность автоматического отстрела ложных тепловых ловушек при атаке самолета ракетами с ИК ГСН [227].

Серийное производство системы IDECM Block 3 началось в 2011 г. Модификация Block 3 предполагает замену блока ложных целей с AN/ALE-50 на AN/ALE-55, обеспечение взаимодействия его со станциями помех AN/ALQ-214(V)4 и AN/ALR-67(V)3, а также с автоматами выброса расходуемых средств РЭБ AN/ALE-47. При этом к 2018 г. планируется полная замена AN/ALE-50 на AN/ALE-55 [227].

Модификация системы IDECM до Block 4 предполагает значительное изменение элементной базы, входящей в ее состав станции помех AN/ALQ-214, с целью увеличения возможностей по противодействию угрозам и ее функциональное объединение с БРЛС на основе АФАР. В дальнейшем для унификации средств РЭП для самолетов F/A-18E/F и F/A-18C/D предполагается доведение системы IDECM до модификации Block 5. Начало поставок ALQ-214 Block 4 — в 2015 г., а Block 5 — в 2016–2017 гг. [227].

2.4.3.8. Комплекс РЭБ стратегического бомбардировщика B-52 Stratofortress

Комплекс РЭБ стратегического бомбардировщика B-52 Stratofortress включает в себя [227]:

- станции предупреждения об облучении: AN/ALR-20, AN/ALR-46, AN/ALQ-153;
- станции активных помех: AN/ALQ-155, AN/ALQ-172, AN/ALQ-122 и AN/ALT-32;
- автоматы выброса расходуемых средств РЭБ AN/ALE-20 (отстрел ложных тепловых целей) и AN/ALE-24 (отстрел дипольных отражателей).

Станция предупреждения об облучении AN/ALR-20 является панорамным приемником и предназначена для обнаружения излучения потенциально опасных РЭС, их идентификации, выбора приоритетных для противодействия и индикации угроз в кабине бортового оператора РЭБ [227].

Цифровая станция предупреждения об облучении AN/ALR-46 обеспечивает обнаружение излучений РЛС в полосе частот 2–18 ГГц и одновременную идентификацию до 16 РЭС. Самолет B-52 является одним из немногих самолетов, на которых установлена данная станция. В настоящее время существенная модернизация системы не планируется [227].

Станция активных помех ALQ-155 предназначена для создания активных маскирующих шумовых заградительных по частоте помех РЛС обнаружения и наведения, а также управления огнем. Она обеспечивает постановку помех в пределах 360° в азимутальной плоскости в диапазоне 1–10 ГГц. Модернизированная станция ALQ-155(V) включает программное обеспечение и технические решения, позволяющие противодействовать современным угрозам в радиочастотном спектре [227].

Станция активных помех ALQ-172(V)2 обеспечивает обнаружение излучения потенциально опасных РЭС, их идентификацию, выбор приоритетных для противодействия и РЭП. Для обеспечения наиболее полной защиты носителя на самолете B-52 установлено до 3 станций ALQ-172 [227].

В настоящее время в ВВС США ведутся работы по модернизации станций помех, с целью придания больших возможностей по обеспечению ситуационной осведомленности экипажа, в том числе определение местоположения опасных РЭС по их излучению. Продолжаются мероприятия по совершенствованию ПО. Так, разработка нового программного пакета для этих станций ожидалась еще в 2015 г. Руководством ВВС США рассматривается замена станций помех ALQ-172 на более новые системы, такие как AN/ALQ-211 или AN/ALQ-214 [227].

Станция активных помех AN/ALQ-122 обеспечивает обнаружение излучения потенциально опасных РЭС, их идентификацию и выбор приоритетных для РЭП, постановку активных имитирующих помех, уводящих по дальности и угловым координатам. Значительная модернизация станции AN/ALQ-122 не намечается [227].

К другим средствам РЭБ, которые могут быть установлены на борту самолетов B-52, можно отнести станцию активных помех средствам радиосвязи AN/ALT-32 [227].

Все системы и средства РЭБ самолета B-52 функционируют независимо и зачастую решают схожие задачи. Так, станции помех ALQ-155 и ALQ-172 работают в различных частотных диапазонах и имеют различные перечни потенциальных угроз, однако решают одинаковые задачи по РЭП РЛС управления оружием зенитных средств и БРЛС истребителей. В связи с этим основным направлением работ по модернизации комплекса РЭБ для обороны самолета B-52 является создание единой интегрированной системы, куда будут входить функциональные подсистемы: исполнительная, информационного обеспечения и управления [227].

2.4.3.9. Комплекс РЭБ стратегического бомбардировщика B-1B Lancer

Комплекс РЭБ для защиты стратегического бомбардировщика B-1B Lancer включает в себя [227]:

- интегрированную систему РЭП AN/ALQ-161;
- автоматы отстрела дипольных отражателей и тепловых целей AN/ALE-49;
- буксируемые ложные цели AN/ALE-50.

Система РЭП AN/ALQ-161, разработанная специально для самолета B-1B, состоит из 108 съемных модулей на борту самолета. Она обеспечивает в автоматическом режиме (с возможностью управления оператором) обнаружение излучения потенциально опасных РЭС, их идентификацию, выбор приоритета и наиболее эффективных мер противодействия, их РЭП в пределах 360° в азимутальной плоскости [227].

В настоящее время на самолетах B-1B используется модернизированная версия системы ALQ-161A. В этой системе используются устройства запоминания и воспроизведения сигналов, что позволяет создавать сигналоподобные помехи, а сама система имеет расширенный диапазон частот. В 2015–2016 гг. планировалось обновление ее ПО, благодаря чему должны увеличиться быстродействие и производительность этой системы [227].

Основными направлениями развития систем и средств РЭБ самолета B-1B являются обеспечение эффективного противодействия будущим угрозам, унификация оборудования и модульность конструкции. Для модернизации системы РЭБ на борту самолета B-1B рассматривается использование средств РЭП AN/ALQ-211 и AN/ALQ-214 [227].

2.4.3.10. Интегрированная система РЭБ INEWS для самолетов F-22, выполненных с использованием технологий малой заметности

Система INEWS предназначена для обеспечения индивидуальной защиты самолетов малой заметности, выполненных по технологии Stealth, от управляемого ракетного оружия и огня зенитной артиллерии за счет постановки активных и пассивных помех радиолокационным и оптоэлектронным средствам системы ПВО противника. В ее состав включены следующие подсистемы [250]:

- приемник диапазона частот 2–40 ГГц;
- доплеровская РЛС обнаружения и предупреждения о пуске управляемых ракет;
- приемники предупреждения о пусках ракет с многоспектральными чувствительными элементами диапазона 2–5 мкм и 6–20 мкм;
- передатчики помех в диапазонах 2–18 ГГц и 20–40 ГГц;
- устройства выброса противорадиолокационных отражателей;
- ИК-ловушки и ПОИ;
- аппаратура обработки и анализа сигналов;
- управляющий процессор.

Кроме этого, в состав комплекса РЭБ INEWS возможно также включение приемника УФ-диапазона [250].

Система РЭБ INEWS интегрирована в единый комплекс бортового РЭО, поэтому обмен данными между ее элементами осуществляется через общесамолетную цифровую мультиплексную шину. Команды, поступающие от самолетной экспертной системы на автоматическое применение средств радио- и оптоэлектронных средств РЭП, выдаются системе INEWS в ходе выполнения боевых задач [250].

Особенностью разработанной системы РЭБ INEWS является то, что она создана для самолета, использующего технологию Stealth (в частности, для

самолета F-22) и обладающего уменьшенными сигнатурами в радиочастотном и ИК-диапазонах длин волн. При разработке была решена проблема сокращения общей эффективной поверхности рассеяния (ЭПР) приемопередающих фазированных антенн системы INEWS за счет создания комбинированных широкодиапазонных ФАР для приемных устройств, передатчиков помех, а также для доплеровской РЛС [250].

Приемопередающие модули выполнены по технологии МСВЧ, которая позволила создать малогабаритные многолучевые комбинированные ФАР, обеспечивающие перехват сигналов РЭС противника в широком диапазоне частот, а в режиме разделения по времени — излучение оптимальных помех одновременно по 10–15 целям. Снижение заметности в радиочастотном диапазоне достигается за счет адаптации сигналов к складывающейся радиоэлектронной обстановке [250].

В системе INEWS применена более совершенная элементная база на основе сверхскоростных интегральных схем, сверхбольших интегральных схем и МСВЧ интегральных схем, а также высокопроизводительных средств обработки данных, что позволило сократить число адаптируемых параметров сигналов до 8 (несущая частота, мощность излучения помехи, поляризация излучаемых сигналов, период повторения и длительность импульсов, ширина спектра, время и интервал излучения). В интегрированной системе INEWS применено цифровое устройство запоминания радиочастот (DRFM), совмещенное в одном модуле формата SEM-E (Standart Electronics Module E-format) с высокопроизводительным процессором и однополосным цифровым модулятором. Основным достоинством DRFM является его способность обрабатывать сигналы непосредственно на несущей и промежуточной частотах. Также DRFM обладает способностью с высокой точностью восстанавливать спектры сигналов от угрожаемых РЭС при одновременном добавлении спектральных составляющих видов помех в сочетании с использованием схем автоматического контроля когерентности синтезированных сигналов. Применение DRFM позволяет значительно повысить эффективность подавления РЭС противника [250].

Для уменьшения уровня собственных излучений самолета F-22 предусмотрен режим использования преимущественно пассивных средств оповещения о пуске управляемых ракет и расходуемых средств противодействия: отражающих диполей, ИК-ловушек и ПОИ. В этом режиме возрастает роль экспертной системы самолета, которая совместно с пассивными устройствами оповещения о пусках ракет определяет степень угрозы источников излучения и вырабатывает оптимальное решение об использовании тех или иных средств противодействия. Например, оптоэлектронные приемники обнаруживают запуск управляемых ракет «земля — воздух» или «воздух — воздух» по излучению факела двигательной установки ракеты в ИК-диапазоне [250].

При этом в настоящее время для перспективных оптоэлектронных приемников частично разработаны и продолжают разрабатываться мозаичные многоспектральные ИК- и УФ-пеленгаторы, отличительными особенностями которых являются широкий мгновенный угол обзора, высокая разрешающая способность, а также малая вероятность ложной тревоги [250].

Интегрирование всего РЭО осуществляется управляющим процессором параллельной архитектуры, разработанной фирмой «Хьюз» на базе стандартных модулей SEM-E, которые являются основными компоновочными элементами подсистемы обработки данных, их анализа и формирования сигнала помех. Эта подсистема представляет собой вычислительную сеть с распределенной архитектурой, динамически изменяемой в зависимости от решаемых задач. Она объединяет функции обработки и анализа сигналов от всех подсистем, что является качественно новым уровнем интеграции элементов системы РЭБ [250].

Производство и опытная эксплуатация системы INEWS были начаты в 2000 г. До 2014 г. ею предполагалось оснастить все запланированные к выпуску тактические самолеты F-22. При этом стоимость разработки системы INEWS оценивается в 1 млрд долл., а стоимость серийного образца комплекса составляет 6 млн долл. Однако такая высокая стоимость, а также высокая стоимость разработки истребителя F-22 Raptor в целом в условиях финансового кризиса привели к сокращению финансирования как программы разработки F-22, так и авионики для него.

В результате по состоянию на 2011 г. комплект средств РЭБ тактического истребителя F-22 Raptor включает [227]:

- станцию предупреждения об облучении AN/ALR-94, которая обеспечивает обнаружение, идентификацию и определение координат излучающих потенциально опасных РЭС;
- систему предупреждения о ракетной атаке AN/AAR-56, которая позволяет обнаруживать пуски ракет в пределах 360° в азимутальной плоскости, состоит из 6 датчиков, распределенных по бортам самолета, при этом каждый датчик перекрывает сектор в 60°;
- автоматы выброса расходуемых средств РЭБ AN/ALE-52, которые функционируют в автоматическом и управляемом режимах и задействуются при обнаружении факта пуска ракет.

При этом, несмотря на сворачивание программы закупок и модернизации самолетов F-22 в 2011 г., предполагалось, что технические наработки по проекту INEWS будут использованы в процессе модернизации других бортовых авиационных средств РЭБ, находящихся на вооружении, а также при разработке новых систем для оснащения перспективных самолетов и вертолетов [250].

2.4.3.11. Комплекс РЭП AN/ASQ-239 Barracuda для самолета F-35 Lightning II

В состав бортового радиоэлектронного комплекса (РЭК) тактического истребителя F-35 Lightning II, который будет принят на вооружение вместо F-22, будет входить комплекс РЭП AN/ASQ-239 Barracuda. Этот комплекс РЭП является модернизированной версией комплекса РЭБ INEWS тактического истребителя F-22A. Комплекс AN/ASQ-239 Barracuda отличает высокая степень интеграции с другими элементами БРЭО самолета и прежде всего — с его вычислительным комплексом. Это позволяет осуществлять накопление и обработку

данных, которые поступают от различных средств информационного обеспечения, находящихся на борту самолета, а также за его пределами. Это дает возможность выдавать летчику сведения о боевой обстановке с высокой степенью детализации. При этом предполагается, что для постановки помех, прицельных по частоте и угловым координатам, будет использоваться антенная система самолета [227].

Станции предупреждения об облучении для самолета F-35 разрабатываются на основе станции AN/ALR-94 самолета F-22. Кроме того, в состав средств информационного обеспечения будет входить устройство AN/AAQ-37, которое посредством шести ИК-датчиков, распределенных по фюзеляжу, будет выдавать информацию о ракетной угрозе. Устройства выброса предполагается оснастить разрабатываемыми пиропатронами MJU-68 и MJU-69 [227].

Комплекс AN/ASQ-239 Barracuda разрабатывается компанией BAE Systems. Наиболее интересным аспектом разработки этого комплекса, является то, что, судя по официальным релизам компании, в комплексе AN/ASQ-239 Barracuda предполагается реализовать технологию «когнитивной РЭБ» [430].

2.4.3.12. Комплекс индивидуальной защиты летательных аппаратов в оптическом и инфракрасном диапазонах

Результаты анализа боевых действий в Ираке и Афганистане внесли существенные изменения во взгляды руководства ВВС США на применение систем и средств РЭБ. В значительной степени это затронуло вопрос о повышении уровня защищенности вертолетов. Так, на боевых вертолетах и вертолетах обеспечения становится стандартом использование интегрированной системы индивидуальной защиты, включающей в себя [223]:

- систему предупреждения о радиолокационном и лазерном облучении;
- систему предупреждения о пуске ракет;
- системы выброса расходуемых ложных целей радиолокационного и инфракрасного диапазонов;
- станцию помех ИК-диапазона.

Для противодействия угрозам в ИК-диапазоне фирмы США и Великобритании расширили выпуск базовых магний-тефлон-витоновых (MTV) ИК ложных целей, в частности M206 и 118MTV, и перспективных, таких как пирофорные M21L кинематические M2I2 и двухдиапазонные M118. Указанные типы ложных целей в ближайшие несколько лет составят основу индивидуальной защиты вертолетов от портативных зенитных систем, использующих наведение на цель по излучению в ИК-диапазоне [223].

Одним из пожеланий экипажей вертолетов является сокращение количества типов ИК ложных целей за счет повышения степени их универсальности. На текущий момент системы предупреждения не обеспечивают должной идентификации угроз, что влечет за собой одновременное использование ложных целей различных типов [223].

В ВВС таких государств, как США, Великобритания, Израиль и ряда других, на вертолетах устанавливаются лазерные средства противодействия в ИК-диапазоне. За последние 20 лет технологии производства таких систем шагнули

далеко вперед — от использования импульсных ламп до более эффективных и надежных многодиапазонных источников лазерного излучения. Хотя раньше считалось, что лазерные системы полностью заменят ИК ложные цели и устройства их выброса, однако в настоящее время последние продолжают активно использоваться [223].

Основным фактором, стимулирующим развитие авиационных систем и средств противодействия в ИК-диапазоне, является наличие большого количества оружия с тепловыми системами самонаведения. Так, в прошедших локальных военных конфликтах на долю ракет этого класса приходится до 90% всех сбитых летательных аппаратов [223].

К современному поколению систем противодействия ВС США в ИК-диапазоне относятся следующие [223]:

- AN/ALQ-212(V) ATIRCM;
- система оптико-электронного противодействия для самолетов тактической авиации TADIRCM;
- единая система предупреждения о ракетной атаке AN/AAR-57(V) CMWS.

Также широкое распространение получили системы оптико-электронного противодействия AN/AAQ-24 Nemesis и LAIRCM для больших самолетов.

В перспективе это направление будет также развиваться, и особое внимание будет уделено созданию средств обнаружения и предупреждения об атаках ракет с ИК ГСН, а также созданию помех головкам самонаведения в ИК- и УФ-диапазонах волн. Совершенствование систем оптико-электронного противодействия будет идти по пути использования многодиапазонных лазерных установок, а также миниатюризации аппаратной части комплексов противодействия [223, 250].

2.4.4. Ложные воздушные цели

Одними из наиболее эффективных средств РЭБ, которые могут применяться непосредственно в пределах зон поражения зенитных систем противника, являются программируемые автономные ложные воздушные цели (АЛВЦ) со средствами создания активных помех, а также буксируемые ложные цели (ЛЦ) [222, 223].

2.4.4.1. Автономные ложные воздушные цели

Планирующие и имеющие силовую установку АЛВЦ кроме решения задачи отвлечения на себя сил ПВО противника предназначены для постановки различного вида помех: радиолокационных, ИК и комплексных. Для этого они могут оснащаться аппаратурой РЭП, линзами Люнеберга и устройствами отстрела дипольных отражателей и ложных тепловых целей [219].

В целях повышения выживаемости боевых самолетов при выполнении ими боевых задач по прорыву системы ПВО противника путем имитации ЭПР, типовых профилей полета, маневров реальных самолетов, а также для вскрытия системы ПВО противника в США с 1995 г. управлением DARPA и фирмой Teledyne Ryan под руководством ВВС ведется разработка миниатюрной

относительно дешевой АЛВЦ ADM-160B MALD (Miniature Air-Launched Decoy) [219].

АЛВЦ типа MALD представляет собой небольшую ракету, отображение которой на экране РЛС аналогично отметке атакующего самолета, что позволяет отвлечь РЛС на сопровождение АЛВЦ и дополнительно вскрыть ее точное местоположение этой РЛС и ее рабочие параметры [257].

Исходя из этого, основными задачами, возлагаемыми на АЛВЦ MALD в интересах подавления ПВО противника, являются [257]:

- физическое уничтожение цели — использование в качестве противорадиолокационной ракеты;
- ложная атака — использование некоторого количества АЛВЦ MALD для имитации атаки, отвлекая системы и средства ПВО от реальных самолетов, атакующих с другого направления;
- забивание приемных трактов средств обнаружения ПВО ложными целями — задача, аналогичная ложной атаке, целью которой является временная парализация работы систем и средств ПВО.

Предполагается использовать АЛВЦ ADM-160 MALD с самолетов типа B-1B, B-2A, B-52H, F-15, F-16, F-35 и F/A-22, а также с боевых БПЛА. Стратегический бомбардировщик B-52H на внешних подвесках сможет нести до 16 таких АЛВЦ, а истребитель F-16 — 4 АЛВЦ [223].

Аналогом АЛВЦ ADM-160 MALD является ITALD (ADM-14/C), разрабатываемая совместно американской фирмой Northrop Grumman Corporation и израильской IMI для ВМС США. Она предназначена для формирования сигналов, идентичных сигнатурам защищаемой платформы. АЛВЦ ITALD является модернизированной версией использовавшейся в Ираке АЛВЦ TALD (ADM-141). В программу АЛВЦ закладывается траектория полета, а навигационное обеспечение осуществляется посредством системы глобального позиционирования GPS, инерционной системы и радиолокационного высотомера. Принцип использования — «выстрелил и забыл». Состав оборудования РЭП в АЛВЦ может меняться в зависимости от решаемых задач. Возможно применение системы оптико-электронного подавления. Рассматривается вопрос об установке АЛВЦ ITALD в ВВС Великобритании на штурмовиках GR-7/9 Harrier и в ВВС Австралии на истребителях F-18 Hornet. Основными направлениями дальнейшей модернизации АЛВЦ ITALD являются: повышение маневренности, дальности полета и эффективности мероприятий РЭП. Исследуется возможность использования уменьшенной модели этой АЛВЦ на БПЛА [223].

В 2006 г. фирма Raytheon начала разработку еще одного варианта АЛВЦ — постановщика помех ADM-160C MALD-J (Jammer). Она в дополнение к стандартной комплектации будет оснащаться модулями передачи помех и имитации электромагнитной сигнатуры самолета, с которого она запускается, а также линией передачи данных для дистанционного управления АЛВЦ и изменения ее заданий в полете. В марте 2008 г. командование ВВС США заключило контракт стоимостью 80 млн долларов с Raytheon сроком на 2 года на реализацию второго этапа разработки АЛВЦ MALD-J Block 2 [219, 430]. На лето

2015 г. компания Raytheon заключило контракт стоимостью 118,5 млн долларов на поставку в ВВС США разработанных АЛВЦ ADM-160C MALD-J [430].

АЛВЦ MALD/MALD-J применяются автономно в пределах зон поражения средств ПВО. Программируемые АЛВЦ MALD и MALD-J предназначены для групповой защиты летательных аппаратов и автономно управляемого оружия класса «воздух-земля» от средств ПВО путем имитации их ЭПР и параметров полета, отвлечения части сил и вскрытия позиций средств ПВО. Они применяются в воздушном пространстве противника в пределах зон поражения зенитных средств. АЛВЦ MALD-J оснащена станцией ответных помех и имеет возможности по радиоэлектронному подавлению РЛС обнаружения, наведения и целеуказания, а также РЛС управления огнем зенитных средств. Предположительно создаваемые помехи — многократные ответные, уводящие по скорости и дальности. Вследствие малой мощности бортовых передатчиков генерация маскирующих помех малоэффективна. Полезная нагрузка АЛВЦ MALD-J составляет до 13 кг при общей массе 136 кг. Максимальная дальность полета не превышает 900 км [222].

В ВВС носителями АЛВЦ MALD-J являются самолеты F-16C/D, который может нести 4 АЛВЦ, и B-52, который может нести до 16 АЛВЦ. Также рассматривается возможность применения таких целей с борта самолета C-130. ВМС планируют снаряжать MALD-J самолеты F/A-18E/F, EA-18G. На самолетах тактической и стратегической авиации они устанавливаются на внешних подвесках. Применять АЛВЦ с борта C-130 планируется путем их сброса из специального контейнера MCALS (MALD Cargo Air Launched System), перевозимого внутри грузового отсека, через открытую рампу. Одновременно может быть произведен сброс до 100 АЛВЦ [222, 430].

Полет MALD-J осуществляется по заранее программируемым траекториям с коррекцией по данным КРНС NAVSTAR. Одновременно можно запрограммировать до восьми маршрутов, и в каждом задать до 100 промежуточных пунктов маршрута. Пилот перед сбросом АЛВЦ имеет возможность выбрать один из запрограммированных маршрутов. Однако возможность управления ими после их сброса отсутствует [222].

Основными направлениями модернизации АЛВЦ MALD-J являются [222]:

- повышение эффективности средств РЭП путем увеличения мощности передатчика помех и улучшения чувствительности приемной аппаратуры;
- повышение помехозащищенности приемного канала бортовой аппаратуры КРНС NAVSTAR.

2.4.4.2. Буксируемые воздушные цели

Комплексы буксируемых ЛЦ в ближайшие 10–15 лет будут продолжать активно разрабатываться в таких государствах, как США, Германия, Великобритания, Швеция. Мощность сигналов, излучаемых этими целями, может превышать 4 кВт. Одним из факторов, ограничивающих темпы распространения комплексов буксируемых ЛЦ на мировом рынке вооружений, является отсутст-

вие единого стандарта для них. Например, ЛЦ «Ариэль» (Великобритания) и AN/ALE-55 (США) имеют разные массогабаритные параметры, что не позволяет размещать их на одной пусковой установке [223].

Буксируемые с помощью волоконно-оптического кабеля радиолокационные ЛЦ «Ариэль» являются основным средством защиты европейского истребителя EF2000 от моноимпульсных РЛС сопровождения. Используемые ЛЦ не просто обеспечивают повтор принимаемых сигналов. С помощью систем и средств радиоэлектронного обеспечения истребителя угроза обнаруживается, определяется ее местоположение, производится идентификация, и на борту самолета генерируется сигнал подавления. Далее он преобразуется в модулированный лазерный импульс и по кабелю длиной 100 м передается на ЛЦ, оборудованную передатчиком. Мощность излучаемого ЛЦ сигнала регулируется в зависимости от мощности сигнала РЛС и эффективной площади рассеяния самолета, которые изменяются в зависимости от ракурса. Те РЛС, где используется метод сопровождения в процессе сканирования, не способны отличить ложную цель от реальной [223].

Дальнейшее развитие буксируемых с помощью волоконно-оптического кабеля активных ЛЦ связано с реализацией в них возможности переключения диаграммы направленности излучений, коррелированной постановки помех с самолета и буксируемой им ЛЦ [223].

2.4.5. Противорадиолокационные ракеты

Помимо средств постановки помех, к средствам РЭБ индивидуальной защиты самолетов можно отнести противорадиолокационные ракеты, являющиеся разновидностью самонаводящегося на радиоизлучение оружия. Основным преимуществом этих управляемых ракет с пассивными головками самонаведения по сравнению со средствами активных и пассивных помех является то, что они уничтожают или значительно повреждают угрожающие РЭС. Эти ракеты широко применялись и во время войн в Персидском заливе. Ими оснащают самолеты A-6 Intruder, F-4 Phantom II, F-16 Fighting Falcon, F/A-18 Hornet, F-111 Aardvark и Panavia Tornado. Последние их модификации устанавливаются и на БПЛА. Кратко рассмотрим характеристики наиболее известных из них.

AGM-45 Shrike — противорадиолокационная ракета, стоящая на вооружении ВМС США (самолеты F-4, A-4, A-6, A-7 и др.). Ракета также находится на вооружении ВВС Израиля. [250]. Принята на вооружение в 1965 г. Имеет дальность действия порядка 40 км [428].

AGM-78 Standart ARM (Anti-Radar Missile) — противорадиолокационная ракета, стоящая на вооружении ВВС США (самолеты F-105G, F-4G). Находится на вооружении морской авиации самолетов A-6B/E, а также используется ВМС США в качестве оружия класса «корабль — корабль» [250]. Принята на вооружение в 1968 г. Имеет дальность действия порядка 90 км [428].

Наиболее известной по результатам применения в локальных конфликтах является ракета AGM-88 HARM. Эти ракеты были приняты на вооружение ВВС и ВМС США в 1983 г. и уже через 3 года использовались во время операции против Ливии [250].

AGM-88 HARM (High-speed Anti-Radar Missile) — высокоскоростная противорадиолокационная ракета, используемая в ВВС и ВМС США. Разрабатывалась как замена ракетам AGM-45 Shrike и способна наводиться на высокочастотные РЛС с непрерывным излучением. Ракета менее уязвима к традиционным видам помех и к помехе типа выключения РЛС при обнаружении запуска ракеты. Ракета HARM вычисляет местоположение цели и способна ее поразить, даже если РЛС была выключена. Дальность действия — 150 км. Ракета может совершать быстрые развороты на расстоянии 5–8 км от цели и оснащена широкодиапазонным приемником с высокой чувствитель ностью [250].

После принятия на вооружение ведется активная доработка этих противолокационных ракет. В результате было создано несколько их вариантов.

К ракете AGM-88A Block-II была добавлена радиолокационная ГСН, которая могла программироваться для наведения на новые радиолокационные объекты по мере их обнаружения. У ракеты AGM-88B, производившейся с 1987 г., была усовершенствована вычислительная аппаратура и интегрирована радиолокационная ГСН, после чего та получила обозначение AGM-88A Block-II. Модернизация AGM-88B была проведена в 1990 г., после этого ракета получила обозначение AGM-88B Block-III. С 1993 г. стал доступен вариант AGM-88C — у нее был доработан фугасный заряд боевой части, добавлены 12 800 поражающих элементов из вольфрамового сплава для поражения антенны РЛС, а также была усовершенствована система наведения и добавлена функция атаки неплановых целей. Более поздние доработки касались обновления программного обеспечения AGM-88C Block-IV. Были проведены дальнейшие модернизации программного обеспечения, после чего появились варианты AGM-88C Block-V и AGM-88B Block-III [428]. Эти модификации ракеты могут поражать РЛС со сменой рабочих частот [250].

Несмотря на три десятилетия, прошедших с момента первого боевого применения, ракеты семейства AGM-88 не проявляют никаких признаков морального старения. После последней модернизации ракета получила новое обозначение — AGM-88F. В соответствии с этой программой модернизации к существующим возможностям ракет AGM-88C Block-IV добавляется наведение по координатам GPS. Добавление системы GPS позволяет ракете противодействовать так называемой тактике «выключения», когда оператор РЛС, обнаруживший приближающуюся ракету, самонаводящуюся на передачу радиосигналов его станции, останавливает ее работу с целью заставить ракету потерять захваченную цель. Кроме того, новая модификация ракеты может программироваться координатами GPS для обозначения зон, через которые ей не разрешено пролетать, причем эти координаты GPS загружаются в ракету перед пуском. Загрузка этих географических параметров в ракету способствует сокращению сопутствующих потерь [428].

Модернизация AGM-88F выполняется для ВВС США, которые устанавливают AGM-88C Block-IV на борту своих истребителей F-16CJ Viper Weasel SEAD, которые оборудованы системой целеуказания и наведения противорадиолокационных ракет AN/ASQ-213A/R7 HTS.

Оборудование AN/ASQ-213R7 размещается на самолете и решает задачи обнаружения сигналов вражеских РЛС и управляет наведением AGM-88F. Кроме того, оборудование AN/ASQ-213R7 добавляет возможность использования авиационных бомб с комплектами высокоточного наведения, такими как комплект Joint Direct Attack Munition для бомб GBU-31/32/35/38/54. В 2010 г. все пилотируемые самолеты, имеющие на ворружении AGM-88F, были оснащены оборудованием AN/ASQ-213R7 [428].

В 2014 г. начались поставки ракет модификации AGM-88F в ВВС США. В дальнейшем планируется дальнейшая модернизация ракеты AGM-88, которая, по планам ВС США, позволит ракете оставаться на вооружении до 2035 г. [428].

Американские ВМФ проводят собственные исследования по повышению эффективности ракет AGM-88B/C, получившие обозначение AGM-88E AARGM (Advanced Anti-Radiation Guided Missile — перспективная управляемая противорадиолокационная ракета). Возглавила эту программу компания Orbital ATK. Эта новая ракета войдет в комплекс вооружения истребителя итальянских ВВС Tornado-ECR SEAD (в 2016 г. она должна была достичь уровня начальной боевой готовности) и поступит на вооружение американских ВМФ. Ракета AGM-88E войдет в состав вооружения палубных истребителей F-18C/D Hornet и F-18E/F Super Hornet и самолета РЭБ EA-18G Growler. Кроме того, эта ракета также предназначена для вооружения истребителей F-16 и F-15. Для варианта AGM-88E взяты существующий двигатель и корпус ракеты AGM-88B/C, но добавлена новая система наведения, а также улучшена система управления. Что касается системы наведения, то в ее состав входит РЛС миллиметрового диапазона, который используется для идентификации и наведения на конечном участке траектории на РЛС, даже если тот выключен. Еще одной мерой борьбы с «выключением» является установка в ракету приемника GPS дополнительно к радиолокационной ГСН, что позволяет повысить точность и нейтрализовать данную тактику. Обновляемая информация о цели может передаваться с самолета-носителя на ракету AGM-88E посредством встроенного широкополосного приемника Integrated Broadcast System Receiver. Одна из важных особенностей ракеты AGM-88E состоит в том, что она может работать без использования системы целеуказания AN/ASQ-213A/R7 (см. выше), поскольку фактически ракета сама выступает в качестве прицельной системы обнаружения чужих радиосигналов. Производство AGM-88E началось в декабре 2009 г.

Кроме того, ВМФ США финансирует проект ракеты с увеличенной дальностью под обозначением AARGM-ER. Разработка этой ракеты началась в 2016 г. и по графику должна завершиться не позднее 2020 г. При этом предполагается, что ракета AARGM-ER будет совместима с внутренними отсеками вооружения нового истребителя F-35A/B/C Lightning-II.

Также к самонаводящемуся на источник излучения оружию относят крылатые ракеты и управляемые авиабомбы с различными головками самонаведения. Развернутая и подробная информация по этим средствам представлена в работах [245, 250, 251].

2.5. Специализированные авиационные комплексы РЭБ (на примере комплексов ВС США)

2.5.1. Тенденции развития и применения специализированных 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 сомнение 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].

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 РЭБ индивидуальной защиты каждого ЛА, но и наличие специализированных самолетов радиоэлектронной борьбы, предназначенных для групповой защиты групп ЛА, 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 и 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, образованный 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, включающий 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, радиотехнической разведки и подавления РЭС противника.

В настоящее время реализуются 4 основных способа применения авиационных групповых средств РЭБ [222].

1. За пределами воздушного пространства, обороняемого противником (как правило, из зон барражирования).
2. В пределах обороняемого противником воздушного пространства без входа в зоны поражения зенитных средств с известным местоположением их позиций («модифицированное сопровождение» боевых порядков прикрываемых сил).
3. В пределах зон поражения зенитных средств в одном боевом порядке с прикрываемой авиацией («проникающее сопровождение» боевых порядков прикрываемых сил).
4. В пределах зон поражения средств ПВО («автономное применение»).

При этом интеграция всех сил и средств РЭБ в единое информационно-коммуникационное пространство, как предусмотрено программой АЕА, позволяет управлять ресурсами РЭП, осуществлять оптимальное распределение этих средств по объектам подавления в зависимости от обстановки в реальном масштабе времени [222].

Функциональные задачи, возлагаемые на системы и средства РЭБ воздушного базирования, могут быть конкретизированы и сведены в соответствующие 4 группы.

1. Подавление РЭС противника из района барражирования, вне зоны действия его ПВО (сфера ответственности ВВС).
2. Подавление РЛС противника самолетом РЭБ, следующим совместно с ударной группой, в целях ее групповой защиты (сфера ответственности ВМС).

3. Подавление в целях индивидуальной защиты от ракет классов «земля — воздух» и «воздух — воздух» (собственные программы ВВС и ВМС).
4. Подавление РЛС противника с помощью БПЛА путем применения расходуемых маневрирующих ложных целей или боевых БПЛА, способных помимо нанесения высокоточных ударов по системам управления и РЭС противника проводить самостоятельные «радиоэлектронные атаки» (совместные программы ВВС и ВМС).

Как показано в работе [235], опыт локальных войн конца XX — начала XXI в. 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 при сопровождении ударной группы авиации самолетами РЭБ ВМС США EA-6B и EA-18G, 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 способ постановки помех используется для обеспечения живучести специализированных 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 РЛС 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 район нанесения удара по объектам противника.

С конца 1990-х гг. единственным обладателем специализированного воздушного комплекса 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, а также в корпусе морской пехоты [257].

Наличие в ВС США только одного типа специализированного воздушного комплекса РЭБ, ориентированного на подавление систем ПВО, связано с выводом из эксплуатации других самолетов РЭБ, ранее 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 по подавлению РЭС противника. Однако позже это мнение было изменено в связи с постоянным совершенствованием систем и средств ПВО возможного противника. Технология Stealth действительно 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 использовать дополнительные комплексы и системы ПВО. Кроме того, планы ВВС США по укомплектованию к концу текущего десятилетия своего парка преимущественно самолетами Stealth не выдерживаются, что актуализирует развитие 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 начали разработку новых систем, способных решать в полном объеме все возложенные на самолеты РЭБ задачи [257].

Такой совместный подход к разработке 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 систем на формирование требований к ожидаемым результатам их использования. При этом главной задачей становится создание взаимно дополняющих средств, удовлетворяющих потребностям не одного, а сразу нескольких видов ВС и ориентированных на взаимодействие в составе единой многофункциональной сети. Такая сетевая организация воздушных компонентов РЭБ позволит обеспечить перекрытие всего спектра возлагаемых на них задач, и в отдельных случаях допускает дублирование функций в целях гарантированного достижения целей применения [257].

Американскими специалистами считается, что даже обычные боевые самолеты, истребители F/A-22 Raptor, оборудованные РЛС с АФАР типа AN/APG-77(V), истребители F-35A с AN/APG-81(V) 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 г. — на самолет РЭБ, разрабатываемый на базе F-35B [218].

С первой половины 1980-х гг. по настоящее время самолет EC-130H CompassCall остается единственной воздушной платформой в ВВС США, выполняющей 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 CompassCall 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 CompassCall, 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 данные задачи, наряду с задачами групповой зашиты от ПВО, EA-18G Growler будет решать, находясь в боевых порядках авиации [223].

2.5.2. Специализированные авиационные комплексы РЭБ

Рассмотрим более подробно характеристики и боевое применение основных специализированных самолетов РЭБ, стоявших и стоящих на вооружении ВВС и ВМС США.

2.5.2.1. Самолет EF-111A Raven

Самолет РЭБ EF-111A Raven был создан в конце 1970-х гг. на базе бомбардировщика F-111 для ВВС США. Эти самолеты РЭБ обеспечивали выполнение следующих задач:

- сопровождение групп тактических истребителей при нанесении ими ударов за линией фронта с подавлением всех РЛС вдоль маршрута полета;
- создание помех РЛС раннего предупреждения и обзорным РЛС большой дальности действия из безопасных зон, барражирование в которых обеспечивается без дозаправки в воздухе в течение 4,5 ч;
- подавление войсковой ПВО противника вблизи линии боевого соприкосновения при непосредственной поддержке сухопутных войск.

Объектами их радиоэлектронного подавления являлись также бортовые РЛС и средства наведения истребителей. Максимальная дальность подавления — 230 км [95].

Работы над самолетом EF-111A Raven начались в 1972 г., а первые два опытных образца поднялись в воздух спустя 5 лет. За основу самолета компания General Dynamics взяла истребитель-бомбардировщик F-111A. Самолет EF-111A был предназначен для операций вторжения на территорию противника и для сопровождения ударных самолетов. Основу БРЭО самолета EF-111A Raven составляла система постановки помех AN/ALQ-99, на 70% аналогичная той, которая устанавливается на самолетах EA-6B Prowler. Кроме нее EF-111A Raven был оснащен широким набором и других средств РЭБ.

Система групповой защиты самолетов AN/ALQ-99 устанавливалась на самолете РЭБ EF-111A и предназначена для подавления [250]:

- РЛС обнаружения, наведения и целеуказания;
- РЛС сопровождения воздушных целей и наведения ракет ЗРК;
- РЛС самолетов дальнего радиолокационного обнаружения (ДРЛО), линий связи и управления.

В состав системы групповой защиты AN/ALQ-99 входят [250]:

- приемник предупреждения об опасности и наведении управляемых ракет — AN/ALR-62 (диапазон рабочих частот 60–18 000 МГц);
- ИК-приемник — AN/AAR-113;
- станция РЭБ индивидуальной защиты AN/ALQ-137;
- устройства AN/ALE для выброса противорадиолокационных отражателей и ИК-ловушек — (диапазон частот 2,5–10,0 ГГц и длин волн 2–3 и 3–5 мкм);
- система РЭБ групповой защиты самолетов тактической авиации.

Система AN/ALQ-99E прошла два этапа модернизации. После завершения работ по модернизации максимальная дальность подавления источников радиоизлучения составляет 500 км, а практическая — 250 км. Число одновременно подавляемых РЛС — 10–16.

Самолеты EF-111A, оборудованные системой групповой защиты на основе AN/ALQ-99E, принимали участие в обеспечении боевых действий в зоне Персидского залива, показав высокую эффективность подавления РЛС системы ПВО Ирака [250].

Самолет EF-111A отличался высоким уровнем автоматизации — всеми его подсистемами при необходимости может управлять один оператор. Оборудование постановки активных помех частично размещается в отсеке фюзеляжа, который на исходном самолете отводился под вооружение. Самолет EF-111A не имел обычного вооружения, но обладал достаточно высокой скоростью полета, что позволяло ему уходить от истребителей противника и держаться под защитой своих порядков.

В 1998 г. самолеты EF-111A были сняты с вооружения ВВС США.

2.5.2.2. Самолет EA-6B Prowler

Палубный самолет ВМС США EA-6B Prowler — базируется на многоцелевых авианосцах (до 4 на каждом), предназначен для ведения радиоэлектронной борьбы и разведки, решения задач РЭП и огневого поражения корабельных и наземных РЛС, а также срыва работы сетей радиосвязи систем

ПВО противника. При выполнении задач прикрытия корабельных группировок, авиационных ударных групп он обеспечивает эффективную постановку помех РЭС противника на дальности до 250 км. При этом эффективная дальность подавления с высоты 9 км достигает 400 км. Кроме того, он обеспечивает и подавление каналов радиосвязи управления истребителями-перехватчиками противника. Самолеты EA-6B Prowler в основном действуют над морем без захода в зону ПВО противника [95, 219].

Прототипом при создании EA-6B Prowler послужил палубный штурмовик A-6 Intruder. При создании машины была увеличена длина фюзеляжа, за счет чего был увеличен экипаж. Также 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 4 человек — пилота и троих офицеров-операторов систем РЭБ. Когда EA-6B Prowler был принят на вооружение, на нём установили тактическую систему постановки помех, способную подавлять сигналы сразу 5 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 следующим направлениям:

- была 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 была 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, всё большее значение в перечне решаемых самолетом EA-6B задач придается подавлению связных РЭС, 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 за EA-18 Growler. Самолеты EA-6B Prowler планируются к выводу из эксплуатации к 2020 г. [222].

2.5.2.3. Самолет EC-130H CompassCall

Особая роль в информационных операциях с участием ВВС отводится специализированному постановщику помех системам связи и управления противника EC-130H CompassCall, действующему из так называемых «безопасных зон» района барражирования, находящихся за пределами зоны поражения ЗРК противника [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.

Самолет 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 EC-130H предназначен для подавления радиоканалов управления истребителей-перехватчиков противника, бортовых и наземных средств навигации и опознавания. Типовая схема применения предусматривает барражирование самолетов EC-130H 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 EC-130H CompassCall составляет автоматизированный комплекс РЭП Rivet Fire. 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 по 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 [219, 250].

Аппаратура системы РЭП самолета EC-130H CompassCall непрерывно совершенствуется, при этом основное внимание уделяется разработке новых алгоритмов анализа радиопередач и управления подавлением, а также повышению точности пеленгования. Основным направлением модернизации аппаратуры РЭБ этого самолета является повышение уровня ее автоматизации.

Командование ВВС США в интересах расширения возможностей по радиоэлектронному подавлению на ТВД с 2001 г. проводит очередную модернизацию самолета РЭП EC-130H CompassCall, находящегося на вооружении с 1982 г. [219].

Проводимая модернизация предусматривает оснащение самолета более совершенными РЭС в интересах расширения существующих и приобретения принципиально новых возможностей. Программой модернизации самолетов EC-130H 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 увеличит возможности по ведению РЭБ на ТВД [257].

При этом рассматриваются следующие дополнительные задачи, возлагаемые на самолеты EC-130H CompassCall после модернизации [219, 223]:

- радиоэлектронное подавление систем коротковолновой, радиорелейной и спутниковой связи военного и государственного управления;
- радиоэлектронное подавление радиосетей управления тактической авиацией, управления комплексами ПВО, современных помехозащищенных систем радиосвязи и передачи данных оперативно-тактического звена сухопутных войск;
- радиоэлектронное подавление гражданских и коммерческих систем подвижной сотовой и транкинговой радиосвязи;
- радиоэлектронное подавление 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 ВТО классов «воздух — земля» и «земля — земля».

Таким образом, в ходе модернизации самолета EC-130H расширяются его возможности — от подавлений сетей систем управления военного назначения до подавления сетей сотовой связи, которые могут использоваться террористическими группировками.

В ходе модернизации на самолете EC-130H производится [218, 219]:

- замена аналоговой радиоприемной аппаратуры и распределения частот подавления новой цифровой перепрограммируемой аппаратурой РЭП TRACS (Tactical Radio Acquisition and Countermeasures Subsystem);
- установка новой аппаратуры технического анализа и средств вычислительной техники;

- установка двух контейнеров с принципиально новой аппаратурой радиоэлектронного подавления УКВ-средств радиосвязи и навигации — SPEAR (Special Purpose Emitter ARray), которая позволяет излучать сигналы помех в диапазоне 0,03–3 ГГц по 4 независимым лепесткам диаграммы направленности антенны, используя 144 дискретных передающих элемента;
- установка терминала системы передачи данных Link-16.

В конце 2006 г. была завершена разработка аппаратуры и видов помех для подавления РЛС ПВО, функционирующих в МВ- и ДМВ-диапазонах длин волн. В течение 2007 г. намечалось проведение работ по обеспечению возможности РЭП перспективных помехозащищенных систем радиосвязи и средств радиолокации [219].

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 CompassCall и самолета РРТР RC-135V/W Rivet Joint. При этом высокоскоростной обмен данными в реальном масштабе времени между ними будет производиться с помощью терминалов системы Link-16, что позволит совместно с самолетом RC-135V/W вести высокоточную разведку и определение местоположения систем и средств радиосвязи противника [219].

Новый вариант самолета EC-130H CompassCall будет более эффективно решать задачи РЭП современных мобильных средств радиосвязи, систем ПВО противника, а также может выдавать в реальном масштабе времени данные по целеуказанию на огневое поражение [219].

По планам командования ВВС США всего планируется иметь на вооружении 12–15 модернизированных самолетов EC-130H CompassCall, которые могут эксплуатироваться еще не менее 10–15 лет. Предполагается, что эти самолеты будут находиться на вооружении до 2025 г. [219, 223].

2.5.2.4. Самолет EA-18G Growler

Палубный самолет РЭБ EA-18G Growler — был разработан фирмой Boeing на базе истребителя F/A-18F Super Hornet для ВМС США. Первый полет совершил 15 августа 2006 г. Серийное производство самолета началось в 2007 г. На флоте EA-18G заменит устаревшие самолеты EA-6B Prowler.

В декабре 2003 г. ВМС заключили контракт стоимостью 979 млн долл. с фирмой Boeing на переоборудование 6 палубных истребителей F/A-18F Super Hornet в вариант специализированного палубного самолета РЭБ EA-18G Growler. Основным отличием новой машины (вариант EA-18G Block 1) от базового образца F/A-18F Super Hornet стало расширение состава бортового РЭО за счет установки современной аппаратуры РЭБ, разработанной в рамках программы ICAP III при модернизации самолета РЭБ EA-6B Prowler [219].

Самолет РЭБ EA-18G Growler ВМС США предназначен для огневого поражения и радиоэлектронного подавления наземных и корабельных РЛС, а также 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 следующие компоненты [218, 219, 223]:

- станцию радиотехнической разведки AN/ALQ-218(V)2;
- 3 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 спутниковой связи MATT;
- 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 (4 цветных дисплея размером 20–25 см на каждом месте).

Помимо указанного БРЭО в состав вооружения EA-18G включены 2 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 концевиках 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 открытым данным результатов лабораторных испытаний), масса аппаратуры 224 кг [218, 219].

Станция активных помех средствам радиолокации AN/ALQ-99F(V) предназначена для постановки помех бортовым РЛС и управляемым ракетам противника, а также для обеспечения групповой защиты боевых порядков самолетов от средств ПВО.

В состав каждого из трех подвесных контейнеров станции активных помех AN/ALQ-99F(V) входят следующие элементы [218]:

- 2 антенные системы (передней полусферы и задней полусферы);
- 2 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 (диапазоны 1/2/3: 64–500 МГц; диапазон 4: 500–1000 МГц; диапазоны 5/6: 1000–2500 МГц; диапазон 7: 2500–4000 МГц; диапазон 8: 4000–7500 МГц; диапазоны 9/10: 7500–40 000 МГц) в разных комбинациях. В зависимости от этого масса контейнера колеблется от 460 кг (при установке двух передатчиков диапазона4) до 494 кг (при наличии двух передатчиков диапазона 9/10). Кроме того, для постановки помех используется антенная система РЛС AN/APG-79 [218]. В перспективных планах модернизации комплекса РЭБ на самолете EA-18G Growler предусмотрена замена станции AN/ALQ-99F(V) на систему NGJ [430].

Вместо станции помех связным РЭС AN/USQ-113, которая используется на самолете EA-6B, на самолете EA-18G устанавливается станция AN/ALQ-227. Ее основу составляют приемное устройство CCSR (Communication Countermeasures Set Receiver) и процессорный блок. Станция AN/ALQ-227 представляет собой отдельный приемник, а не приемник с передатчиками помех, как AN/USQ-113. Для излучения сигналов помех используется передатчик контейнерной станции помех РЛС УКВ-диапазона ALQ-99(V). При этом в передатчиках новой контейнерной станции постановки помех вместо ламп бегущей волны используются твердотельные элементы. Кроме этого, она будет связана с двумя антенными устройствами, что позволяет 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. В период до 2013–2015 гг. ВМС США планировали приобрести около 90 самолетов EA-18G Growler [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 использоваться 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 средств ПВО и ГСН управляемых ракет [222].

2.5.2.5. Перспективный комплекс РЭБ CCJ для самолета B-52H

В 2007 г. ВВС США в целях повышения эффективности борьбы с современными средствами разведки и управления систем ПВО противника возобновили программу создания нового комплекса РЭБ — CCJ (Core Component Jammer), размещаемого на борту стратегического бомбардировщика B-52H Stratofortress, для постановки помех наземным РЛС дальнего обнаружения воздушных целей в составе систем ПВО противника. Данные самолеты получат обозначение EB-52 или B-52 CCJ. Они сохранят свои возможности по применению ядерного и высокоточного обычного оружия, а также смогут решать широкий круг задач РЭБ с помощью многофункциональной аппаратуры радиоэлектронной разведки и постановки помех при длительном патрулировании (до 12 ч) на удаленных ТВД [219].

Комплекс РЭБ CCJ предполагается размещать в двух контейнерах (длина 9,1–12,2 м, масса около 2300 кг), устанавливаемых на узлах подвески внешних топливных баков самолета [219].

Аппаратура комплекса CCJ будет обеспечивать: обнаружение, распознавание, определение местоположения и подавление современных и перспективных РЛС в диапазоне частот 70–40 000 МГц и срыв работы сетей радиосвязи систем ПВО противника в диапазоне 20–2000 МГц. Комплекс сможет осуществлять эффективную постановку помех одновременно нескольким десяткам РЭС противника на дальностях до 400 км в секторе 180°. Предусмотрена постановка широкополосных (заградительных), прицельных по частоте и сопряженных по спектру, а также ответных и дезинформирующих (уводящих по углу места, дальности, скорости) помех [219].

При создании комплекса CCJ в качестве основы использована аппаратура, разработанная в рамках программы модернизации самолета РЭБ EA-6B Prowler. Отличительной особенностью новых станций помех является использование АФАР (длина каждой антенной решетки более 2,5 м, работает в X и Y частотных диапазонах), формирующей многолучевую диаграмму направленности. Данная АФАР создана на базе решетки, установленной в контейнере SPEAR самолета EC-103H CompassCall. Применение такой антенны позволит формировать мощную узконаправленную помеху в заданном направлении перпендикулярно маршруту полета самолета. Мощность потребляемой комплексом CCJ электроэнергии составит до 60 кВт при возможностях энергетической установки самолета 100 кВт [219].

В дополнение к комплексу РЭБ CCJ предполагалось часть основного вооружения (крылатые ракеты воздушного базирования (КРВБ), управляемые ракеты класса «воздух — земля») самолета B-52H оснащать боевыми частями, создающими мощный электромагнитный импульс, в том числе СВЧ-диапазона, для вывода из строя РЭС противника (в первую очередь электронно-вычислительной техники), а также использовать автономные ложные воздушные цели ADM-160B MALD с аппаратурой постановки помех РЛС [219].

В июне 2008 г. командование ВВС США заключило контракты стоимостью 15 и 20,8 млн долларов на предварительные исследования по эскизному проектированию комплекса РЭБ CCJ, перспективных технологий и элементов для него (передающие АФАР, имеющие высокую мощность излучения, усовершенствованные широкополосные возбудители и приемные устройства) и его интеграции в самолет B-52H. По состоянию на начало 2009 г. был создан макет подсистемы обработки и управления комплексом РЭБ AMMP (AEA Mission Management Processing) и проведены его испытания в лабораторных условиях [219].

Несмотря на активную разработку комплекса CCJ и создание демонстрационной платформы, в 2009 г. эта программа была снова закрыта. После этого ВВС США сделали акцент на использование менее дорогих вариантов, предусматривающих применение систем и средств РЭБ непосредственно в районе решения боевых задач [222, 223].

2.5.2.6. Перспективная система РЭП NGJ для самолета F-35B

После закрытия программы CCJ по разработке специализированного самолета РЭБ на основе стратегического бомбардировщика B-52 самолет EC-130H является единственным носителем многофункционального комплекса РЭБ, ориентированного 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 комплексов 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 опытного образца;
- испытания в лабораторных условиях;
- разработка специального ПО.

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 программы NGJ. 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 диапазон» (18–40 ГГц), в котором функционируют РЛС управления огнем ряда современных и перспективных ЗРК, ГСН, а также 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 нитрид-галлиевые 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 турбин 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 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 DRFM, предназначенных для сохранения и воспроизведения сигналов, а также новых алгоритмов их обработки.

Появление системы NGJ позволит США осуществить значительный технологический прорыв в области создания средств РЭБ. Система NGJ может стать основой для разработки других средств РЭБ различного назначения и базирования [222].

В зарубежных СМИ отмечается, что станцией активных помех, разрабатываемой по программе NGJ, планируется оснащать самолет F-35B. Этот 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, позволит успешно решать весь комплекс задач по обеспечению действий военной авиации [222].

По состоянию на апрель 2016 г. компания Raytheon заявила о поставке 15 опытных образцов системы NGJ американскому ВМФ в течение следующих 4 лет в рамках контракта на 1 млрд долларов [430].

2.5.3 Перспективы использования систем 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 и отсутствия летного состава позволяет использовать его в самых опасных районах боевых действий, а также устанавливать на него дополнительное вооружение. 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, систему РТР LR-100, оптико-электронный комплекс Skyball, телевизионную и ИК-аппаратуру и др.), мощное бомбовое и ракетное вооружение. Рассматриваются варианты, в соответствии с которыми 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 Surveil-

lance 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), радиовзрыватели мин. Успешная апробация комплекса NERO показала возможность применения средств РЭБ на БПЛА, с учетом решения задач его автономного полета и управления, а также задач электромагнитной совместимости комплекса РЭБ и радиоканалов управления БПЛА [221].

Назначением БПЛА, оснащенных комплексами РЭБ, является решение следующих задач:

- 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 радио- и радиотехническая разведка, 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 подавление РЭС 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 [249].

Все существующие и разрабатываемые БПЛА подразделяются на 3 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 эффективными 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 радиоэлектрон-

ной 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 [249].

Отдельно необходимо отметить маневрирующие автономные ложные воздушные цели. Они представляют собой летательные аппараты, отображающие на экране РЛС метку, идентичную отметке атакующего самолета. Корпус ложных воздушных целей выполнен из композиционных материалов. В ее состав входит миниатюрная станция РЭБ, генерирующая помехи для РЛС противника, что затрудняет захват и сопровождение атакующих средства ПВО самолетов. Маневрирующие автономные ложные воздушные цели, оборудованные средствами РЭБ, в перспективе должны найти самое широкое применение [249].

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 возможностей 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 [249].

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 [249].

Необходимо отметить влияние уровня развития вычислительной техники на возможности по созданию высокоэффективных БПЛА РЭБ. Вычислительные средства, используемые на таких БПЛА, предназначены в первую очередь для следующих функций [249]:

- 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, разработанных 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. Однако предполагается, что необходимый уровень при отсутствии качественных скачков в развитии вычислительной техники может быть достигнут не ранее 2025–2030 гг. [249].

Обобщая вышесказанное, можно утверждать, что в ближайшем будущем комплексы РЭБ на основе БПЛА вытеснят и заменят специализированные самолеты РЭБ. Однако для этого разработчикам систем и средств РЭБ для БПЛА необходимо решить следующие основные задачи технического и тактического характера [249].

- Определение оптимальной дистанции для эффективного проведения радиоэлектронных атак 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, самонаводящимися на излучение ракетами).
- Обеспечение устойчивой связи с удаленными абонентами во время проведения радиоэлектронных атак (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 запрограммировать 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 успешности 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.

В настоящее время ведутся активные исследования по созданию комплексов РЭБ на БПЛА. Так, для задач РЭБ может быть использован создаваемый в США специализированный ударный БПЛА X-45A (разрабатывается по

программе UCAV), выполненный из композиционного материала по технологии малой заметности Stealth. Взлетная масса этого БПЛА 6800 кг, и на его борту устанавливается разнообразная разведывательная аппаратура (РЛС с ФАР, станция РТР, оптико-электронная аппаратура и др.) [257].

В интересах ВМС США ведется разработка БПЛА Pegas с базированием на авианосцах. В его тактические задачи входят: разведка, наблюдение, удары по морским и наземным целям, подавление ПВО противника [257].

Решение задач РЭБ с помощью БПЛА прежде всего направлено на подавление РЛС противника, а также его систем управления и связи. Для этого первоначально планировалось использовать два вида средств: автономные ложные воздушные цели типа ADM-160 MALD и специально оборудованные БПЛА. Под последними подразумевалось использовать разрабатываемые в ВВС и ВМС США боевые БПЛА, оснащенные соответствующим оборудованием РЭБ. Однако между ВВС и ВМС, которые работали отдельно по концепции БПЛА РЭБ, возникли существенные разногласия. Для их разрешения программы по БПЛА РЭБ этих двух ведомств в октябре 2003 г. были объединены и переданы под централизованное управление DARPA [223].

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 связи 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 БПЛА, способные нести полезную нагрузку, состав которой варьируется от средств физического уничтожения цели до средств РЭП. При этом делается акцент не на создании новых пилотируемых платформ, а на модификации существующих с максимально возможным сохранением их первоначальных тактико-технических характеристик и вооружения.

2.6. Наземные средства радиоэлектронной борьбы

Как показано в работах [258–261], основным воинским формированием, которое решает задачи радиоразведки и радиоэлектронной борьбы в США, являются батальоны разведки и РЭБ мотопехотных и бронетанковых дивизий, ко-

торые 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.

2.6.1. Современные наземные средства РЭБ

2.6.1.1. Наземная станция РЭП КВ- и УКВ-радиосвязи AN/TLQ-17A (V)1 Traffic Jam

Наземная станция радиоэлектронного подавления КВ- и УКВ-радиосвязи AN/TLQ-17A (V)1 Traffic Jam обеспечивает ведение радиоразведки в диапазоне 1,5–80 МГц и постановку радиопомех в диапазоне 20–80 МГц.

В составе станции радиоразведки и радиоподавления имеются:

- радиоприемник РРТР — 2107/TLQ-17A диапазона 1,5–80 МГц;
- радиопередатчик РЭП — 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 радиопомех размещается на 0,25 т автомобиле повышенной проходимости М-151А1/А2, прицепе М-416, М-569.

2.6.1.2. Вертолетный комплекс радиоразведки и РЭП AN/ALQ-151(V)2 Quick Fix II

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 себя [213, 214]:

- радиоприемник радиоперехвата R-2017/U в диапазоне 20–150 МГц;
- приемопеленгатор AN/ALQ-151 в диапазоне 1,5–80 МГц;
- станцию радиопомех AN/TLQ-27A 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 (3 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 [213, 214].

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 [213, 214].

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 [214].

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. Однако в связи со сворачиванием программы IEWCS комплекс AN/ALQ-151(V)3 эксплуатируется как самостоятельный вертолетный компонент РЭБ [213].

2.6.1.3. Комплекс разведки и РЭБ IEWCS

Модернизация систем РРТР и РЭБ сухопутных войск США началась в начале 90-х гг. XX в. с замены морально устаревших станций и комплексов, разработанных в основном для борьбы с аналоговыми средствами связи и передачи данных ВС Советского Союза [215].

Станции AN/TSQ-138 Trailblazer, AN/TLQ-17 Traffic Jam, AN/TRQ-32 Teammate и ряд других, а также переносные средства РРТР и РЭБ на то время были довольно эффективными. Вместе с тем расширение рабочего диапазона частот в принимаемых на вооружение перспективных системах связи, применение современных способов обработки и передачи сообщений, появление новых протоколов, отвечающих за маршрутизацию и передачу сообщений, и другие инновации стали причиной начала НИОКР по созданию перспективных средств разведки и РЭБ, отвечающих современным требованиям [215].

Совершенствование системы разведки и РЭБ сухопутных войск США происходило в направлении разработки перспективных комплексов по программе «Единые средства разведки и радиоэлектронной войны» (РЭВ) — IEWCS.

В комплекс датчиков IEWCS входят три подсистемы с общими радиоэлектронными модулями [215, 229, 250]:

- универсальный датчик наземного базирования для «тяжелых» дивизий GBCS-H, в качестве которого будет использоваться система EFVS;

- универсальный датчик наземного базирования для «легких» дивизий GBCS-L, размещенный на многоцелевой колесной машине высокой проходимости;
- усовершенствованная система РРТР AN/ALQ-151(V)3 Advanced Quick Fix, устанавливаемая на вертолете ЕН-60 или на самолете.

Кроме того, по программе IEWCS разрабатывались различные средства РРТР и РЭБ воздушного базирования на самолетах и БПЛА, которые интегрировались с вышеуказанными датчиками (GBCS-H, GBCS-L, Advanced Quick Fix) в единую сетецентрическую среду. Подробно проект IEWCS рассмотрен в работе [229].

Вместе с тем в процессе доводочных и эксплуатационных испытаний первых образцов комплекса IEWCS были выявлены серьезные недостатки. Так, испытываемые образцы аппаратуры не обеспечивали требуемой точности определения местоположения объектов и целей разведки. Более того, в связи с несовершенством антенной системы и устанавливаемого программного обеспечения невозможно было провести испытания с использованием всего частотного диапазона. При этом в ходе проверки ревизионной комиссией министерства обороны США были обнаружены серьезные недостатки как в руководстве и управлении, так и в реализации всей программы разработки. По заключению комиссии, на проектирование и разработку комплекса ушло 9 лет, израсходовано более 902 млн долларов, при этом было выпущено всего 12 комплектов аппаратуры для пехотных дивизий, и те исключают возможность проведения радиоэлектронных атак РЭС противника. В результате в 1998 г. программа была признана неудачной и закрыта [215].

2.6.1.4. Мобильная система РЭБ EFVS

Мобильная система РЭБ 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 системы IEWCS [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. К таким дополняющим системам можно отнести [250]:

- тактическую систему AN/MLQ-34 TACJAM, размещаемую на гусеничном шасси M1015 и предназначенную для постановки помех средствам связи в ОВЧ-диапазоне;
- систему AN/TLQ-17A Traffic Jam, устанавливаемую на грузовой автомашине и предназначенную для обнаружения средств связи ВЧ-, ОВЧ- и УВЧ-диапазонов и создания для них помех;
- систему перехвата сигналов радиосвязи и их анализа AN/TRQ-32 Teammate, размещаемую в аппаратной кабине машины M1028;
- систему обнаружения и идентификации РЛС противника AN/MSQ-103 Team Pack, устанавливаемую на шасси M1015;
- систему перехвата сигналов средств связи и пеленгации их источников AN/TSQ-114 Trailblazer, также устанавливаемую на шасси M1015.

2.6.1.5. Воздушно-наземный комплекс разведки и РЭБ AN/MLQ-40 Prophet

В основу структурно-схемных решений системы Prophet положены наработки по программе IEWCS, которая после 9 лет реализации была закрыта. Также, 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 [216].

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 [215].

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 трех подсистем:

1. подсистема управления и контроля;
2. воздушная подсистема;
3. наземная подсистема.

Подсистема управления и контроля. С помощью нее осуществляются 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 органами дивизионного звена управления (группой анализа и управления, бригадной группы анализа и управления ASAS, а также позволяет использовать комплекс Prophet в качестве удаленной станции разведки системы ASAS. При этом планируется объединить подсистему контроля Prophet с перспективной системой сбора, обработки и распределения разведывательной информации сухопутных войск DCGS-A [215, 216].

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 высокую надежность и эффективную защиту этой подсистемы, раздельное базирование, работу в движении и непрерывность функционирования при передислокации [215, 216].

Воздушная подсистема обеспечивает радио- и радиотехническую разведку, а также радиоэлектронное подавление формирований, находящихся на удалении 15–20 км от переднего края района боевых действий. В качестве носителей средств этой подсистемы выступают вертолет EH-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 [215, 216].

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 м выдвижной мачте. Время развертывания станции составляет 2 мин [215].

Последняя модификация наземных станций AN/MLQ-40(V)3 может функционировать в трех вариантах: стационарно с 6 м 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. Экипаж новой станции составляет 4 человека, а имеющиеся запасы продовольствия, снаряжения и топлива, обеспечивают автономную работу в течение 72 ч. 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. В состав первого рабочего места входит переносной компьютер, позволяющий подключаться к приемнику-анализатору MD-405A и отображать данные радиоэлектронной обстановки на площади 150×120 км, формировать базу данных источников радиоэлектронного излучения, принимать и получать информацию от центров управления и командных постов, а также организовывать взаимодействие с другими станциями. Основу второго рабочего места составляет приемник-анализатор MD-405A, который является самым важным элементом переносной станции. Третье рабочее место включает в себя аппаратуру определения точного местоположения для обеспечения функционирования станции в движении и аппаратуру связи SINCGARS (Single Channel Ground and Airborne Radio System). 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 [215].

Планами командования сухопутных войск предусматривалось, что комплекс Prophet будет функционировать как составная часть системы FCS, в составе 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 [215].

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 ProphetBlock 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., представляют собой многофункциональные разведывательные комплексы с акустическими, инфракрасными и радиолокационными датчиками [215].

Полностью развернутый наземный комплекс будет состоять из пяти машин: двух машин РРТР и РЭБ, двух машин специальной технической разведки и одной машины управления [215].

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 огневыми средствами, осуществлять радиоэлектронное подавление средств связи, радиолокации и сигналов КРНС противника, подготавливать точные данные об излучающих объектах на поле боя, обеспечивать защиту своих войск. Данный комплекс будет обладать необходимой в современных условиях боевой обстановки универсальностью и мобильностью, что позволит быстро перебрасывать его в районы предназначения [215].

2.6.2. Перспективные наземные средства РЭБ

В конце XX в. под влиянием концепции сетецентрического управления в ВС США начали прорабатываться проекты построения децентрализованных многоэшелонированных систем разведки и РЭБ. При этом наибольших успехов в данном 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. А 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. Таким образом, современное развитие наземных средств РЭБ США происходит под влиянием опыта применения сухопутных войск в локальных конфликтах, в которых они участвовали на рубеже XX–XXI вв. в Ираке и Афганистане.

Рассмотрим наиболее интересные проекты конца XX века и современные тенденции развития наземных средств РЭБ.

2.6.2.1. Наземный сетецентрической комплекс РЭБ Wolf Pack

В США в конце 90-х гг. XX в. были начаты работы по созданию принципиально новых децентрализованных комплексов РЭБ для сухопутных войск. Заказчиком нового комплекса выступило управление DARPA. В соответствии с проектом, получившим наименование Wolf Pack, в результате НИОКР должно быть создан комплекс РРТР и РЭП основанный на сетецентрических принципах

управления и ориентированный против тактических средств управления и связи противника, [220].

Необходимость создания такого комплекса, по мнению американских военных специалистов, обусловлена следующими основными причинами.

Во-первых, состоящие на вооружении комплексы РЭБ, осуществляющие подавление РЭС противника, находясь в боевых порядках войск, создают при этом помехи также своим системам и средствам управления и связи.

Во-вторых, основными тенденциями развития систем радиосвязи в тактическом звене в настоящее время являются применение метода передачи с коммутацией пакетов и переход к работе с пониженными уровнями мощности излучений передающих средств, а в средствах радиолокации — всё более широкое использование сигналов повышенной скрытности (с очень малой длительностью излучения, расширенным спектром и изменением несущей частоты от импульса к импульсу и т. д.).

В состав комплекса Wolf Pack входят управляющая станция и комплект распределенных на местности автономных малогабаритных приемопередающих устройств (МППУ), интегрированных в единую сеть. Эта сеть имеет открытую архитектуру построения, что позволит в последующем осуществлять ее модернизацию как на аппаратном, так и на программном уровне [220].

Управляющая станция в сети решает задачи централизованного сбора данных о радиоэлектронной обстановке в реальном масштабе времени, контроля работоспособности и дистанционного перепрограммирования режимов работы МППУ в зависимости от обстановки и приоритетности выполнения задач [220].

Комплект автономных МППУ осуществляет автоматический высокоскоростной анализ спектра в диапазоне 20–15 000 МГц, перехват сигналов средств радиосвязи и РЛС противника, в том числе повышенной скрытности, их идентификацию и определение местоположения на участке местности площадью до 100×100 км, а также создает оптимальные по мощности и виду радиоэлектронные помехи. Планируется, что мгновенная полоса обзора комплекса Wolf Pack будет не менее 2,5 ГГц, разрешающая способность — не хуже 1 кГц, а скорость поиска в разведываемом диапазоне составит 3000 ГГц/с [220].

Количество МППУ в комплекте определяется спецификой источников радиоизлучений противника и их предполагаемого расположения на местности. МППУ имеют открытую модульную архитектуру построения и малые массогабаритные характеристики (менее 1,4 кг и 570 см) и обеспечивают непрерывную работу [220]:

- в режиме ожидания — до 60 сут.;
- в режиме радиомониторинга — до 10 сут.;
- в режиме постановки активных радиопомех — 5–10 ч.

Предусматривается использование МППУ в непосредственной близости от объектов воздействия (от 100 до 1000 м) с принятием мер защиты на аппаратном и программном уровнях в случае несанкционированного захвата этих устройств противником и попыткой использования их в своих целях [220].

Основные достоинства комплекса Wolf Pack [220]:

- высокая эффективность вскрытия радиоэлектронной обстановки;
- оптимальное подавление линий радиосвязи и комплексов ПВО противника целенаправленными маломощными помехами без задействования традиционных мощных средств РЭП;
- возможность использования комплекса в режиме противодействия средствам РРТР противника при ведении ими разведки систем связи и управления.

При решении задач вскрытия и отслеживания изменений радиоэлектронной обстановки на заданном участке местности комплекс Wolf Pack обеспечивает [220]:

- перехват сигналов типовых средств радиосвязи (20–15 000 МГц) и радиолокации (в диапазоне 100–15 000 МГц);
- классификацию и идентификацию (при скорости ППРЧ 1400 и более скачков в секунду) сигналов всех известных РЭС;
- определение менее чем за 2 с местонахождения радиостанций и РЛС противника с круговой вероятной ошибкой не более 10 м при условии установки МППУ на удалении 3–5 км от источников радиоизлучения.

Проработано несколько сценариев развертывания комплекса Wolf Pack в зависимости от оперативно-тактической обстановки. Например, когда предполагается, что противник в скором времени будет действовать на участке местности (в том числе в городских условиях), который в настоящий момент находится под контролем своих сил, установка МППУ должна осуществляться аналогично тому, как формируется минное поле. В других случаях, когда местность контролируется противником, доставка МППУ в районы предназначения будет производиться пилотируемыми летательными аппаратами и БПЛА, разведывательно-диверсионными группами или высокоточными артиллерийскими снарядами. Предпочтительными местами установки МППУ являются деревья, холмы, естественные и искусственные возвышенности, то есть места, с которых обеспечивается хорошее прохождение радиоволн. При этом для эффективной работы комплекса требуется проведение предварительной разведки РЭС противника и местности, где будут расположены МППУ [220].

При решении задачи подавления средств радиосвязи и ПВО противника предполагается три варианта боевого применения комплекса Wolf Pack [220].

1. В случае, когда имеется минимальная информация о местонахождении объекта подавления на местности, осуществляется так называемая «всеобъемлющая атака». При этом задействуются все постановщики помех вблизи предполагаемого района нахождения РЭС противника. Помеха ставится на его рабочей частоте, и МППУ работают автономно с максимальной мощностью излучения.
2. При наличии данных о местонахождении объекта подавления и прямой его радиовидимости комплекс задействуется в режиме «направленной атаки». В таком случае постановщики помех работают в сети и с пониженной мощностью излучения.

3. При точном знании местонахождения подавляемого РЭС и его режимов работы, а также наличия прямой радиовидимости используется режим «точной атаки». При этом задействуется одно или несколько МППУ в режиме постановки помехи относительно малой мощности.

Решение задачи подавления средств ПВО противника будет осуществляться комплексом Wolf Pack путем обнаружения, идентификации, определения местоположения РЛС и постановки им, а также линиями радиоуправления пусковыми установками оптимальных по типу и мощности радиопомех. Формирование и излучение сигналов помех производятся одним или несколькими МППУ, расположенными наиболее близко от объектов подавления. При применении комплекса Wolf Pack для радиоэлектронной защиты своих систем связи и управления от радиоэлектронной разведки противника предполагается размещать МППУ вблизи его средств РРТР и обеспечить их функционирование в режиме постановки шумовых или дезинформирующих помех [220].

При этом, по расчетам разработчиков, любой из вышеприведенных вариантов боевого применения комплекса Wolf Pack будет создавать более эффективные помехи в сравнении с традиционными средствами РЭП [220].

Анализ сценариев боевого применения, состоящих на вооружении американских сухопутных войск, комплексов РЭП в интересах обоснования ТТХ комплекса Wolf Pack показал следующее. Самолет РЭБ EA-6B Prowler при подавлении РЭС противника на удалении 400 км создает помеховый сигнал его приемным устройствам с уровнем мощности, не превышающим 1 Вт. При этом в радиусе около 20 км от самолета будут создаваться помехи с уровнем мощности более 400 Вт. Наземная типовая станция РЭП для подавления работы радиолинии (мощность сигнала около 50 Вт) между объектами противника, удаленными от нее на расстояние до 50 км, должна создавать помеху с уровнем мощности более 50 кВт. При этом в обоих случаях эффективная работа своих средств связи и управления практически будет невозможна. В то же время одно МППУ комплекса Wolf Pack при размещении от объектов подавления на удалении до 1 км обеспечивает эффективное решение этой задачи постановкой помехи с уровнем мощности менее 10 Вт [220].

Разработка комплекса Wolf Pack велось в несколько этапов. Тактико-техническое обоснование облика комплекса было завершено в 2004 г. А опытная эксплуатация и решение о серийном производстве комплекса планировалось на 2006 г. [220].

В 2000-х гг. американское военно-политическое руководство рассматривало принятие на вооружение подразделений сухопутных войск комплекса Wolf Pack в качестве одного из важных элементов реализации сетецентрической концепции в РЭБ, а также как перенос акцента с традиционных форм воздействия на противника к противоборству в информационно-интеллектуальной области путем завоевания превосходства благодаря установлению полного контроля за функционированием РЭС, используемых противником в системах управления и связи [220].

Однако практика боевых действий в Ираке и Афганистане, где сухопутные войска США столкнулись с массовым применением радиоуправляемых само-

дельных взрывных устройств, внесла коррективы в планы развития наземных систем РЭБ.

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 [228].

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.

2.6.2.2. Интегрированная система электронной войны IEWS

Интегрированная система электронной войны 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 [230].

Система IEWS включает в себя 3 подсистемы [230]:

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 территориально-распределенной группировки средств РЭБ наземного и воздушного базирования. Кроме того, большое внимание уделяется разработке новых маломощных режимов излучения помех при совместном использовании различных средств РЭБ [230, 231].

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 выше-

указанных 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 РЭС 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 [230, 231].

Комплекс радиоэлектронной защиты DEA основан на разработках, выполненных по программе Duke, и обеспечивает защиту мобильных сил и средств, 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 [230, 232].

Таким образом, развитие современных наземных средств РЭБ ведется по пути интеграции разнородных наземных систем в единые территориально распределенные 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.

2.7. Функциональное поражение радиоэлектронных средств электромагнитным излучением

2.7.1. Общие принципы функционального поражения радиоэлектронных средств электромагнитным излучением

Функциональное радиоэлектронное поражение электромагнитным излучением (ЭМИ) — функциональное поражение РЭС, заключающееся в разрушении и/или повреждении элементов РЭС 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 подавления являются физические принципы нанесения 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 электромагнитными полями (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 РЭС 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 и материалом полупроводникового элемента.

Мощности ЭМИ, формируемых известными средствами функционального радиоэлектронного поражения, могут превышать десятки ГВт, 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.

Перечень типовых нарушений работоспособности радио- и электротехнического оборудования РЭС при их эксплуатации в условиях воздействия ЭМИ приведен в таблице 2.4 [252, 253].

Таблица 2.4 — Типовые нарушения работоспособности радио- и электротехнического оборудования РЭС при воздействии ЭМИ [14]

Тип устройства	Характер нарушения	Причина нарушения
1. Антенно-фидерные устройства	- отказ антенного коммутатора; - пробой изоляции антенны, излучателя и кабельной системы фидера; - выход из строя входных устройств приемника и выходных устройств передатчика. Все нарушения в основном носят необратимый характер	- появление перенапряжений в АФУ; - низкая электрическая прочность входной элементной базы
2. Приемные и передающие устройства, генераторы синусоидальных сигналов и сигналов специальной формы	- обратимые изменения электрического режима СВЧ-генераторов; - временное увеличение коэффициента шума, изменение коэффициента шума, частоты и мощности генерируемых сигналов; - сбои, выдача ложных импульсов и подавление полезных сигналов	- превышение по амплитуде полезных сигналов наводками; - перекрытие спектров полезных сигналов спектрами помеховых наводок; - высокая чувствительность полупроводниковых элементов
3. Устройства управления, стабилизации и формирования команд	- сбои в структуре команд; - выдача ложных команд по разрядам кодовых групп; - уменьшение амплитуды полезных сигналов; - ложные срабатывания при обработке команд, их исполнении и отработке	- наложение импульсов помех в цепях устройств на формируемые полезные сигналы и их суперпозиция во времени
4. Линейные усилители	- выход из строя входных и выходных цепей; - искажение формы входных (выходных) сигналов и появление ложных сигналов; - самовозбуждение	- появление перенапряжений в линиях связи; - низкая электрическая прочность входных элементов усилителей; - изменение тока поджига защитных разрядников

Тип устройства	Характер нарушения	Причина нарушения
5. ЭВМ и цифровые системы автоматики и управления	- сбои в работе, нарушение нормального хода программ; - потери информации в регистрах оперативной памяти; - ошибки и искажения вводимой и получаемой информации	- наводки во внешних и внутренних цепях и схемах; - выход из строя систем ввода и вывода информации
6. Источники питания	- выход из строя первичных и вторичных источников электропитания; - значительные амплитудные изменения выходного напряжения первичных источников и временное пропадание выходного напряжения вторичных источников питания	- перенапряжение в питающих ЛЭП; - срабатывание линейной защиты и скачки тока и напряжения в питающих линиях; - наводки по цепям питания и системам заземления; - низкая электрическая прочность элементов преобразования

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 поражением ЭМИ практически не зависит от функционального назначения поражаемых РЭС.

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 индивидуальных устройств защиты собственных РЭС от мощного ЭМИ);
- негативное воздействие мощного ЭМИ на биологические объекты.

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 порядка 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 [233, 236].

Таблица 2.5 — 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
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
Электромагнитная бомба – взрывомагнитный генератор (ВМГ)	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

Перспективность электромагнитного 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 нелетальное, 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.

Более подробные сведения о функциональном поражении на основе ЭМИ представлены в работах [233, 236, 245, 248, 251].

2.7.2. 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 электромагнитным волнам СВЧ-диапазона довольно часто применяется обобщенное понятие «микроволновое излучение», 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 высокоэнергоемкие 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 уста-

новка 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.

В таблицах 2.6 и 2.7 приведены энергетические уровни поражения некоторых элементов, блоков и узлов радиоэлектронной аппаратуры (РЭА).

Таблица 2.6 — Энергетические уровни поражения элементов РЭС при воздействии СВЧ-импульсов [250]

Тип прибора	**Энергия повреждения, мкДж**
СВЧ-диоды	0,1 – 10
Интегральные схемы	0,1 – 300
Цифровые интегральные схемы	80
Полевые транзисторы	10
Маломощные транзисторы	$1\cdot10^4 – 3\cdot10^4$
Транзисторы средней и большой мощности	$400 – 4\cdot10^4$
Выпрямительные диоды	$100 – 4\cdot10^5$
Быстродействующие переключающие диоды	20
Туннельные диоды	500
Кремниевые тиристоры	3000
Низкочастотные транзисторы	–

Таблица 2.7 — Уровни функционального поражения некоторых блоков и узлов РЭС при воздействии импульсного СВЧ-излучения [250]

Тип изделия	**Плотность потока энергии, Вт/см^2**	**Поток энергии, Дж/см^2**	**Длительность импульса, с**	**Частота следования импульсов, кГц**	**Длительность воздействия, с**
Усилители системы управления	10 – 40	$10^{-2} – 4\cdot10^{-2}$	10^{-3}	–	–
Узлы системы управления на ИС и БИС	70 – 600	$0{,}7\cdot10^{-2} – 6\cdot10^{-2}$	10^{-6}	1	1
Элементы радиопередатчиков	$10^4 – 10^5$	$10^{-3} – 10^{-4}$	10^{-7}	–	–
Радиоприемники через антенну с $S_{эфф}$ = 1–2 м^2	1 – 100	$10^{-5} – 10^{-6}$	10^{-7}	–	–
Телевизионные системы на видиконах (повреждение видеоусилителя)	$3\cdot10^3 – 5\cdot10^3$	0,6–2	$2\cdot10^{-4} – 4\cdot10^{-4}$	–	–

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. ВМГ 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.

В таблице 2.8 приведены некоторые характеристики нескольких типов мощных СВЧ-генераторов миллиметрового и сантиметрового диапазонов волн [250].

Таблица 2.8 — Характеристики некоторых мощных СВЧ-генераторов миллиметрового и сантиметрового диапазонов волн [250]

Тип генератора	**Частота, ГГц**	**Длительность импульса**	**Выходная мощность**	**КПД, %**	**Примечание**
Гиратрон с импульсным соленоидом, обладающий стабилизируемым носителем энергии	500	2 мкс	Более 100 кВт		Эксперимент
Тиратрон с высокой эффективностью моды TE_{031}	140	2 мкс	100 кВт	30	Эксперимент
Тиратрон с резонаторами моды TE_{031}	100	–	1000 кВт	–	–
Виркатор	До 40	3–5 нс	до 1 ГВт	–	–
Релятивистский гиратрон	35	55 нс	0,2 ГВг	–	Разработан
Взрывомагнитный генератор	–	1 мкс	10^{10} кВт	–	Разработан в Лос-Аламосе

Как видно из таблицы 2.8, наиболее короткие импульсы достигаются в виркаторах, а наибольшая выходная мощность реализуется во взрывомагнитных генераторах. 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 [250].

Наибольший эффект от использования СВЧ-оружия предполагается достигнуть за счет воздействия на РЭС противника критически важной военной и государственной инфраструктуры. 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 ВС, а также министерством энергетики.

Разрабатываемое в США СВЧ-оружие относится к [14]:

- тактическому (наземные, корабельные и авиационные комплексы);
- стратегическому (наземный комплекс противокосмической обороны).

Основные направления НИОКР по СВЧ-оружию, проводимых в интересах армии 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.

По виду базирования СВЧ-оружие можно классифицировать [14]:

- забрасываемые средства (СВЧ-генератор используется вместо обычного взрывчатого вещества на ракетах, снарядах и авиабомбах) однократного (невозвращаемые) или многократного применения (возвращаемые);
- стационарные и мобильные СВЧ-установки, устанавливаемые на различных носителях (автомобиль, самолет, танк и т. д.), многократного применения.

По типу первичного источника энергии СВЧ-комплексы можно классифицировать [14]:

- обычные;
- взрывные.

В части забрасываемых СВЧ-средств 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 основе 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 [233, 236, 245, 248, 251].

2.7.3. 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 РЭС и системы электроснабжения. По механизму воздействия это излучение подобно ЭМИ ядерного взрыва [338].

Современные средства функционального поражения условно можно классифицировать следующим образом [250]:

- мобильные;
- одноразового действия;
- 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; массу 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 операции, 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 РЭС. В результате взрыва специального заряда этой бомбы образовался мощный электромагнитный импульс, действие которого нарушило работу телецентра. Во время этой же операции ВМС США для подавления РЭС управления и связи Ирака использовали в нескольких из запущенных ракет Tomahawk боевые части, создающие мощный ЭМИ. Применяемая в ракете боевая часть 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 доста-

точно 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 ВМГ, устанавливаемым в корпусе осколочно-фугасной боевой частью Мк84 калибра 2000 фунтов. Для крылатых ракет воздушного базирования и управляемых ракет класса «воздух — земля» разрабатываются специальные боевые части, создающие мощный ЭМИ. 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 мощности. 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 Boeing контракт, предусматривавший разработку в течение 3 лет в рамках проекта CHAMP (Counter-electronic High Power Microwave Advanced Missile Project) демонстрационного образца нелетального СВЧ-оружия, размещаемого на борту крылатой ракеты, либо на другой воздушной платформе. Это СВЧ-оружие предназначено для подавления РЭС противника без нанесения им физических повреждений. Основу этого оружия составляют перезаряжаемые емкостные накопители, а также генераторы с АФАР и электронным управлением лучом [237].

Фирма Boeing разрабатывает крылатую ракету воздушного базирования большой дальности и управляемые бомбы серии JDAM-ER с перспективными СВЧ-боевыми частями, а фирма Raytheon — 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 ЭМИ 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 «ЭМИ-выстрелов», и протестировать ее [237].

Особое место среди СВЧ-систем занимает СВЧ-боеприпас, поражающее воздействие которого на РЭС 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 такого СВЧ-боеприпаса положены способы преобразования кинетической энергии взрыва, горения и электрической энергии постоянного тока в энергию электромагнитного поля высокой мощности [237].

В ВМС США также имеются на вооружении экспериментальные ракеты, неядерные боевые 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 [237].

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, а также 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 для 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 ВМС 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].

Специалисты ВС США планируют оснастить АФАР тактические истребители, а также стратегические бомбардировщики. Ряд американских 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 Vigilant Eagle 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, 237].

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 Vigilant Eagle 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, 237].

2.7.4. Особенности функционального поражения лазерным излучением

Лазер, являющийся оптическим квантовым генератором, способен формировать сильное ЭМИ в оптическом диапазоне волн с высокой плотностью энергии (средняя выходная мощность лазера более 20 кВт) в весьма узком телесном угле. Свойство очень узкой направленности луча и высокая энергетическая плотность излучения позволяют в принципе применять лазер в качестве средства функционального поражения радио- и оптико-электронных средств управления войсками и оружием [245, 300].

Атмосфера прозрачна для лазерного излучения в диапазоне длин волн 0,3–1 мкм. Это несколько шире видимой области. Лазеры способны генерировать ЭМИ в широком оптическом диапазоне, однако как средства функционального поражения практический интерес представляют оптические кванто-

вые генераторы, работающие в так называемых «окнах прозрачности» атмосферы, которым соответствуют волны оптического диапазона λ = 0,5–2 мкм, за исключением «непрозрачных» участков λ = 0,95; 1,15; 1,3–1,5 мкм [245].

В ИК-диапазоне тоже есть «окна прозрачности», где отсутствуют линии молекулярного поглощения различных атмосферных газов и аэрозольных примесей. Однако для длин волн менее 0,3 мкм атмосфера абсолютно непрозрачна. Но даже в диапазоне прозрачности атмосферы лазерный луч рассеивается в облаках, в тумане, на аэрозолях и пылинках [245].

Из всего многообразия лазеров наиболее целесообразными к использованию в качестве лазерного оружия считаются твердотельные, химические, со свободными электронами, рентгеновские лазеры с ядерной накачкой и др. [300]. Обобщенные характеристики лазерных устройств приведены в таблице 2.9.

Таблица 2.9 — Обобщенные характеристики лазерных устройств

Активная среда	Длина волны, мкм	Энергия импульса, Дж	Длительность импульса, с	Диаметр луча на выходе, мм
Рубин	0,69	300	10^{-3}	6
Стекло с ниодимом	1,06	150	10^{-3}	6
Полупроводник	0,84	10^{-4}	–	
Газовая He+Ne	1,15	$2 \cdot 10^{-2}$	Непрерывный режим	10

Сформированное лазером ЭМИ обладает высокой степенью пространственно-временной когерентности. Временная когерентность поля достигает значения $\tau_{ког} \approx 0{,}1$ с, благодаря чему удается получить сигнал с узким спектром ($f \approx 10$ Гц) [245].

Высокая степень пространственной когерентности позволяет с помощью простых оптических устройств концентрировать энергию лазера в весьма узком телесном угле. Эта способность лазера позволяет при сравнительно небольшой энергии излучения на выходе оптической системы даже на больших расстояниях до подавляемого РЭС формировать ЭМИ с плотностью, энергии которой достаточно для достижения эффекта функционального поражения некоторых оптико- и радиоэлектронных устройств на значительных расстояниях (около 10 км). Однако вследствие весьма малого сечения лазерного луча (0,2–0,8 м^2) на расстоянии от 20 км и выше возникает проблема точного наведения луча на цель [245].

Можно выделить два механизма функционального поражения радио- и оптико-электронных средств лазерным оружием [245]:

1. непосредственное поражение электронных приборов путем прямого воздействия сильного узконаправленного лазерного ЭМИ;
2. выведение из строя объекта за счет вторичного индуцированного излучения плазмы, порождаемой взаимодействием сильного электромагнитного поля и твердого вещества (например, материала обтекателя антенны). В этом случае возможно обратимое (временное) пора-

жение РЭС, которое через некоторое время восстанавливает свои функции.

Кроме того, лазерные лучи деструктивно воздействуют на поверхностный слой материала цели, в результате они могут разрушить тонкостенные оболочки тепловым или ударным воздействием. В этом случае 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 признаков в виде огня, дыма, звука, высокой точностью, прямолинейностью распространения и практически мгновенным действием [245, 300].

Вышеуказанные поражающие свойства лазерного излучения предопределили их широкое использование для оптико-электронного подавления ИК-систем управления оружием, а также систем наведения и целеуказания. При этом основным фактором, стимулирующим развитие средств противодействия в ИК-диапазоне на основе лазерного излучения, является широкое распространение оружия с ИК ГСН. Так, в локальных военных конфликтах конца XX — начала XXI в. на долю управляемых ракет с ИК ГСН приходится до 90% всех сбитых летательных аппаратов [223].

Эффективность комплексов оптико-электронного подавления и поражения может быть значительно повышена при использовании в их составе станций помех на основе лазеров, так как они позволяют генерировать помехи с высокой плотностью энергии.

Воздействие когерентных лазерных помех на ИК-датчики ГСН управляемых ракет вызывает значительные ошибки в измеряемых ими информационных параметрах, а при большой плотности энергии — приводит к выходу из строя ГСН.

Можно отметить следующие основные способы подавления оптико-электронных систем противника, ориентированные на противодействие вооружению (прежде всего — управляемым ракетам) с ИК-датчиками наведения и целеуказания [245]:

- механическое повреждение элементов ИК ГСН;
- создание плазмы на обтекателе ракеты;
- засветка (ослепление) ИК ГСН;
- воздействие на систему автоматической регулировки усиления ИК ГСН.

Воздействие лазерного излучения с большими плотностями энергии на элементы ИК ГСН приводит к их механическому повреждению. Наиболее уязвимыми элементами при этом являются модулирующие диски, фотоприемники и спектральные фильтры [248].

Одним из основных элементов ИК ГСН, подвергающихся лазерному излучению, является фотоприемник. Рассмотрение воздействия излучения большой мощности на фотоприемники основывается на процессах взаимодействия лазерного излучения с полупроводниками, из которых изготавливают приемники излучения ИК ГСН. Экспериментальные исследования показали, что при плотности энергии лазерного излучения $5 \cdot 10^{-3}$–10^{-2} Дж/см^2 и длительности импульсов 0,3 с температура наружной поверхности фильтра на площади, куда попало излучение, превышает температуру плавления его поверхностного слоя. При плотностях энергии импульсного лазерного излучения на входном зрачке ИК ГСН порядка 10^{-2} Дж/см^2 происходит быстрый нагрев приемника излучения до высокой температуры. Такие уровни облучения могут быть созданы лазерным источником с энергией излучения в импульсе 200–300 Дж на дальностях 5 км [251].

Разрушение элементов ИК ГСН требует создания лазеров с большой мощностью излучения, что приводит к увеличению массы и габаритов лазерного устройства создания помех.

При облучении обтекателей управляемых ракет с ИК ГСН лазерным излучением с плотностью мощности порядка 10 Вт/см^2 вблизи поверхности обтекателя возникает мощное плазменное образование, являющееся источником некогерентного оптического излучения. При использовании импульсного лазера, обеспечивающего попадание на приемник излучения ИК ГСН от плазмы энергии порядка 2–4 Дж в диапазоне 2–5 мкм, может происходить нарушение работоспособности ИК ГСН [248].

Влияние таких высоких энергий на приемники излучения (поликристаллические фоторезисторы на основе PbS с германиевыми фильтрами и монокристаллические фоторезисторы на основе InSb с кремниевыми фильтрами) исследовалось экспериментально. Под влиянием излучения плазмы сопротивление фоторезисторов изменяется, что приводит к резкому уменьшению коэффициента передачи входного каскада ИК ГСН, а при попадании на приемник излучения лазерной энергии порядка 3 Дж — к полному его «ослеплению». Процесс изменения сопротивления фоторезисторов, как подтвердили эксперименты, является обратимым. Однако восстановление свойств фоторезисторов происходит через десятки секунд и более, что с учетом скоростей процесса наведения управляемой ракеты на цель можно интерпретировать как выход ИК ГСН из строя [248].

Помимо так называемого «силового» воздействия, для которого требуется большая энергия излучения, с помощью лазеров можно вводить помеховые сигналы в контур управления ракеты и обеспечить срыв слежения ИК ГСН за защищаемым объектом. Характерными помеховыми воздействиями для подавления ИК ГСН с помощью импульсных лазеров являются [245]:

- создание помех на частоте сканирования (прицельные и заградительные помехи);
- возбуждение переходных процессов в контуре слежения ИК ГСН;

- нарушение работоспособности вследствие воздействия прерывистых помех на систему автоматической регулировки усиления (для ИК ГСН с автоматической фокусировкой матрицы (АФМ)).

Наименьшие требования к мощности лазера, обеспечивающего введение помехового сигнала в контур управления ракеты, предъявляются в том случае, когда длина волны излучения лазера попадает в область спектральной чувствительности приемника излучения ИК ГСН. В настоящее время для этих целей разработаны твердотельные и газовые химические лазеры на молекулах водорода, фтора, дейтерия и хлора.

Среди общих преимуществ лазерного оружия военные специалисты отмечают огромную концентрацию энергии на единице площади, практически мгновенное поражение объекта на недостижимых для других видов оружия дальностях, высокую избирательность поражения. При этом лазерные боевые комплексы могут быть наземного, морского, воздушного и космического базирования с различной мощностью, дальностью действия, скорострельностью и боезапасом. Объектами поражения таких комплексов могут быть живая сила противника, его оптические системы, летательные аппараты и ракеты различных типов [95, 300].

Более подробная общетеоретическая информация о методах и способах функционального поражения лазерным излучением представлена в работах [245, 248, 251].

2.7.5. Средства функционального поражения лазерным излучением (на примере средств ВС США)

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» — программы «Стратегической оборонной инициативы (СОИ)». Один из самых известных достижений в этой области — 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 вместить только 6 химических

модулей COIL общей мощностью 6 МВт, вместо запланированных 14 МВт. 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 является катастрофическим. Тем более что на борту находятся еще и емкости с жидким кислородом. Второй барьер — плавление линз и, как следствие, расфокусировка луча лазера. Температура при излучении лазера такова, что кварцевое стекло не выдерживает. В результате в июне 2009 г. Пентагон прекратил финансирование проекта «Воздушный лазер» (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 три лазера: лазер TILL (Track Illuminator Laser), который предназначен для обнаружения и сопровождения (подсветки) цели, а также для корректировки параметров оптической системы, с помощью которого будет осуществляться поражение цели; второй — лазер BILL (Beacon Illuminator), используемый для компенсации атмосферных искажений, 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 уничтожить ракету 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 основные 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 созданного Northrop Grumman Corporation «Морского лазера-демонстратора» MLD (Maritime Laser Demonstrator). 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 Paul Foster — выведенного из боевого состава эсминца типа Spruance. В пресс-релизе по итогам тестирования сообщалось, что впервые боевая лазерная система для корабля была интегрирована с его РЛС 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 предпочтение отдается лазерам на свободных электронах FEL (Free Electron Laser). Считается, что они лишены недостатков 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 БПЛА 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 гг. [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 гг. для борьбы с небольшими БПЛА и ракетами на расстоянии в 1,5–2 км, а в 2014 г. — против моторных лодок [136].

Определенные успехи в создании компактных лазерных систем побудили США вновь вернуться к разработке этих систем устанавливаемых на воздушной платформе. В 2017 г. ВС США объявило конкурс на разработку БПЛА способного нести лазерное вооружение и предназначенного для решения задач ПРО путем поражения МБР на этапе их разгона после пуска. Компания Northrop Grumman уже заявила, что планирует для решения этой задачи модернизировать свой БПЛА RQ-4 Global Hawk. При создании БПЛА с лазерным вооружением предполагается задействовать наработки полученные в ходе более ранних программы создания лазерного оружия воздушного базирования [431].

Корпорация Boeing в кооперации с британским подразделением европейского консорциума BAE System создала 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 «Фарнборо-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 шестью 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. Ведется разработка установки 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 такого 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 течении трех лет планируется довести его 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 10 импульсов мощностью по 150 кВт между перезаряжанием, которое займет 3 мин. Компания проектирует контейнер массой 1360 кг, в котором разместится лазерная установка и в 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 м^3. 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 [217].

В ноябре 2011 г. в Швейцарии немецкая компания Rheinmetall продемонстрировала перехват БПЛА 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 80 000 ч, 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 работают разведывательные оптико-

электронные приборы и ГСН 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].

2.8. Перспективы и тенденции развития систем и средств РЭБ

2.8.1. Общие перспективы развития систем и средств РЭБ

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, но даже 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].

В конце XX столетия в ряде стран НАТО и США были проведены многочисленные модернизации авиационных комплексов РЭБ, находящихся на вооружении, разработан ряд новых средств, а также способов РЭБ. В результате проведенных исследований были созданы средства РЭБ, которые обеспечили возможность подавления когерентных РЛС (импульсно-доплеровских со сжатием импульсов, с другими видами частотного и фазового кодирования), а также РЛС с моноимпульсным излучением [250].

Из достаточно широкого круга задач, стоящих перед современными комплексами РЭБ, можно выделить задачи, определяющие ряд их принципиальных особенностей [238, 248]:

- «жесткая» целесообразность перекрытия диапазонов работы всех РЛС обнаружения, целеуказания, управления оружием, а также РЭС связи и навигации;
- функциональная необходимость одновременного выполнения большого количества сложных задач — прием и высокоточный анализ сигналов РЭС, определение их координат, типа, режима работы и степени опасности, подавление нескольких РЭС, взаимодействие с другими комплексами (прежде всего РРТР и огневого поражения).

Указанные задачи определяют принципиальные особенности построения перспективных средств и комплексов РЭБ [238, 248]:

- сверхширокополосность радиотехнической части аппаратуры (более 3 октав);
- необходимость реализации параллельной сигнальной обработки принимаемых радиотехнических сигналов в мгновенной полосе частот, равной нескольким гигагерцам;
- максимальное увеличение функциональной плотности исполнения аппаратуры для снижения ее массогабаритных показателей и обеспечения возможности ее системной интеграции;
- предельная унификация базовых цифровых элементов аппаратуры, позволяющая снизить себестоимость, облегчить процессы модификации и модернизации аппаратуры.

Указанные особенности перспективной аппаратуры средств и комплексов РЭБ определяют целесообразность ее построения на основе цифровых сверхширокополосных устройств сигнальной обработки, позволяющих в максимальной степени реализовать приведенные выше особенности и дополнительно получить возможность быстрой реструктуризации аппаратуры обработки путем перезаписи проектов сигнальной обработки в программируемых логических интегральных схемах (ПЛИС) [248].

Таким образом, перспектива развития систем и средств РЭБ тесно связана с применением новейших информационных технологий, которые должны обеспечить желаемую эффективность в условиях качественно меняющихся требований к средствам и методам ведения боевых действий. Так, в перспективных системах РЭБ предполагается осуществление функциональной и аппаратурной интеграции бортового радиоэлектронного оборудования (БРЭО) со средствами РЭП и с системами обнаружения, использующими другие физические принципы функционирования (оптико-электронное оборудование, ИК- и УФ-системы и др.). С разработкой интегрированных бортовых систем усложняется разветвленная логика переключения режимов интегрированных подсистем, что позволяет воздействовать на этот процесс с помощью так называемых алгоритмических воздействий. Кроме того, несмотря на бурное развитие цифровой техники, узким местом всегда будут оставаться объем памяти и быстродействие бортовых вычислительных систем, что также позволит производить

алгоритмические воздействия с целью информационной перегрузки бортовых процессоров [250].

Таким образом, развитие техники РЭБ в значительной степени определяется двумя взаимосвязанными научно-технологическими направлениями развития элементной базы современной радиоэлектроники [245]:

1. созданием высокоскоростных процессоров и вычислительных систем с последних достижений микроэлектроники;
2. расширением возможностей цифровой обработки сигналов, обеспечивших преобразование совокупности средств РЭБ в высокоскоростные цифровые системы.

В 70-х гг. прошлого века самолет, летящий на высоте 12 км, облучался примерно 40 000 импульсами в секунду. В 80-х гг. плотность облучения возросла до 1–2 млн импульсов в секунду, а в начале нынешнего века прогнозируется увеличение этой плотности до 10–20 млн импульсов в секунду [245]. Справиться с селекцией, фильтрацией и анализом поступающей информации в этих условиях может только специализированный цифровой процессор. Для примера укажем, что станция активных помех ALQ-135 (V) для самолетов F-15 имеет 20 параллельно работающих процессоров [245]. Именно высокое быстродействие способно обеспечить адекватную реакцию средств и систем РЭБ на быстро меняющуюся радиоэлектронную обстановку на ТВД.

Таблица 2.10 — Требования к БЦВМ, решающим задачи РЭБ [248]

Каналы поступления данных для обработки	Требования к БЦВМ		
	Производительность, опер./с	Емкость ОЗУ, Мбайт	Емкость ПЗУ, Мбайт
РЭБ	50 млн	> 500	1
РЭР	1 млрд	50	1
Опознавание	10 млн	40	1
БРЛС	40 млн	1600	1

Комплекс РЭБ, функционирующий в современных условиях, должен практически мгновенно реагировать на внезапно возникающие угрозы. Реакция комплекса на угрозу не должна превышать 0,05–0,1 с. Только цифровые ЭВМ с высоким быстродействием и большим объемом памяти способны управлять ресурсами комплексов РЭБ, включающими [245]:

- совокупность станций активных помех;
- расходуемые средства создания помех (буксируемые активные ловушки; противорадиолокационные управляемые ракеты; передатчики помех одноразового действия; дипольные отражатели, подсвечиваемые помеховым сигналом; снаряды с электромагнитной боевой частью);
- набор видов помех и способов их боевого применения;
- средства функционального поражения РЭС (СВЧ и лазерное оружие функционального поражения);
- распределение энергетического потенциала станций активных помех для одновременного подавления нескольких РЭС;

- способность быстрого изменения ориентации и ширины лучей диаграммы направленности антенн (фазированных антенных решеток) станций активных помех в заданных секторах пространства;
- способность управления последовательностью временных интервалов создания помех нескольким РЭС одной ведущей станцией активных помех.

При этом существует тенденция объединения многочисленных радиотехнических и оптико-электронных средств (средств радиолокации, РЭБ, госопознавания, радионавигации, передачи данных, лазерных, ИК- и других датчиков информации), размещенных на одном носителе (летательном аппарате) в единый интегрированный радиоэлектронный комплекс [245].

Среди имеющихся проблем создания перспективных средств и систем РЭБ можно выделить три группы, отличающиеся содержанием и технологиями их решения [238]:

- энергетические;
- информационные;
- функциональные.

Сущность энергетических проблем заключается в сложности реализации требуемых энергетических характеристик комплексов РЭБ при заданных ограничениях (по массе, габаритам, энергопотреблению) и существующей элементной базе. Одним из основных путей их решения является применение АФАР, имеющих высокий коэффициент усиления. Принципиальными особенностями построения АФАР для аппаратуры РЭБ являются [240]:

- возможность адаптивного управления формой диаграммы направленности антенны для реализации различных режимов работы и формирования «провалов» в направлении на источники активных помех;
- расширенная в 7–8 раз полоса рабочих частот (30–40% от центральной частоты для АФАР и 5–6% — для ФАР);
- повышенная в 15–20 раз мощность излучения, снимаемая с одинаковой апертуры;
- необходимость одновременного формирования нескольких независимых лучей для обслуживания пространственно-разнесенных объектов воздействия;
- существенно сниженные потери (до 15–17 дБ) при обработке сигнала;
- конформость и малая величина ЭПР;
- высокая надежность (среднее время наработки на отказ сравнимо со сроком службы самолета).

Использование АФАР в составе комплексов РЭБ при наличии соответствующей элементной базы (мощных полупроводниковых СВЧ-усилителей и переключателей) позволяют получить энергетический потенциал практически любого уровня. Расчеты показывают, что в ближайшее время при наличии соответствующей электронной компонентной базы может быть создана станция активных помех с энергетическим потенциалом до 10^{10} Вт [240].

Проблемы информационного характера обусловлены тем, что технические характеристики существующей системы радиоэлектронной разведки зачас-

тую не позволяют организовать на должном уровне информационное обеспечение систем и средств РЭБ. Прежде всего это относится к достоверности определения объектов воздействия и назначения им соответствующих приоритетов обслуживания при функционировании в сложной, динамично меняющейся радиоэлектронной обстановке [248].

Решение этой проблемы видится в переводе большинства составных частей аппаратуры радиоэлектронной разведки на цифровую обработку. В настоящее время прорабатываются возможности повышения эффективности технологии быстродействующей цифровой аппаратуры РЭБ на базе ПЛИС с переходом на этапе серийного производства на специализированные СБИС типа «система на кристалле». Актуальным представляется разработка быстродействующих АЦП и ЦАП с тактовыми частотами 1 ГГц и выше, а также разрядностью в 12–14 разрядов [248].

Функциональные проблемы прежде всего связаны с необходимостью одновременного (квазиодновременного) подавления РЭС, имеющих различные пространственные и сигнальные признаки, при жестком ограничении на время радиоэлектронного конфликта. Преодолеть указанные трудности можно путем применения [240]:

- антенных устройств с независимым управлением пространственными каналами создания помех;
- многоканальных приемопередающих устройств, работающих в широком диапазоне частот с параллельным анализом каналов;
- быстродействующих систем определения и воспроизведения радиосигналов (DRFM).

В перспективе актуально создание систем DRFM базового построения в плане унификации ее технических параметров для применения большинством разработчиков техники РЭБ. В новой технике РЭБ, основанной на АФАР с цифровым формированием лучей, система будет интегрироваться с устройствами формирования помех в формате малогабаритных приемопередающих модулей АФАР [240].

На рис. 2.10 приведена динамика расширения типажа помех, формируемых современными комплексами РЭБ.

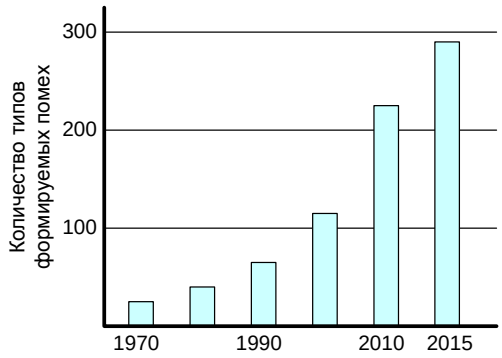


Рис. 2.10. Динамика расширения типажа помех,
формируемых современными комплексами РЭБ [248]

Расширение номенклатуры формируемых помех позволяет реализовать «индивидуальный подход» к подавлению каждого конкретного РЭС. Вместе с тем в связи с насыщением вооружений радиоэлектроникой количество РЭС, находящихся на вооружении, постоянно растет при одновременном повышении количества режимов их работы. В связи с этим в ближайшее время будет достигнут технологический предел номенклатуры формируемых помех, ориентированных на конкретные РЭС и отдельные режимы их работы. При этом актуальным станет поиск новых способов формирования режимов помех для комплексов РЭБ.

В связи с этим интересны исследования, проводимые научно-исследовательской лабораторией ВВС США и ориентированные на разработку новых способов выборочного подавления РЭС — «когнитивного подавления». Новые способы постановки помех должны обеспечивать подавление широкого спектра РЭС противника (связные, навигационные, РЛС и т. д.), использующих современные средства и методы радиоэлектронной защиты, при этом не нарушая функционирования РЭС своих и союзных сил, а также гражданских РЭС. С целью создания новых способов подавления с соответствующим управлением Научно-исследовательской лаборатории ВВС США был заключен контракт на сумму 2,45 млн долларов на срок до 6 лет. За это время должны быть созданы аппаратная часть и программное обеспечение новых станций для реализации «когнитивных помех» для дальнейших их испытаний в условиях, максимально приближенных к боевым. Предполагается, что такие станции помех могут быть установлены как на специализированных самолетах РЭБ, так и на обычных самолетах стратегической и тактической авиации для обеспечения их индивидуальной радиоэлектронной защиты [223].

Одной из наиболее перспективных тенденций развития РЭБ является интегрирование воздушных, наземных, морских и космических средств РЭБ в единую сеть. Концепция интеграции базируется в основном на развитии цифровых направлений техники РТР и активного РЭП. Предусматривается возможность мгновенного опознавания источника излучения и, при необходимости, создание им помех разными способами [223]:

- точечная постановка маломощных активных помех;
- использование объектов ложной информации (ложные цели или сообщения);
- внедрение пакетов алгоритмов, которые могут брать на себя командование сетями противника и, возможно, управление датчиками противника.

Кроме того, перспективным направлением РЭБ является изменение условий распространения и отражения ЭМВ. В связи с этим актуальным является создание специальных боеприпасов с аэрозольным наполнением, обеспечивающих изменение условий распространения радиоволн и воздействующих на функционирование РЭС. С этой целью разрабатываются новые специальные композиции аэрозольных систем, обеспечивающие ослабление напряженности электромагнитного поля, и новые композиции и покрытия, обеспечивающие интенсивное поглощение электромагнитных волн [248].

При этом для защиты собственных РЭС и оптико-электронных средств от самонаводящегося оружия и активных помех различных диапазонов разрабатываются методы и устройства пространственно-сигнальной имитации защищаемых объектов с целью отвлечения на них атакующих элементов, а также устройств пространственно-сигнальной селекции помеховых сигналов [248].

Важнейшие направления исследований для развития систем РЭБ представлены в таблице 2.11. Частные важные направления развития систем радиоэлектронного поражения приведены в таблице 2.12.

Таблица 2.11 — Важнейшие направления развития систем РЭБ [248]

Направления	**Пути реализации**
Интеграция сил и средств РЭБ со средствами разведки и огневого поражения в едином информационно коммуникационном пространстве всех видов ВС	- реализация сетецентрических систем сбора, обработки и доведения до потребителей информации о РЭО; - внедрение защищенных компьютерных технологий для анализа РЭО и принятия решений; - разработка алгоритмов и программ поддержки принятия решений на основе методов искусственного интеллекта
Создание систем РТР (пассивной локации) для достоверного вскрытия РЭО и высокоточного определения местоположения объектов	- создание корреляционно-базовых разностно-дальномерных комплексов пассивной локации; - разработка однопозиционных комплексов, существенно повышающих точность определения местоположения целей за счет измерения крутизны фронта падающей волны; - создание систем искусственного интеллекта для анализа РЭО
Совершенствование системы мониторинга сигналов в различных физических полях	- создание единой государственной инфраструктуры сбора, обобщения и доведения результатов мониторинга; - обеспечение мониторинга в радиочастотном и оптическом диапазонах

Анализируя тенденции развития технологий по разработке и созданию новых радиопоглощающих материалов, можно отметить, что современные поглощающие материалы позволят в ближайшей перспективе обеспечить [248]:

- коэффициент отражения электромагнитного излучения (в диапазоне 1–10 ГГц) порядка — 30–40 дБ независимо от направления зондирования и поляризации сигнала;
- коэффициент отражения в УФ-, видимом и ИК-диапазонах менее 0,1 дБ, причем отражение будет носить диффузионный характер.

Можно прогнозировать, что в ближайшей перспективе будут созданы многофункциональные маскировочные покрытия, работающие одновременно в радиолокационном, УФ-, оптическом и ИК-диапазонах волн [248].

С учетом того, что 90% средств РЭБ являются средствами защиты авиации от систем ПВО и ориентированы на подавление РЛС и оптико-электронных средств управления, целеуказания и наведения этих систем, ниже эти средства и комплексы РЭБ представлены более подробно.

Таблица 2.12 — Важные направления развития
систем радиоэлектронного поражения [248]

Направления	Пути реализации
Создание нового класса комплексов, совмещающих возможности РЭС разведки, управления оружием и станций помех	Реализация информационно-аппаратной интеграции задач в интересах создания устройств, работающих в режимах: - РЛС и наведения оружия; - РРТР; - постановки помех
Создание пространственно-распределенных систем радиоэлектронной защиты объектов и их сигнальной маскировки	Разработка системы активных помех, формирующей ложную сигнально-информационную обстановку в группировке для защиты своих войск и объектов
Создание твердотельной элементной базы нового поколения в интересах повышения эффективности средств РЭБ	Создание ряда широкополосных АФАР на основе твердотельных приемно-передающих модулей в гибридном монолитном исполнении.
Освоение новых участков радиочастотного и оптического диапазонов	- создание электровакуумной и твердотельной широкополосной приемно-передающей аппаратуры миллиметрового и субмиллиметрового диапазонов; - создание высокоэффективных средств разведки и подавления в ИК- и УФ-диапазонах, в т. ч. на основе приемных матриц, излучающих диодов и лазеров
Создание новых носителей для размещения средств РЭБ, обеспечивающих увеличение дальности разведки и подавления	Разработка БПЛА нового поколения и использование алгоритмов на основе искусственного интеллекта
Функциональное поражение РЭС и ОЭС сверхмощными СВЧ-импульсами и ЭМИ нано- и микросекундной длительности	- разработка сверхмощных релятивистских СВЧ-генераторов; - создание малогабаритных ВМГ нового поколения; - создание полупроводниковых генераторных приборов сверхвысокой мощности

2.8.2. Перспективы развития систем РЭБ для защиты авиации от радиолокационных станций комплексов ПВО

Современные средства РЭБ требуют создания помех, прицельных по частоте, но с упреждением по времени. Применяемые в качестве упреждающих широкополосные заградительные шумовые помехи являются энергетически невыгодными. Однако с этим приходится мириться, так как, только обеспечив упреждение, можно рассчитывать на исключение преимуществ, которые имеют РЛС противника при изменении несущей частоты от импульса к импульсу или от пачки импульсов к пачке. Принципиальная возможность создания энергетически выгодных упреждающих прицельных по частоте помех появилась только после внедрения в системы РЭБ высокоскоростных цифровых устройств запоминания частоты перехватываемых сигналов на длительное время. Такие устройства позволяют вместо заградительной шумовой помехи формировать «гребенку» прицельных по частоте маскирующих шумовых помех. При этом спектр каждого «зубца» гребенки сосредоточен в пределах минимально необходимой полосы около частоты, соответствующей одной из множества дискретных со-

ставляющих, запомненных, а затем воспроизведенных частот РЛС. При таком подходе к постановке помех перестройка частоты, осуществляемая РЛС путем скачкообразного перехода на одну из конечного множества фиксированных частот, не защищает РЛС от такой помехи [245].

Важно подчеркнуть, что цифровые устройства обеспечивают запоминание не только частоты, но и сигнала РЛС в целом. Это позволяет решить проблему формирования сигналоподобных помех в ответ на каждый импульс когерентным РЛС (импульсно-доплеровским и со сжатием импульсов). В запоминающее устройство ЭВМ системы РЭБ вводится библиотека параметров всех известных РЛС и режимов их работы. Эта ЭВМ выявляет тип и степень угрозы, определяет приоритеты и стратегию радиоэлектронного подавления, вид и мощность помехи на каждую цель в порядке снижающейся приоритетности. Формирование помех полностью цифровым способом посредством коммутируемой матричной логической структуры позволяет перепрограммировать весь процесс радиоэлектронного подавления, включая пространственно-временную модуляцию помеховых сигналов, настройку по частоте, калибровку по мощности и момент излучения помехи. А это значит, что по мере совершенствования средств ПВО и авиации потенциального противника нет необходимости создавать новую аппаратуру РЭБ — достаточно обновлять ее математическое обеспечение [245].

Таким образом, техническая реализация наиболее перспективных процедур подавления РЛС включает в себя [245]:

- периодическую постановку помех (период создания помехи определяется временем доразведки и излучения помехи с заданными параметрами — процедура типа «Цикл»);
- обеспечение функционирования в системе РЭП алгоритма подавления, включающего в себя своевременный расчет параметров помех (моментов начала и окончания создания помехи, частоты, мощности, ширины спектра и направления создания) и формирование помехи с требуемыми характеристиками сигналов — процедура типа «конвейер»;
- обеспечение в системе РЭП процедуры преобразования входного сигнала с помощью местного гетеродина в сигнал промежуточной частоты, аналого-цифровом преобразовании, стробировании, запоминании фазовой структуры сигнала и формировании помехи путем модуляции сигнала по амплитуде и фазе с задержкой по времени излучения — процедура типа DRFM (цифровая радиочастотная память).

За последние годы в области развития комплексов РЭБ наметился существенный прогресс в рамках трех классов защиты [248]:

1. индивидуальной;
2. индивидуально-взаимной;
3. групповой.

Этот прогресс обусловлен разработкой следующих направлений [248]:

- оптимальное управление ресурсами подавления (формирование по отношению к каждой конкретной РЭС соответствующих видов помех с параметрами, гарантирующими ее эффективное подавление);

- обеспечение эффективного выбора приоритетности объектов РЭБ (например, избирательное подавление РЛС, исходя из степени угрозы для защищаемого ЛА).

Развитие средств РЭБ авиационного базирования в последние годы сосредоточено на совершенствовании средств и комплексов РЭБ, позволяющих увеличить вероятность выполнения боевой задачи при минимальных потерях ЛА. Основными факторами при этом являются следующие [240]:

- комплексная оптимизация характеристик средств РЭБ и снижения заметности с учетом особенностей объектов защиты, массогабаритных и энергетических ограничений;
- построение аппаратуры по принципам, обеспечивающим наращивание ее по функциональным возможностям и техническим параметрам, что позволяет легко проводить их последующую модернизацию;
- глубокая функциональная и аппаратурная интеграция РЭС различного назначения в составе комплекса с целью совершенствования алгоритмов обработки информации и принятия решения для высокоэффективной реализации задач РЭБ;
- повышение точности пеленгации и моноимпульсное измерение частоты источника излучения, необходимое для угловой селекции РЛС с целью совершенствования информационной поддержки применения бортового ВТО, в частности целеуказания ракетам с радиолокационными ГСН;
- реализация регулируемой чувствительности аппаратуры РТР в комплексе РЭБ для осуществления целеуказания ракетам с радиолокационными ГСН по боковым лепестками диаграммы направленности антенн РЭС и организации эффективного применения расходуемых средств;
- существенное повышение качества адаптации параметров помех к характеристикам каналов подавляемых РЭС по несущей частоте, поляризации, спектру и задержке в реальном масштабе времени для обеспечения скрытности применения помех и минимальных энергетических потерях;
- формирование конфликтно-устойчивых видов помех с улучшенными имитационными свойствами на основе DRFM, нейтрализующих возможные виды обработки информации в объектах подавления;
- расширение рабочих частотных диапазонов комплекса РЭБ и освоение новых диапазонов для сокращения аппаратуры помех и расширения номенклатуры подавляемых средств;
- обеспечение возможности обмена информацией между комплексами РЭБ различных ЛА, позволяющей формировать пространственно-распределенные помехи при защите строя ЛА;
- «дозированное» по мощности излучение помех и обеспечение практически мгновенного формирования диаграмм направленности антенн передатчиков помех;

- разработка аппаратуры создания когерентных и некогерентных помех, излучаемых с одного или нескольких ЛА, для противодействия угломерным координаторам вне зависимости от применяемого способа пеленгации;
- разработка быстродействующих спецпроцессоров и применение высокопроизводительных бортовых ЭВМ с целью обеспечения высокой пропускной способности и уменьшения времени реакции на вновь возникающие угрозы;
- разработка широкополосных передатчиков, в том числе с применением АФАР, с высоким КПД, с пониженным уровнем внеполосных и побочных излучений, с малым уровнем собственных шумов для улучшения массогабаритных и энергетических характеристик аппаратуры и обеспечения электромагнитной совместимости на борту ЛА;
- формирование облака искусственных пространственно-распределенных поглощающих образований, позволяющих уменьшить ЭПР защищаемого объекта и создать области пространственно-информационной неопределенности;
- массированное и комплексное применение средств создания активных помех и расходуемых средств РЭБ нового поколения (передатчиков и ретрансляторов одноразового действия, авиационных ложных целей, буксируемых ловушек), существенно усложняющих радиоэлектронную обстановку и приводящих к дефициту временного ресурса РЛС при обслуживании истинных целей;
- разработка номенклатуры узлов и блоков 5-го поколения в модульном исполнении для формирования нового класса средств РЭБ для малоразмерных объектов широкого применения.

Для авиационных комплексов РЭБ перспективными направлениями их развития и повышения эффективности является [241]:

- применение специальных видов помех против РЛС с пространственной компенсацией помех;
- оптимальное адаптивное управление ресурсами системы защиты ЛА по составу и динамике их использования;
- использование бортовых многофункциональных РЛС в качестве высокопотенциальных средств помех и информационной поддержки системы помех, в частности для сопровождения атакующих управляемых ракет на траектории;
- комплексный учет применения разнородных средств РЭБ — станций активных помех, пассивных помех, ложных целей, противорадиолокационных ракет.

Разработка цифрового когерентного приемника с функциями пеленгатора источников излучения обеспечит возможность совмещения функций РТР и РЭП в одном элементе и тем самым решит задачи обнаружения и анализа угрозы с одновременной постановкой помех нескольким целям, создавая предпосылки временного и пространственного управления ресурсами подавления. Возможность когерентного цифрового приемника на базе технологии DRFM

позволит имитировать для РЛС противника фантомы цели со всеми необходимыми характеристиками, особенностями «портрета» цели по отражательной способности, динамики движения, протяженности (геометрических размеров), спектральных характеристик объекта. Решение проблемы создания широкополосного когерентного цифрового приемника, работающего в реальном масштабе времени при современной сложной фоно-целевой обстановке, позволит обеспечить защиту ЛА от современного и перспективного управляемого оружия [242].

Направления и основные пути создания перспективной техники РЭП ориентированной на подавление РЛС приведены в таблице 2.13 [244].

Таблица 2.13 — Основные направления создания перспективной техники ориентированной на подавление РЭП РЛС [244]

Направления	**Пути реализации**
Обеспечение энергетической избыточности	- использование мощных электровакуумных приборов и антенн с большими КНД; - использование ФАР и АФАР; - создание помех из нескольких точек пространства; - приближение средств помех к объекту подавления; - использование РЛС для создания помех
Обеспечение информационной избыточности	- разведка всех параметров РЭО, в том числе координат источников излучения в реальном масштабе времени; - запоминание и воспроизведение когерентных и сверхширокополосных сигналов
Обеспечение частотной избыточности	- использование приемо-передающей элементной базы с широкополосностью 2 октавы и более; - применение широкополосных ФАР; - создание двух диапазонных антенных систем
Обеспечение возможностей перманентной модернизации	- использование принципа открытой архитектуры при выборе функционально-технической структуры комплекса; - обеспечение электромагнитной совместимости, информационной и программной совместимости технических устройств
Повышение уровня системной организации	- обеспечение функционально-технического сопряжения разнородных комплексов РЭП при решении общих задач; - аппаратурная интеграция комплексов РЭП с РЭС защищаемых объектов
Использование помех, обеспечивающих перевод РЛС в нештатный режим работы	- создание комбинированных помех, переводящих систему в режим СДЦ, в том числе с использованием ракет — постановщиков помех; - сочетание нестационарных маскирующих и имитирующих помех высокой плотности; - создание поляризационных и когерентных помех; - создание помех, использующих конструктивные особенности РЛС, а также особенности алгоритмов обработки сигналов в ней
Развитие средств РЭП, инвариантных к параметрам излучаемых РЛС сигналов	- создание пассивных и активных ретрансляционных ловушек и ложных целей; - развитие оружия, самонаводящегося по излучениям РЛС; - создание средств функционального поражения РЛС и изменения условий распространения ЭМВ; - снижение заметности защищаемых объектов и комплексная оптимизация средств РЭП и снижения заметности

Реализация вышеуказанных направлений развития техники РЭП ориентированных на подавление РЛС должна обеспечить возможность создания нового поколения комплексов и систем РЭП, в том числе [248]:

- адаптивных комплексов РЭП для индивидуально-взаимной защиты ЛА от ВТО с радиолокационными и комбинированными ГСН, аппаратно-интегрированных с БРЭО защищаемых объектов;
- многофункциональных адаптивных пространственно-распределенных систем РЭП для индивидуально-взаимной защиты и многоэлементных объектов от РЭР и ВТО;
- многофункциональных пространственно-распределенных систем РЭП, средств РЭР, радионавигации, связи и управления оружием «воздух — поверхность» для защиты войск и объектов инфраструктуры, информационно и функционально сопряженных с системами ПВО;
- средств РЭП с новыми физическими принципами формирования ЭМИ для функционального поражения РЛС.

2.8.3. Перспективы развития систем РЭБ для защиты авиации от оптико-электронных средств в комплексах ПВО

В настоящее время авиационные бортовые системы подавления инфракрасных и оптических средств активно развиваются. Эти бортовые системы ориентированы на противодействие системам управления оружием в комплексах ПВО. При этом для разработки перспективных комплексов защиты летательных аппаратов от систем ПВО с ракетами на основе ИК ГСН необходимо решить ряд задач.

Совокупность этих задач может быть квалифицирована как оптико-электронное противодействие по замкнутому циклу [248]:

- обнаружение с высокой степенью достоверности факта пуска ракеты и определение с требуемой точностью ее угловых координат;
- сопровождение атакующей ракеты с ГСН на траектории с точностью, необходимой для наведения помехового излучения;
- генерация лазерного излучения в пределах спектральных диапазонов современных и новых поколений ГСН;
- обеспечение противодействия в течение времени, достаточного для того, чтобы помеховое воздействие на ГСН приводило к срыву процесса наведения;
- генерация лазерного излучения подавления с плотностью потока мощности значительно выше (на порядки), чем плотность потока мощности ИК-излучения самолетов и вертолетов в соответствующем спектральном диапазоне для обеспечения удовлетворительного соотношения (сигнал помехи/сигнал от цели);
- генерация лазерного излучения с мощностью, достаточной для формирования отраженного излучения от ГСН атакующей ракеты (это дает возможность системе противодействия выделить ракеты с оптическим наведением от других угроз, измерять дальность до атакующей ракеты, а также осуществлять оценку результатов противодействия).

Для адаптации оптико-электронных средств комплексов РЭБ ЛА к современному уровню развития средств перехвата воздушных целей, оснащенных ИК и оптико-электронными средствами наведения оружия необходимо провести ряд мероприятий, основные направления которых приведены в таблице 2.14.

Таблица 2.14 — Основные направления развития средств оптико-электронного поражения для самолетов и вертолетов [246]

Объекты оптико-электронного поражения	**Направления развития**	**Пути разработки**
Оптические головки самонаведения со спектральной селекцией	Создание низкотемпературных ложных тепловых целей	Использование в ложных тепловых целях низкотемпературных пирофорных излучателей или излучателей на основе углеводородных топлив
Двухканальные оптические головки самонаведения, работающие в ИК- и УФ-диапазонах длин волн	Создание многоспектральной станции подавления на некогерентных источниках излучения	Использование в излучающих модулях станции разнотипных газоразрядных ламп
Оптические головки самонаведения с матричными фото-приемными устройствами	Создание лазерной станции оптико-электронного поражения для функционального поражения оптических элементов ГСН ракет	Разработка химических и твердотельных лазеров высокого энергопотенциала, а также систем точного наведения лазерного излучения на основе матричных фотоприемных устройств УФ- и ИК-диапазонов
Оптико-визуальные, телевизионные и тепловизионные средства сопровождения целей систем наведения ЗРК	Создание вертолетного устройства аэрозольной и дымовой защиты направленного действия	Разработка аэрозолеобразующих составов для формирования быстродействующих широкодиапазонных завес в оптическом и радиолокационном диапазонах

Таблица 2.15 — Основные направления развития средств оптико-электронного поражения для самолетов и вертолетов [246]

Объекты ОЭП	**Направления развития**	**Пути разработки**
Оптико-визуальные и телевизионные средства сопровождения целей систем наведения ЗРК	Создание управляемых средств снижения заметности в видимом диапазоне длин волн	Разработка электро-хромных и люминесцентных покрытий
Тепловизионные средства сопровождения целей систем наведения ЗРК	Создание управляемых средств снижения заметности в ИК-диапазоне длин волн	Разработка покрытий с селективными излучательными характеристиками
Оптические головки самонаведения с матричными фото-приемными устройствами		
Двухканальные оптические головки самонаведения, работающие в ИК- и УФ-диапазонах длин волн	Создание управляемых средств компенсации отрицательного контраста цели в УФ-диапазоне	Разработка многослойных матриц светоизлучающих диодов в УФ-диапазоне

2.8.4. Перспективы развития систем РЭБ, ориентированных на нарушение функционирования сетецентрических систем военного управления

Представленные в данном разделе перспективные подходы основаны на научных исследованиях автора по обоснованию новых подходов к радиоэлектронным воздействиям, ориентированным на нарушение функционирования сетецентрических систем военного управления. При этом предполагается, что указанные радиоэлектронные воздействия будут менее энергоемкими и более бескомпороматными, а также то, что они могут быть реализованы существующими «традиционными» средствами и комплексами РЭБ только за счет изменения логики их функционирования.

В основу данного материала были положены обзорные работы по общим военно-прикладным принципам нарушения функционирования сетецентрических систем военного управления [195, 371], а также работы [190–192, 194, 196, 198–201, 204, 205] с теоретическим обоснованием новых способов и технологий РЭП, ориентированных против объединенных сетей связи, являющихся основой сетецентрической среды.

2.8.4.1. Перспективные подходы к воздействию на сетецентрические системы управления

Основная парадигма ведения войн в ближайших десятилетиях будет основана на концепции управления боевыми действиями по сетецентрическому принципу на основе объединения средств функционально взаимосвязанных подсистем: информационной, сенсорно-разведывательной и боевой на основе единой сетецентрической среды. При этом основу такой системы управления составляет информационная подсистема, объединяющая подсистемы разведки и боевого воздействия.

Анализ использования сетецентрического принципа управления позволяет выявить основные тенденции в изменении характера военного противоборства между развитыми в техническом отношении государствами в период до 2020 г. и на дальнейшую перспективу [371]:

- постоянно возрастающая угроза нанесения противником упреждающего комплексного удара огневыми и высокоточными средствами, совмещенного с информационными и радиоэлектронными воздействиями на информационную инфраструктуру;
- переход к избирательному поражению объектов на территории противника преимущественно критических объектов инфраструктуры страны и ее ВС с использованием ВТО;
- возрастание роли разведки, оперативной маскировки и защиты войск, населения и объектов тыла от перспективных средств поражения;
- скоротечность воздушно-наземных сражений, резкие изменения обстановки и способов действий войск;

- проведение информационных, психологических, маскировочных (прежде всего дезинформационных) и других специальных операций для завоевания и удержания глобального и «всеохватывающего» информационно-психологического превосходства;
- радиоэлектронное поражение элементов систем управления войсками и оружием, применение программно-технических средств, экономических методов борьбы и др.;
- расширение масштаба применения космических средств для ведения разведки, управления войсками и оружием группировок сухопутных, военно-воздушных и военно-морских сил, нанесения ударов в космосе и из космоса;
- возрастание повсеместного использования беспилотных, роботизированных и дистанционно управляемых средств ведения и обеспечения вооруженной борьбы на всех уровнях;
- расширение сферы применения сил специальных операций для диверсионно-террористических и разведывательно-диверсионных действий в глубоком тылу наших войск.

При этом основными характерными чертами системы ведения вооруженной борьбы при реализации сетецентрического принципа управления будут следующие [371]:

- средства вооруженной борьбы являются информационно насыщенными и содержат в своем составе элементы сетевой информационной инфраструктуры;
- сокращаются циклы принятия решений, возникает необходимость учета дополнительных факторов в процессе управления, что требует увеличения пропускной способности информационной подсистемы;
- принятие управленческих решений с учетом автоматизированных систем поддержки, основанных на информационных интеллектуальных системах;
- аппаратно-программные средства, обеспечивающие взаимодействие внутри телекоммуникационных сетей, формируют сложную сетевую глобальную информационную инфраструктуру;
- элементы сетевой инфраструктуры (средства вооруженной борьбы, обеспечения, управления и коммуникации) по своей сути являются информационно-вычислительными системами разного уровня сложности и организации.

В то же время сетецентрическая система управления будет уязвима по следующим направлениям [371]:

- разрушение информационных потоков, циркулирующих между элементами системы;
- снижение скорости информационного обмена между элементами системы, что позволит резко увеличить продолжительность цикла «обнаружение — опознавание — целеуказание — поражение» и свести к минимуму эффективность сетецентрического принципа управления;

- обеспечение достаточно массированного и долговременного вывода из строя сетеобразующих средств;
- насыщение многочисленных средств разведки и воздействия «коллективными интеллектуальными алгоритмами функционирования» в интересах повышения боевой эффективности решения задач системоразрушения.

Таким образом, для реализации вышеуказанных направлений деструктивного воздействия на сетецентрические системы управления необходимо принять меры по совершенствованию и скоординированности действий систем и средств разведки, комплексов и средств РЭП, связи, управления и средств поражения, по созданию оружия направленного воздействия, способного нарушать работу автоматизированных баз данных и локальных вычислительных сетей, выводить из строя основные органы управления, связи и разведки противника.

Рассмотрим одно из перспективных направлений деструктивного воздействия на системы военного управления на основе сетецентрического принципа, достаточно легко реализуемое на практике в ближайшей перспективе.

Информационная подсистема системы сетевого управления образуется вычислительными системами разного уровня сложности, которые объединяются сетями связи в единую сетецентрическую среду. При этом одним из основных свойств системы управления, характеризующим их способность функционировать по назначению, является устойчивость системы связи.

Таким образом, снижение устойчивости системы связи за счет интегрального применения обычного и высокоточного оружия, комплексов и средств РЭП приведет к нарушению сетевого принципа управления.

Применительно к современным системам управления можно выделить три слоя сетецентрической среды, образованной системой связи, которые могут быть подвержены воздействиям [195, 371]:

1. физический слой (техническая инфраструктура систем связи);
2. семантический слой (данные);
3. синтаксический слой (протоколы передачи данных).

Такого рода подход позволяет определить следующие воздействия [195, 371]:

- воздействия на физический слой, направленные на реальную инфраструктуру информационно-вычислительных систем, систем передачи данных и подразумевающие их физическое разрушение;
- воздействия на семантический слой, связанные с нарушением целостности и корректности информации;
- воздействия на синтаксический слой, направленные на повреждение данных и нарушение логики функционирования систем.

В силу ряда обстоятельств воздействия на семантический и синтаксический слои представляются более простыми, доступными и легко реализуемыми средствами, чем воздействия на физическом уровне с использованием обычного и высокоточного оружия при сопоставимом уровне достигаемого результата. В связи с этим их разработке уделяется всё больше внимания. Современ-

ный подход к воздействию на семантический и синтаксический слои сетецентрической среды предполагает комплексное сбалансированное применение комплексов и средств РЭП с одновременным проведением мероприятий по защите своих систем управления и информационных ресурсов [371].

Ввиду недостаточно разработанной теоретической базы проведения такого рода действий наиболее простым, целесообразным способом воздействия средств РЭП на сети радиосвязи в составе системы связи с целью снижения их устойчивости функционирования в интересах нарушения синтаксического слоя сетецентрической среды противника [371].

Вместе с тем проведенный анализ использования существующей «традиционной» тактики подавления и применения комплексов и средств РЭП показал, что оно недостаточно эффективно при использовании противником сетецентрического принципа управления.

Основанный на «традиционном» подходе к воздействию РЭП пример нарушения работы иерархической системы управления (тактической авиацией) показан на рис. 2.11. В этом случае нарушения управления достигались при воздействии средств РЭП на любом уровне иерархической системы управления, в результате блокирования прохождения информации к средству поражения и, как следствие, невыполнения им боевой задачи [371].

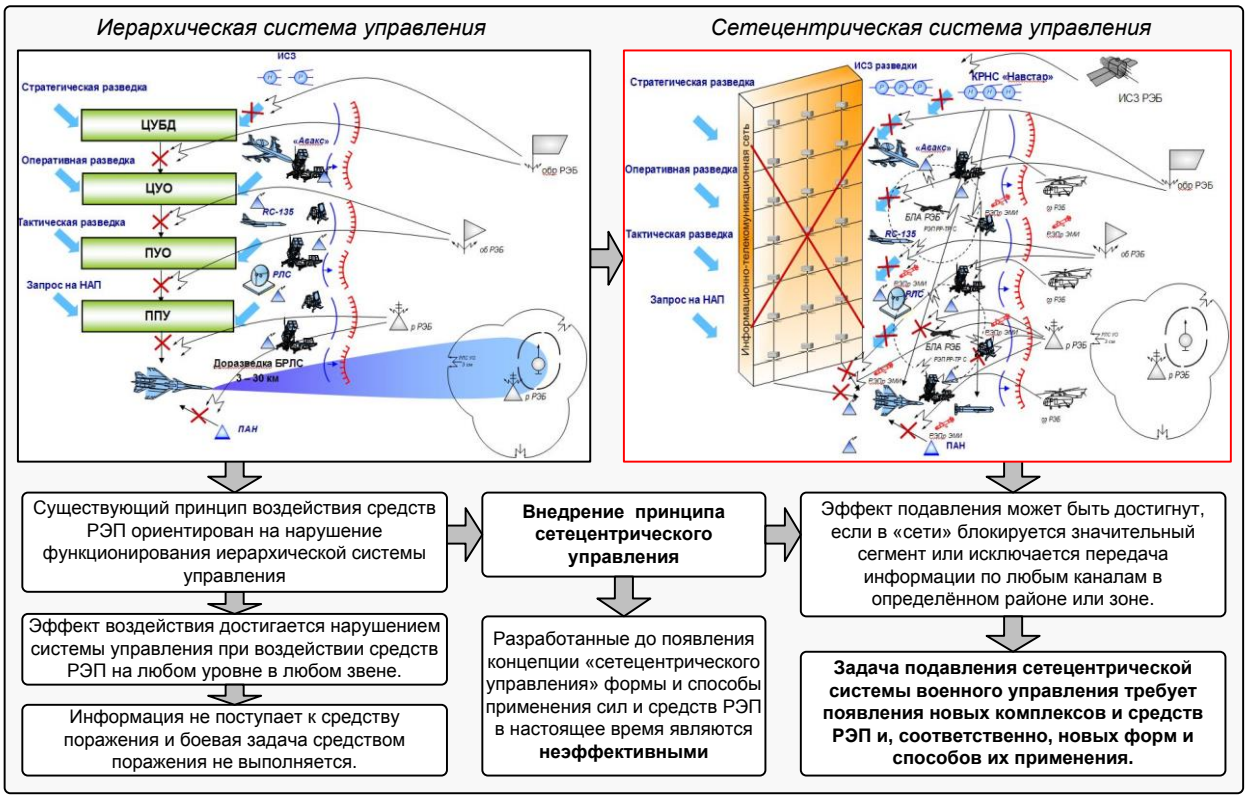


Рис. 2.11. Применение комплексов и средств РЭП
в интересах дестабилизации системы управления [371]

Таким образом, формы и способы применения комплексов и средств РЭП, разработанные до появления концепции сетецентрического управления, будут неэффективны против вооруженных формирований, управляемых через

единую сетецентрическую среду. В подобной системе полностью перекрыть каналы информационного обеспечения и управления практически невозможно. Для нарушения работы такой системы (рис. 2.11) необходимо исключить все каналы управления и передачи информации или вывести из строя все технические или боевые средства. Фактически эффект может быть достигнут, если в системе блокируется значительный сегмент или исключается передача информации по любым каналам в определенном районе или зоне. Решение такой задачи требует разработки новых комплексов и средств РЭП и, соответственно, новых форм и способов их применения [371].

Обобщая вышеуказанное, можно сделать следующие выводы [371]:

- существующий подход по воздействию средств РЭП на отдельные элементы системы связи как основы сетецентрической среды является неэффективным;
- воздействуя на информационную инфраструктуру сетецентрической системы военного управления, техническую основу которой составляют системы связи и АСУ, можно достигнуть значимого эффекта поражения данной системы.

Воздействие территориально распределенной разнородной группировки средств РЭП позволит реализовать следующие из основных направлений противодействия системам управления, построенным в соответствии с сетецентрическим принципом, сформулированные ранее [371]:

- разрушение информационных потоков, передаваемых в сетецентрической среде;
- снижение скорости информационного обмена между элементами сетецентрической системы;
- обеспечение достаточно массированного и долговременного вывода из строя сетеобразующих средств.

Исследования, представленные в работах [188, 189, 191, 192, 195, 371, 411], показывают, что наиболее действенным для деструктивного воздействия на сетецентрические системы военного управления будет поражение именно космического сегмента информационной подсистемы, который, с одной стороны, осуществляет глобальные функции информационного обеспечения, а с другой — строится на основе средств радиосвязи и вследствие этого уязвим для применения средств РЭП.

Снижение качества функционирования космической группировки приведет к множественным проблемам в работоспособности информационной подсистемы, а также в применении многих видов ВВТ, поскольку именно космический сегмент, включающий космические системы разведки, связи, навигации, топогеодезического и метеорологического обеспечения, интегрированные в единый информационно-управляющий контур, является основой архитектуры глобальной информационной подсистемы. При этом реализация поражения различных компонентов такого информационно-управляющего контура приведет к невозможности каждой из систем обеспечивать выполнение всех или части присущих ей функций.

В частности, можно выделить [371]:

- в космической разведке — невозможность с требуемой своевременностью передавать сообщения об обнаружении объектов, целеуказании и оперативном контроле результатов воздействия ударными средствами, а также данных о складывающихся условиях обстановки для определения применяемых ударных средств;
- в космических системах связи — невозможность с заданным качеством обеспечить передачу сообщений боевого управления, осуществлять обмен данными между воинскими формированиями и органами управления, включая оперативную передачу на пункты управления данных для подготовки ударов, и их результат;
- в космических топогеодезических системах — невозможность передавать сообщения по обеспечению органов военного управления всех уровней достоверными топографическими и геодезических данными с заданной своевременностью, обеспечить войска специальными картами и фотодокументами местности, а также сделает невозможным доступ к цифровым информационным массивам в интересах систем наведения ВТО;
- в космических радионавигационных системах — подавление радиоканалов управления КА приведет к отказу СРНС и, соответственно, к невозможности создания навигационных полей, которые используются при определении местоположения воинских формирований, боевой и другой техники, ударных средств и средств поражения.

Таким образом, с учетом специфики современного перехода к реализации сетецентрического принципа управления интерес представляет использование существующих комплексов и средств РЭБ в качестве основы для поражения такой системы военного управления.

2.8.4.2. Перспективные научно-методические подходы к обоснованию способов радиоэлектронного воздействия на сетецентрические системы управления

Исходя из приведенных выше аргументов, представляется возможным сформулировать ряд подходов к технологической реализации деструктивного воздействия на системы связи, образующие сетецентрическую среду сетецентрической системы управления. С учетом специфики современного перехода к реализации сетецентрического принципа управления, интерес представляет использование радиоэлектронных воздействий, основанных на развитии форм и способов применения существующих комплексов и средств РЭП в качестве основы для поражения такой системы военного управления [195, 371].

До последнего времени основная часть работ по РЭП была посвящена решению задач подавления отдельных линий радиосвязи, т. е. подавлению на физическом уровне модели взаимодействия открытых систем OSI (Open Systems Interconnection). Имеются отдельные исследования, посвященные подавлению сетей радиосвязи с учетом их структуры, логики функционирования и ценности передаваемой информации. Вместе с тем, анализируя возмож-

ности использования «традиционных» средств РЭП, можно прийти к выводу, что их воздействия возможны и на другие объекты транспортной подсистемы модели OSI (физический, канальный, сетевой и транспортный уровни). Объектами радиоэлектронного воздействия на физическом уровне традиционно являются РЭС и каналы связи. На канальном уровне к таким объектам относятся каналы множественного доступа, предназначенные для образования отдельных сетей (например, на основе протоколов TDMA, ALOHA, DVB-RSC). К объектам радиоэлектронного воздействия на сетевом уровне OSI относятся узлы, транспортные каналы объединенной сети связи, а также протоколы маршрутизации и сигнализации, обеспечивающие их функционирование. На транспортном уровне к объектам воздействия следует отнести протоколы и аппаратно-программные средства обеспечения качества обслуживания информационных потоков, передаваемых по объединенной сети связи. Воздействие средств РЭП приводит к различного рода негативным эффектам на различных уровнях OSI, часть из которых представлена на рис. 2.12.

Рис. 2.12. Некоторые негативные эффекты, которые могут вызвать радиоэлектронные воздействия на различных уровнях транспортной подсистемы модели OSI [195, 371]

Современная методология применения «традиционных» средств РЭП ставит своей целью снижение показателей качества обслуживания отдельных сетей и каналов радиосвязи ниже значений, определенных требованиями по качеству связи. При этом основная часть работ по РЭП посвящена решению задач подавления отдельных ЛРС, а также сетей радиосвязи, то есть подавлению на

физическом уровне модели OSI. Однако объединение отдельных систем передачи данных, в том числе радиосетей, в объединенную глобальную сеть связи сетецентрической среды ведет к тому, что подавление отдельных радиосетей в ее составе не приведет к информационным потерям или снижению своевременности передачи данных. Подавление отдельных радиосетей приведет лишь к перемаршрутизации информационных потоков в объединенной сети связи без снижения оперативности и потери работоспособности объектов сетецентрической среды, а следовательно, и системы сетецентрического управления [195].

Воздействие «традиционных» средств РЭП на сети связи происходит на физическом уровне модели OSI. Однако это воздействие проявляется также и на вышестоящих уровнях транспортной подсистемы модели OSI — канальном, сетевом и транспортном [195].

Именно за счет использования новых эффектов от радиоэлектронных воздействий на канальном, сетевом и транспортном уровнях OSI предполагается решение проблемы комплексного подавления объединенных сетей связи, являющихся технической основой сетецентрической среды для сетецентрических систем военного управления. При этом непосредственным объектом воздействия будут отдельные ЛРС и радиосети, функционирующие в составе объединенных сетей связи. Таким образом, перспективные способы подавления объединенных сетей связи будут использовать эффекты деструктивного влияния радиоэлектронных воздействий на физическом уровне как основу для формирования эффектов подавления на вышестоящих уровнях модели OSI — канальном, сетевом и транспортном [195].

В настоящее время для решения задач обеспечения качества обслуживания телекоммуникационных сетей проводятся многочисленные исследования эффективности функционирования сетей связи и коммутационных устройств различного уровня в условиях передачи трафика сложной структуры (наличие самоподобных свойств, непуассоновское распределение времени поступления пакетов и др.), а также маршрутизации информационных потоков в сетях с динамически изменяемой топологией. В исследованиях по этой тематике указывается на значительное снижение быстродействия и оперативности обслуживания указанных информационных потоков при передаче их по сетям с динамически изменяющейся топологией. Предлагается использовать имеющиеся результаты данных исследований в области оценки качества обслуживания телекоммуникационных сетей для разработки новых решений по организации радиоэлектронного подавления сетецентрических систем [195].

Предполагается использовать отображение отдельных видов радиоэлектронных воздействий на физическом уровне на более высокие уровни функционирования системы связи — канальный, сетевой и транспортный. При этом данные воздействия позволяют организовать новые квази-бескомпроматные помехи на физическом уровне, которые, с одной стороны, не определяются существующими средствами помехозащиты, а с другой — ориентированы на снижение эффективности функционирования протоколов сетевого и транспортного уровня, из-за того, что вызывают ряд негативных эффектов на этих уровнях (рис. 2.13) [195].

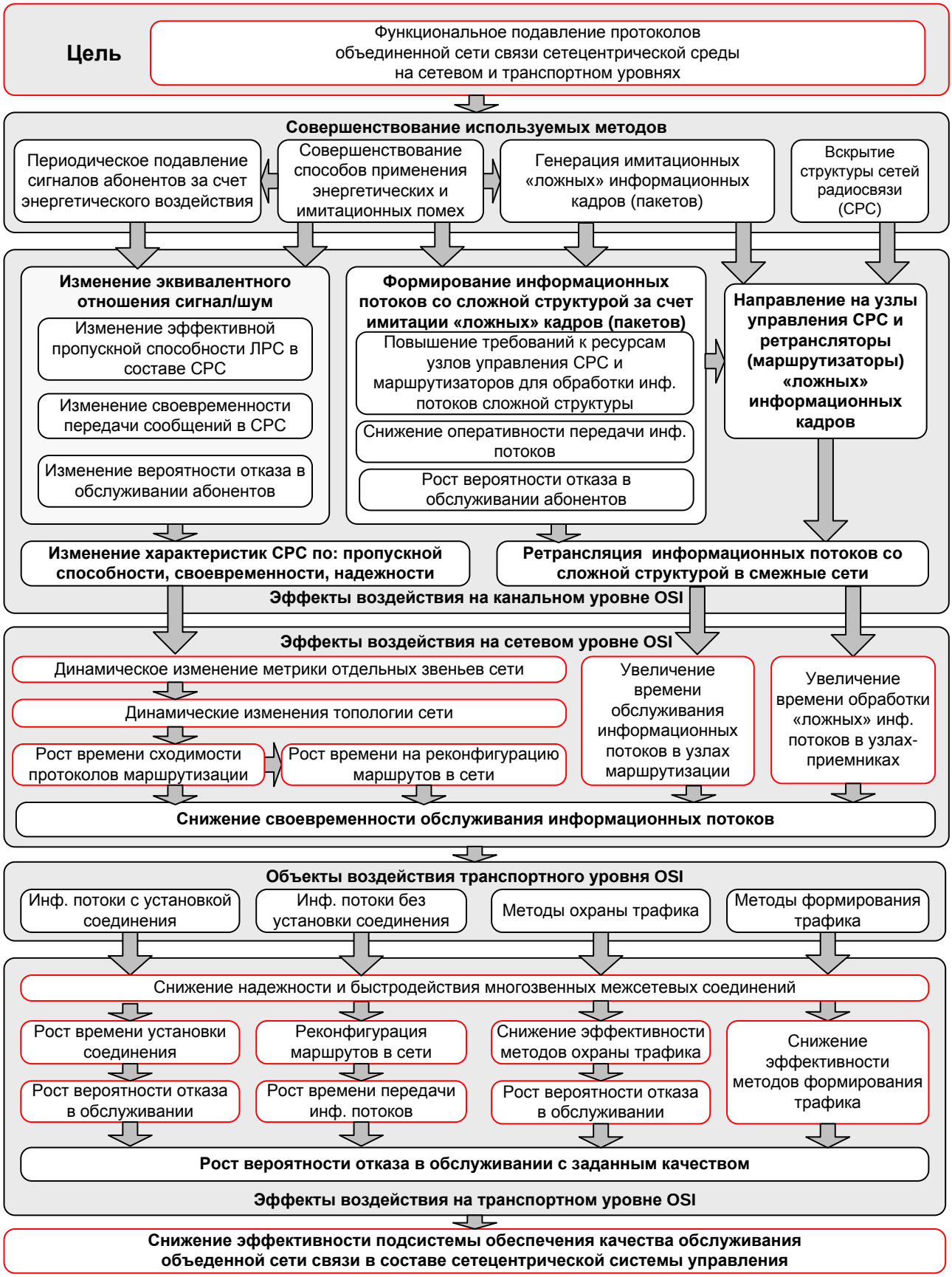


Рис. 2.13. Радиоэлектронные воздействия, ориентированные на функциональное подавление протоколов объединенной сети связи сетецентрической системы управления [195, 371]

Рассмотрим некоторые из перспективных направлений разработки радиоэлектронных воздействий, ориентированных на подавление объединенных сетей связи за счет учета особенностей функционирования протоколов на канальном, сетевом и транспортном уровнях модели OSI. Основной особенностью рассматриваемых воздействий является учет динамики влияния помех, что позволяет рассмотреть динамические нестационарные и переходные режимы в объектах подавления, а также функциональные зависимости между протоколами на различных уровнях модели OSI.

1. Радиоэлектронные воздействия, ориентированные на подавление отдельных сетей множественного доступа. Исследования возможностей радиоэлектронных воздействий по подавлению протоколов связи на канальном уровне, представленные в работах [190, 192, 412], показали следующее. Известно, что пакетным радиосетям, использующим для передачи пакетов общий канал со случайным множественным случайным доступом (МСД), свойственна нестабильность функционирования. Такие радиосети требуют коррекции при большом времени непрерывной работы. Таким образом, возможна реализация радиоэлектронного воздействия, направленного на подавление радиосети на основе общего радиоканала со случайным МСД путем периодического воздействия преднамеренных помех и за счет использования специфических свойств метода случайного доступа. Данный подход при подавлении радиосети был впервые предложен С.И. Бабусенко и получил развитие в работах [190, 191] применительно к сетям на основе протоколов CSMA/CA и S-Aloha.

Процесс обслуживания пакетов в этих радиосетях со случайным МСД был представлен в виде марковского процесса гибели-размножения, в котором интенсивность обслуживания пакетов определяется пропускной способностью, которая, в свою очередь, зависит от текущего значения ОСШП. Проведенное моделирование показало, что динамическое периодическое воздействие помех на общий канал таких радиосетей ведет к сносу их в заблокированное состояние даже после снятия радиоэлектронного воздействия. При этом эффект подавления может быть достигнут без полного подавления канала МСД, а за счет частичного снижения его пропускной способности, в пределах 10–20%. Данный способ радиоэлектронного воздействия, ориентированный на канальный уровень OSI, может быть осуществлен «традиционными» средствами РЭП за счет введения режима динамических помех, временные параметры которых согласованы с параметрами протокола случайного МСД, используемого в радиосети [190, 191].

Современные системы связи строятся на основе MIMO технологий, в которых для передачи сообщений адресату могут быть выбраны несколько путей. В дальнейшем вышеуказанное направление разработки радиоэлектронных воздействий получило развитие в виде модели многоканальной системы массового обслуживания с блокировкой отдельных каналов, моделирующей MIMO систему связи, представленной в работе [412]. Периодическое воздействие в виде подавления отдельных радиоканалов в многоканальной системе связи ведет к существенному снижению качества обслуживания такой системы и в конечном итоге — к перегрузке системы пакетами и переходу ее в заблокированное

состояние. Проведенное в работе [412] моделирование показало, что при выполнении критерия блокировки системы ее пропускная способность снижется со 100% до 70%, а время обслуживания в многоканальной системе радиосвязи увеличивается в 10–20 раз относительно уровня, соответствующего ее нормальному функционированию.

Таким образом, динамические радиоэлектронные воздействия позволяют осуществить перевод радиосети в нестационарный режим работы, увеличить длительность и глубину переходных процессов в них. Увеличение интенсивности воздействий позволяет перевести радиосеть в заблокированное состояние вследствие снижения интенсивности обслуживания ею входного потока пакетов ниже критических значений.

2. Радиоэлектронные воздействия, ориентированные на подавление объединенных территориально распределенных смешанных сетей связи. Принцип воздействия помехами с динамически изменяемыми параметрами для варьирования пропускной способности каналов в их рабочем диапазоне ОСШП (чтобы исключить срабатывание средств помехозащиты физического уровня) в дальнейшем получил развитие для разработки радиоэлектронных воздействий, ориентированных на подавление объединенных сетей связи за счет учета особенностей функционирования их протоколов на сетевом уровне модели OSI.

Для учета эффектов динамического радиоэлектронного воздействия на сетевом уровне был предложен пересчет качества обслуживания отдельных сетей и каналов радиосвязи в коэффициенты метрики сети, используемые соответствующими протоколами при решении задач сигнализации в сети и маршрутизации в ней информационных потоков. Математическая модель, формализующая оценку метрики каналов сети в условиях динамического воздействия помех применительно к спутниковым каналам DVB-S/S2, представлена в работе [192]. Проведенное моделирование для канала связи DVB-S2 показало, что периодическое изменение ОСШП в канале (как в сторону увеличения, так и в сторону снижения) приводит к выдаче сообщений об изменении метрики канала, которые, в свою очередь, ведут к остановке процесса передачи и пересчету топологии сети. Интенсивность данных сообщений прямо пропорциональна периодичности и глубине изменения ОСШП, а время между отдельными сообщениями в общем случае может быть аппроксимировано экспоненциальным распределением. Анализ эффектов воздействия средств подавления на адаптивно-лавинные протоколы маршрутизации (OSPF, IS-IS, EIGRP и др.), которое было проведено в работах [196, 198, 199], показало, что такое воздействие ведет к росту интенсивности перемаршрутизации информационных потоков и снижению адекватности таблиц маршрутизации.

Исследование процесса функционирования маршрутизатора с адаптивно-лавинным протоколом (на основе OSPF), проведенное в работе [413], показало, что вероятность подавления сети связи определяется интенсивностью отказов отдельных каналов вследствие воздействия помех, а также параметром протокола маршрутизации по ожиданию времени восстановления связи. Причем размер сети связи практически не влияет на эффективность ее подавления. Суще-

ствует принципиальная возможность подавления сети связи при воздействии с заданной интенсивностью даже на единственный радиоканал в ее составе.

В работе [414] для обоснования временных параметров радиоэлектронного воздействия, направленного на нарушение функционирования протоколов маршрутизации без установления соединения, была разработана модель функционирования объекта связи в условиях отказов каналов связи в виде Марковского процесса переходов между состояниями «нормальное функционирование» — «отказ канала» — «ожидание восстановления связи» — «реконфигурация маршрутизатора». Использование данной модели в составе методики обоснования временных параметров радиоэлектронного воздействия на протокол маршрутизации по состоянию каналов (на примере протокола OSPF) позволил определить наиболее сложные условия функционирования для этого протокола маршрутизации. Результаты моделирования показывают, что при согласовании временных параметров воздействия и протокола маршрутизации достигается снижение коэффициента готовности отдельного маршрутизатора до 0,5. За счет лавинной рассылки смежным узлам сообщений об изменении метрики отдельных каналов каждый из маршрутизаторов сети снижает свой коэффициент готовности из-за постоянного пересчета кратчайших путей. В результате эффект снижения устойчивости распространяется на всю сеть в целом. При этом показатель устойчивости сети по показателю «среднесетевая вероятность устойчивости информационного направления связи» снижается до значений 0,4–0,2. При этом уровень снижения устойчивости сети пропорционален средней длине направления связи.

В работе [200] для обоснования временных параметров радиоэлектронного воздействия, направленного на нарушение функционирования протоколов маршрутизации с установлением соединения, была разработана модель функционирования информационного направления связи, учитывающая не только процесс реконфигурации отдельных маршрутизаторов вследствие отказа каналов, но и учет структуры соединений, а также принятого подхода в сети к резервированию путей. Результаты моделирования эффектов от радиоэлектронного воздействия показывают, что сети связи на основе протокола маршрутизации с установлением соединения снижают свою устойчивость за счет снижения устойчивости соединений, проходящих через узлы, подвергшиеся воздействию. При этом уровень снижения устойчивости пропорционален количеству узлов, на которые осуществляется воздействие. На основе этой модели в дальнейшем была разработана методика обоснования временных параметров радиоэлектронного воздействия на протокол маршрутизации с установлением соединений, которая позволяет обосновать временные параметры динамических помех, снижающих устойчивость сети до значений ниже требуемых.

Для подтверждения адекватности разработанного научно-методического аппарата обоснования способов радиоэлектронного воздействия и практического подтверждения эффектов функционального подавления сетей были проведены экспериментальные исследования на основе сети с протоколом OADV (Ad hoc On-Demand Distance Vector), результаты которых представлены в работе [196]. Сравнение теоретических расчетов и полученных эксперименталь-

ных данных позволяет сделать вывод о практическом подтверждении возможностей таких радиоэлектронных воздействий осуществлять эффективное функциональное подавление сетей.

Вышеуказанные перспективные направления разработки радиоэлектронных воздействий, ориентированных на сетевой уровень модели OSI, могут быть реализованы территориально-распределенными «традиционными» комплексами РЭП за счет введения режима динамических низкоэнергетических помех, временные параметры которых согласованы с параметрами протокола маршрутизации используемых в подавляемой сети.

Дополнительно был проведен анализ влияния криптографической защиты информации в каналах связи на эффективность рассматриваемых радиоэлектронных воздействий. Данный анализ показал, что использование стандартных VPN и криптомаршрутизаторов с пакетным режимом передачи (которые составляют подавляющее большинство современных решений криптозащиты) не является затруднением для подобных радиоэлектронных воздействий и позволяет максимально реализовать их функционал для подавления как сетей, так и отдельных информационных направлений связи.

3. Радиоэлектронные воздействия, ориентированные на нарушение функционирования протоколов обеспечения качества обслуживания в объединенных сетях связи. Перспективным направлением разработки радиоэлектронных воздействий, ориентированных на подавление объединенных сетей на транспортном уровне модели OSI, является разработка воздействий, ориентированных на формирование трафика и нарушение функционирования протоколов обеспечения качества обслуживания.

Так, перспективными радиоэлектронными воздействиями являются воздействия, ориентированные на формирование в канале связи потока пакетов сложной структуры с коэффициентом вариации больше единицы и существенно отличающегося от простейшего. Анализ результатов моделирования обработки потоков сложной структуры в узлах коммутации сети, представленный в работах [415, 416], показал, что своевременность обработки таких потоков в десятки раз ниже относительно обработки простейших потоков! При этом данный эффект наблюдается на высоконагруженных коммутаторах.

Первый вариант такого радиоэлектронного воздействия представлен в работе [204] и основан на внедрении дополнительного имитационного трафика, что позволяет сформировать выходной поток пакетов из канала связи со структурой, существенно отличающейся от простейшего (коэффициент вариации больше единицы). Отличительной особенностью этого воздействия является необходимость внедрения дополнительных пакетов, которые являются копиями ранее переданных пакетов, что в ряде случаев может привести к «разрушению» информационного потока. Кроме того, ряд протоколов (например, IPSec) нумеруют пакеты внутри сессии передачи данных, что позволяет им обнаруживать внедренные пакеты в трафик. Указанного недостатка лишен второй вариант РЭИВ, ориентированный на полный перехват и преобразование структуры информационного потока [205].

Оценка результатов воздействия указанных радиоэлектронных воздействий, ориентированных на формирование передаваемого в сети трафика сложной структуры, критичного к задержкам, показала, что устойчивость сети снижается за счет снижения своевременности обслуживания трафика в ее узлах и фактической блокировки узлов, передающих сложный трафик. Данные радиоэлектронные воздействия представляют собой вариант сложной DOS-атаки. Кроме того, эффект воздействия проявляется в том, что сформированные информационные потоки передаются дальше по сети, снижая своевременность обработки и в других узлах. Таким образом, данные радиоэлектронные воздействия способны адресно подавлять отдельные информационные направления связи. При этом уровень снижения устойчивости сети при таких воздействиях пропорционален количеству модифицированных информационных потоков, их скорости, а также средней длине направления связи.

Дальнейшим перспективным развитием направления создания радиоэлектронных воздействий, ориентированных на подавление сетей на транспортном уровне, является разработка комплекса моделей, отражающих процесс функционирования модели Diff Serv при обеспечении качества обслуживания абонентов и информационных потоков, а также технологий формирования трафика (traffic shaping) и технологий контроля параметров трафика (traffic policing) в условиях направленных деструктивных воздействий. Наличие таких моделей позволит обосновать множество радиоэлектронных воздействий, ориентированных на функциональное подавление современных сетевых технологий обеспечения качества обслуживания. Их применение не позволит обеспечить требуемые значения показателей функционирования объединенной сети связи, а именно — снизить вероятность устойчивости информационного направления связи и повысить вероятность отказа обслуживания.

Перспективные направления разработки радиоэлектронных воздействий, ориентированных на транспортный уровень сетей связи, могут быть реализованы как комплексами территориально распределенных средств РЭП, реализующих принципиально новые способы подавления, так и аппаратно-программными закладками и специальными программными средствами (вирусами), внедряемыми в телекоммуникационное оборудование сети.

Необходимо отметить, что применение всех вышеуказанных радиоэлектронных воздействий целесообразно исключительно против пакетных сетей с развитой топологией. Применение подобных воздействий против сетей с древовидной топологией бессмысленно ввиду возможности достижения эффекта подавления «классическим» подавлением каналов.

Таким образом, одним из наиболее перспективных способов противодействия сетецентрической системе военного управления является применение радиоэлектронных воздействий, ориентированных на синтаксический слой сетецентрической среды и нарушающих свойство доступности информационных ресурсов этой среды за счет воздействия на подсистему связи. Перспективные способы радиоэлектронных воздействий, ориентированные на подавление сетей, будут использовать эффекты деструктивного воздействия на физическом уровне как основу для формирования эффектов подавления на канальном, сете-

вом и транспортном уровнях модели OSI. При этом к новым на данном этапе проведения исследований, и в достаточной степени проработанным способам радиоэлектронных воздействий можно отнести следующие:

- способ радиоэлектронного воздействия на канальном уровне, ориентированный на перегрузку сетей множественного доступа, за счет динамического изменения ОСШП в общем радиоканале [190, 191];
- способ радиоэлектронного воздействия на канальном уровне, ориентированный на перегрузку систем многоканальной связи за счет периодического подавления отдельных каналов связи в такой системе [412];
- способ радиоэлектронного воздействия на сетевом уровне, ориентированный на снижение эффективности протоколов маршрутизации в сети за счет периодического изменения пропускной способности отдельных каналов связи сети, что приводит к динамическому изменению топологии [192, 196, 198, 199, 200, 413, 414];
- способ радиоэлектронного воздействия на транспортном уровне, ориентированный на снижение эффективности протоколов обеспечения качества обслуживания в сети за счет направленного формирования сложной структуры передаваемого трафика [204, 205].

В качестве цели для таких радиоэлектронных воздействий целесообразно рассматривать космический сегмент информационной подсистемы сетецентрической системы военного управления, так как он, с одной стороны, осуществляет глобальные функции информационного обеспечения, а с другой — строится на основе средств радиосвязи и вследствие этого уязвим для применения средств РЭП [371, 411].

В целом, новизной этих способов радиоэлектронных воздействий является использование «традиционных помех» для порождения и развития внутрисистемных конфликтов в системе связи на верхних уровнях ее функционирования [201]. В частности, рассматриваются помехи с динамически изменяемыми параметрами, которые приводят к переходным и нестационарным процессам на верхних уровнях OSI. Достигаемый новый военно-прикладной эффект — подавление сети связи в целом, в том числе и проводного сегмента, за счет воздействия через радиоканалы как своеобразные «точки входа радиоэлектронного воздействия». В настоящее время автор планирует теоретическое обобщение отдельных радиоэлектронных воздействий в рамках разработки теоретических основ моделирования динамического многоуровневого информационного конфликта системы связи и системы воздействия. В направлении данного развития опубликованы работы [194, 201], а также продолжаются дальнейшие исследования.

2.8.5. Перспективные технологии РЭБ (на основе анализа проектов DARPA)

Разработка новых систем РЭБ требует существенного научно-технического задела во многих областях фундаментальной и прикладной науки. Ниже представлены основные тенденции перспективных исследований, проводимых в интересах совершенствования систем РЭБ на примере анализа проектов,

выполняемых Агентством передовых оборонных исследовательских проектов Министерства обороны США — DARPA.

DARPA — агентство передовых оборонных исследовательских проектов в структуре Министерства обороны США, целями которого являются сохранение технологического превосходства ВС 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. Несмотря на то, что деятельность DARPA концентрируется преимущественно на военной проблематике, заметная часть его программ посвящена разработке технологий, имеющих двойное назначение. 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 [234].

Далее представлена краткая характеристика проектов DARPA за 2015 г., которые напрямую или опосредованно ориентированы на формирование научно-технического задела в области РЭБ.

2.8.5.1. Технологии радиотехники

Программные алгоритмы и методы адаптивной РЭБ — Behavioral Learning for Adaptive Electronic Warfare (BLADE). 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 их 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].

Адаптивное средство радиопомех — Adaptive Radar Countermeasures (ARC). В современном бою широко используются средства РЭП РЛС противника. Программа ARC предусматривает создание средств эффективного противодействия РЛС противника, работающих в адаптивном режиме, для повышения живучести собственных боевых авиационных платформ. Новые 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. Технология ARC будет

основана на технологии самообучающихся машин и разработке алгоритмов подавления нового поколения, которые могут использоваться существующими системами РЭП для обеспечения их носителям превосходства в воздухе [234].

Адаптивные радиочастотные технологии — Adaptive Radio Frequency Technology (ART). Программа ART предусматривает удовлетворение потребности вооруженных сил в доступных, компактных, энергетически эффективных коммутационных и сенсорных интерфейсов 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].

Адаптивная фазированная антенная решетка — Adaptive Phased Antenna Array (APAA). 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 АФАР в одну [234].

Разработка цифрового приемника широкого диапазона — Direct SAMpling Digital ReceivER (DISARMER). Программа предназначена для производства гибридных фотонно-электронных аналого-цифровых преобразователей, способных работать во всём 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 РТР, так как потенциально позволяет существенно сократить расходы, размер и вес таких систем [234].

Перспективные приемо-передающие устройства миллиметрового диапазона длин волн — Millimeter-wave Frequencies Transceiver. Программа MWFT предусматривает развитие систем связи, радиолокации, радиоразведки и РЭБ на основе приемопередающих средств в миллиметровом диапазоне длин волн. Это позволит обеспечить как уменьшение загруженности приемо-передающих трактов при заданной пропускной способности системы, так и снижение вероятности обнаружения и перехвата радиосигнала вероятным противником. Реализация программы будет основана на использовании набора широкополосных приемо-передающих устройств с высоким динамическим диапазоном и фотонных компонентов, обладающих высокими характеристиками скорости обработки данных мониторинга в миллиметровом диапазоне длин волн [234].

Технологии повторного использования спектра радиочастот — Spectrum Efficiency and Access. В настоящее время в связи с широким распростра-

нением радиосредств гражданского и военного назначения остро стоит вопрос нехватки имеющейся полосы частот. Министерству обороны необходимы технологии, нуждающиеся в меньшей ширине спектра. Программа предусматривает разработку принципов повторного использования спектра, например совместное использование частот и координации между средствами РРТР, РЛС, РЭБ и системами связи [234].

Новые алгоритмы и принципы для систем передачи информации на поле боя — Computational Leverage Against Surveillance Systems (CLASS). 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. Программа будет сосредоточена на трех основных исследовательских направлениях [234]. Во-первых — разработка сигналов сложной формы, не поддающихся анализу и дешифровке без знания их исходных свойств и параметров модуляции. Во-вторых — пространственное распределение приемо-передающих систем, позволяющее динамически и адаптивно изменять кажущееся положение источника полезного сигнала для средств РТР и РЭП вероятного противника. В-третьих — управляемая интерференция для многопозиционных систем передачи, которая учитывает естественный рельеф местности и позволяет создавать зоны «гашения» сигнала в местах дислокации противника.

Гарантированная функциональность коммуникационных систем за пределами прямой видимости — Assured Beyond Line-of-Sight Communications (ABLSC). 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].

2.8.5.2. Технологии электроники

Кортикальный процессор — 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. Существующие вычислительные подходы в подавляющем большинстве ресурсоемки и способны извлечь лишь ограниченную часть полезной информации из больших объемов данных. Современный машинный интеллект систем РТР и РЭБ плохо распознаёт 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].

Терагерцовая электроника — Terahertz Electronics. Переход в терагерцовый диапазон позволит в будущем создавать РЛС высокого разрешения, близкого к разрешению оптико-электронных систем, надежные системы связи с миниатюрными антеннами, а также высокоэффективные системы РТР и РЭБ, ориентированные против таких РЛС и систем связи. Программа предусматривает разработку и демонстрацию материалов и технологий производства транзисторов, микросхем приемников и задающих генераторов терагерцовых частот, а также малогабаритных мощных усилителей с масштабированными вакуумными приборами [234].

Разнообразные методы интеграции разнородных электронных систем — Diverse & Accessible Heterogeneous Integration (DAHI). Характеристики электронных микросистем играют важную роль 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 программы DAHI проводятся исследования по поиску новых методов и технологий интеграции, позволяющих комплексировать электронные микросистемы различного назначения и материалов изготовления в единой микросхеме [234].

2.8.5.3. Технологии вычислительных систем

Нетрадиционная обработка сигналов для интеллектуального использования данных — Unconventional Processing of Signals for Intelligent Data Exploitation (UPSIDE). 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 ЭВМ, реализующая «мягкие» вычисления, с более низким энергопотреблением, чем сравнимые с ней по вычислительной мощности традиционные компьютеры [234].

Технологии вероятностного программирования для самообучающихся машин — Probabilistic Programming for Advancing Machine Learning (PPAML). В этой программе разрабатываются интеллектуальные машины, которые будут обучаться с помощью алгоритмов вероятностного программирования, обрабатывать базы данных сигналов большого объема и выбирать наилучшие варианты решения задач, в том числе задач РРТР и РЭБ. Разработанный в ходе этой программы искусственный интеллект поможет более эффективно

решать множество аналитических задач — таких как обнаружения сигналов, радио и радиотехническая разведка, анализ сигналов в поисках ценных источников. При этом предполагается использование самых различных аппаратных платформ — суперкомпьютеров на базе многоядерных процессоров, кластеров обычных ПК и облачных сетей [234].

Высокоэффективные встраиваемые вычислительные системы — Power Efficiency Revolution For Embedded Computing Technologies (PERFECT). Программа PERFECT решает проблему нехватки вычислительных ресурсов для создания встраиваемых цифровых систем нового поколения. В рамках программы должны быть созданы новые компьютерные системы производительностью 75 Гфлопс/Вт, при этом действующие системы показывают пока в 75 раз худшие результаты. Согласно результатам предварительных экспериментов, нижняя граница энергетической эффективности 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.

Разработки в рамках проекта PERFECT подразумевают работы по пяти основным направлениям [234]: программно-аппаратная архитектура; параллельная обработка множества потоков; устойчивость системного и прикладного ПО по отношению к программным ошибкам и преднамеренным воздействиям; оптимизация трафика обрабатываемых данных; новые алгоритмы, обеспечивающие высокую устойчивость работы и низкое потребление энергии.

Создание защищенной облачной инфраструктуры, обеспечивающей сетевую поддержку военных операций, — Mission-oriented Resilient Clouds (MRC). 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 средствами РЭБ, а ключевые узлы вследствие побочных эффектов функционируют со сбоями [234].

2.8.5.4. Технологии разведки, наблюдения и целеуказания

Перспективные технологии радиочастотного картирования местности на поле боя — Advanced RF Mapping. Одним из ключевых аспектов достижения превосходства на поле боя является возможность эффективного использования и управления радиочастотным диапазоном для обеспечения надежного функционирования своих систем связи и разведки, одновременно с подавлением средств потенциального противника. В рамках программы ARFM планируется разработка системы управления информацией, передаваемой в радиочастотном диапазоне, на основе совокупности распределенных сенсорных и вычислительных блоков, а также демонстрация функциональных преимуществ нового подхода по сравнению с традиционным централизованным, в условиях, максимально приближенных к реальным боевым, включая подавление точек связи потенциального противника [234].

Радиоэлектронные системы наблюдения и разведки открытой архитектуры — Software-Defined ISR (SDISR). 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 и будет востребовано при разработке перспективных средств РРТР [234].

3. Информационное противоборство

3.1. Актуальность развития информационных средств и способов воздействия в современных сетецентрических войнах

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 [318].

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 сбора, передачи обработки и представления информации а также системы управления [318].

К субъектам информационного противоборства относят: государства, их союзы и коалиции; международные организации; негосударственные незаконные вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности (в том числе международные); транснациональные корпорации; виртуальные социальные сообщества; медиакорпорации и СМИ; виртуальные коалиции [318].

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 это 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. Другими словами, 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 в коалициях[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 информа-

ционных 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. Специалисты полагают, что такое построение защиты важных информационных ресурсов Пентагона заставит потенциальных противников США расходовать значительные средства, чтобы получить возможности для ее преодоления [95].

3.2. Развитие подходов к месту и роли информационного противоборства в современных сетецентрических войнах

Изменение подходов к асимметричным и сетевым способам военных действий повлияло на оценку роли информационного противоборства в будущих конфликтах. Сегодня ряд американских военных специалистов придерживаются точки зрения, согласно которой информационное противоборство понимается ими гораздо шире, нежели просто вид обеспечения операций ВС путем нарушения процессов контроля и управления войсками, радиоэлектронного подавления и др.

3.2.1. Взгляды экспертов RAND Corporation на стратегическое информационное противоборство

В 1995 г. компании RAND Corporation было поручено проведение ряда исследований в рамках мероприятий, проводимых МО США с целью выявления национальных приоритетов в концепции информационного противоборства. Результат этих работ, который должен был служить в качестве подготовительного этапа к осмыслению роли и места информационного противоборства в национальной военной стратегии США, был изложен в отчете за номером MR-661-OSD Strategic Information Warfare. A new face of War (1996 г.) [2, 16, 206, 207].

В дальнейшем полученные результаты получили свое эволюционное развитие и были опубликованы в отчетах MR-963-OSD The Day After … in the American Strategic Infrastructure (1998 г.) и MR-964-OSD Strategic Information Warfare Rising (1998 г.) [2, 16].

Сотрудники RAND Corporation выдвинули концепции кибернетического и сетевого противоборства, предположив, что в ходе будущих военных конфликтов решающую роль будет играть информация, а ключом к успеху станет достижение информационного превосходства.

По мнению исследователей RAND Corporation, концепция кибернетической войны становится всё более актуальной, особенно когда речь идет о конфликтах высокой интенсивности. Кибернетическая война подразумевает достижение превосходства над противником за счет широкого внедрения новых технологий в системах боевого управления и связи и, что особенно важно, совершенствования организации и управления в военной области [16].

Роль сетевого противоборства возрастает в конфликтах низкой интенсивности и при проведении так называемых «операций, отличных от войны»,

а также в конфликтах, террористических действиях и специальных операциях, носящих невоенный характер. Концепция сетевой войны подразумевает использование информационных инфраструктур противника в своих целях. В этом отношении данный вид информационного воздействия имеет много общего с ведением террористической борьбы, в которой главными действующими лицами выступают небольшие взаимосвязанные и координирующие свои действия группы, не имеющие единого командования. В подобном случае можно говорить, что организационная структура строится не на иерархическом, а на сетевом принципе [16].

Таким образом, согласно экспертной группе RAND Corporation, основные отличия между сетевым и кибернетическим противоборством касаются исключительно интенсивности конфликта. Они являются более сложными формами будущих военно-политических конфликтов, в ходе которых в борьбе за информационное доминирование будут использоваться социальные и национальные особенности сторон, вовлеченных в конфликт [16].

Важным результатом исследований, как следствие осознания возможностей информационного оружия, стало появление термина «strategic information warfare» — *стратегическое информационное противоборство,* который определяется как «…использование государствами глобального информационного пространства и инфраструктуры для проведения стратегических военных операций и уменьшения воздействия на собственный информационный ресурс…». Появление такой терминологии существенным образом отличается от официальной трактовки информационного противоборства, закрепленной в директиве Министерства обороны США DOD TS 3600.1 (декабрь 1992 г.), которая трактует информационное противоборство в достаточно узком смысле [2].

В отчете RAND Corporation MR-661-OSD отмечается, что изменения в общественно-политической жизни ряда государств, вызванные быстрыми темпами информатизации и глобализации общества, ведут к пересмотру геополитических взглядов руководства этих стран, к возникновению новых стратегических интересов (в том числе и в информационной сфере), которые приводят к изменению политики, проводимой этими государствами. Учитывая, что один из основных тезисов сформированных К. Клаузевицем — «война есть продолжение политики другими средствами», то разрешение глобальных противоречий потребует новых средств и методов их разрешения — стратегического информационного противоборства [2].

В отчете MR-964-OSD введена классификация стратегического противоборства на первое и второе поколения.

Стратегическое информационное противоборство первого поколения рассматривается наряду с традиционными средствами противоборства (ядерными, химическими, биологическими и др.) и в большей степени ориентировано на дезорганизацию деятельности систем управления (преимущественно технического характера) и проводится скорее как обеспечение действий традиционных сил и средств. Такое восприятие информационного противоборства свойственно начальному этапу осмысления этой проблемы. В отчете MR-964-OSD стратегическое информационное противоборство первого поколе-

ния определено как «… одна из нескольких компонент будущего стратегического противоборства, применяемая совместно с другими инструментами достижения цели …» [2].

Стратегическое информационное противоборство второго поколения (2nd generation Strategic Information Warfare) — «… принципиально новый тип стратегического противоборства, вызванный к жизни информационной революцией, вводящий в круг возможных сфер противоборства информационное пространство и ряд других областей (прежде всего экономику) и растянуто во времени на недели, месяцы и годы …» [2].

Экспертами RAND Corporation отмечается, что развитие и совершенствование подходов к ведению стратегического информационного противоборства второго поколения приведет к полному отказу от использования силы, поскольку скоординированные информационные акции просто не позволят применить ее. Подчеркивается, что, если последствия стратегического информационного противоборства первого поколения еще могут быть прогнозируемы с использованием существующих методик, то второе поколение противоборства на текущий момент весьма трудно формализуемо и существующие методики прогноза могут быть применены к анализу ее последствий весьма условно.

К основным задачам, которые решаются посредством ведения информационного противоборства второго поколения, относят следующие [2]:

- создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию противника;
- манипулирование общественным сознанием и политической ориентацией социальных групп населения страны с целью создания политической напряженности и хаоса;
- дестабилизацию политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигания недоверия, подозрительности, обострения политической борьбы, провоцирование репрессий против оппозиции, провокация взаимоуничтожения;
- снижение уровня информационного обеспечения органов власти и управления, инспирация ошибочных управленческих решений;
- дезинформацию населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;
- провоцирование социальных, политических, национальных и религиозных столкновений;
- инициирование забастовок, массовых беспорядков и других акций экономического протеста;
- затруднение принятия органами управления важных решений;
- подрыв международного авторитета государства, его сотрудничества с другими странами;
- нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и в других сферах.

Необходимо отметить, что большинство положений, представленных в отчетах RAND Corporation, вошло в успешно реализуемую в ВС США концеп-

цию сетецентрической войны, хотя они всё же не получили своего прямого продолжения. Это представляется особенно важным, поскольку устанавливает связь между прикладными проблемами реформирования ВС США и более ранними теоретическими построениями, касающимися ведения информационной войны.

Таким образом, американские военные эксперты ко второй половине XX века значительно продвинулись в развитии методологии использования информационной сферы как новой сферы противоборства. В ряде конфликтов была отработана первоначальная концепция ведения информационной войны. Были определены ее слабые звенья. При этом главным вопросом был вопрос о создании единой общегосударственной информационной стратегии, поскольку только в масштабах всего государства, с привлечением всех доступных средств возможно ведение эффективной информационной войны.

3.2.2. Концепция стратегического информационного доминирования, разработанная экспертами Университета ВВС США

Как показал анализ работ [16, 208–211] представителей теоретической группы Университета ВВС США (Air University, Maxwell Airforce Base, Alabama) — Дж. Стейна, Р. Шафрански и О. Дженсена, — они полагали, что в будущих военных конфликтах решающую роль будет играть сама информация, которая при этом она будет являться одновременно и оружием, и целью конфликта.

Данные специалисты предполагали, что вследствие развития концепции информационной войны устаревшими окажутся не только традиционные системы вооружений, но и считающиеся в настоящее время перспективными системы ВТО, комплексы боевого управления и разведки. Новые информационные технологии позволят вести боевые действия на уровне сознания за счет комплекса информационно-психологических операций, активно использующих информационные сети и различные СМИ для адаптированной пропаганды и создания у противника искаженной картины мира.

Информационные технологии в этом случае рассматривались только как средство, облегчающее *стратегическое информационное доминирование*, под которым в данном случае понимается создание таких информационных условий, в которых действия противника в конечном итоге неизбежно окажутся выгодными противоположной стороне или будут направлены на обслуживание ее интересов.

В значительной мере с концепцией, предложенной аналитиками Университета ВВС США, согласуется мнение одного из теоретиков в области информационного противоборства — М. Либики [16, 212], — который акцентируется не на психологическом, а на экономическом и военном (в традиционном смысле) аспектах.

По его мнению, в будущем информация станет основным средством сдерживания вооруженных конфликтов, так как взаимосвязанная информационная система, состоящая из сети космических спутников слежения, наземных,

воздушных и морских датчиков, позволит контролировать любую военную активность на планете, а значит, позволит применять превентивные меры.

В таких условиях любые действия потенциального агрессора будут абсолютно прозрачны для противоположной стороны и международного сообщества в целом. Соответственно, агрессор может быть лишен даже самой возможности провести военные приготовления, поскольку глобализация мировых информационных систем позволит парализовать и отрезать его экономические и информационные системы от остального мира.

3.2.3. Концепции «стратегического паралича» и «навязанной стоимости»

В интересах развития теории информационного противоборства О. Иенсеном предложена концепция «стратегического паралича», задача которой — сделать дальнейшее сопротивление противника невозможным [16].

В качестве основных целей воздействия (по степени убывания приоритетов целей) в соответствии с данной концепцией при проведении соответствующих информационных операций определены [16]:

- политическое и военное руководство страны;
- базовое производство (промышленность, энергетика);
- инфраструктура (транспорт, коммуникации);
- гражданское население;
- воинские подразделения.

Степень воздействия на государственную систему противника в целом будет определяться конкретными задачами, которые призван решить конфликт. При этом наиболее важным О. Иенсен считает нарушение функционирования или уничтожение любых средств передачи информации.

С данной концепцией согласуется концепция «навязанной стоимости», автором которой является полковник ВВС США Дж. Варден. Согласно концепции «навязанной стоимости», если противнику удастся навязать такой образ действий, который впоследствии окажется слишком затратным для него, то противник в конечном итоге откажется от продолжения борьбы [16].

Реализация указанной стратегии предполагает проведение следующих мероприятий [16, 212]:

- оценка системы ценностей противника, его сильных и слабых сторон;
- определение на основе полученных сведений «болевого порога» противника;
- осуществление информационных операций, направленных на достижение и превышение этого порога, с целью вызвать частичный паралич и создать угрозу полного паралича деятельности командных структур противника.

Как предполагается разработчиками, такая стратегия позволит урегулировать конфликт уже на стадии психологического воздействия на управляющее звено противника либо на ранних стадиях боевых действий.

Рассмотренные выше различные теоретические концепции ведения информационного противоборства не только являются объектом самого серь-

езного обсуждения в научных кругах ведущих зарубежных стран, но и используются при разработке соответствующих мероприятий.

Анализ теоретических построений позволяет выявить общий вектор развития теории информационного противоборства. В частности, наиболее характерная черта подходов середины XX века заключается в том, что основное внимание в них, в отличие от предыдущих, уделялось уже не собственно технической (технологической) стороне проблемы, а организационным и психологическим аспектам информационных войн. Причем сама по себе информация рассматривалась как цель и средство действий, предпринимаемых для разрешения конфликта.

Подобное изменение приоритетов не снимет задачи разработки и совершенствования технических аспектов информационных технологий, поскольку они выступают необходимыми компонентами и технической основой информационной войны. Классифицируя рассмотренные подходы в соответствии с теми объектами, на которые предполагается оказывать целенаправленное информационное воздействие в ходе ведения информационного противоборства, можно выделить четыре основные группы таких целей [16, 208]:

- системы управления и принятия решений (гражданские, военные, социальные, культурные);
- гражданская информационная инфраструктура (системы телекоммуникации, информационные системы транспорта, энергетики, финансов, промышленности);
- военная информационная инфраструктура (системы контроля, управления и связи, разведка);
- системы вооружений.

Указанные цели могут подвергаться различному воздействию в ходе конкретных информационных операций. Кроме того, информационные системы могут сами стать средой, в которой ведется противоборство.

Проведенный анализ позволяет выделить следующие направления ведения информационного противоборства [16, 208]:

- борьба с системами управления;
- информационно-разведывательные операции;
- радиоэлектронная борьба;
- психологические операции;
- «хакерская» борьба;
- «кибернетическое» и сетевое противоборство;
- экономическая информационная борьба.

3.2.4. Операции на основе эффектов — третье поколение методов информационного противоборства, ориентированных на использование в сетецентрических войнах

В июле-августе 2002 г. в США прошли масштабные учения «Millennium Challenge — 2002», к которым было привлечено более 13 500 человек личного состава всех родов войск. Бюджет учений составил более 235 млн долларов. Цель учений — отработать связанность и взаимодействие частей и подразделе-

ний всех родов войск ВС США, а также порядок взаимодействия с другими федеральными ведомствами в ходе проведения «быстрых решающих действий».

Как отмечают военные эксперты армии США, «быстрые решающие действия» RDO (Rapid Decisive Operations) — новая форма военных действий в сетецентрической войне. RDO сосредоточены прежде всего на оперативном уровне, однако понятие RDO имеет также стратегические и тактические значения. Подготовка к RDO является целенаправленной и непрерывной, сосредотачиваясь на действиях, позволяющих влиять на поведение противника и удерживать его от принятия тех или иных решений. В том случае, если сдерживание терпит неудачу, RDO обеспечивают способность к быстрому и решительному принуждению или нанесению поражения противнику с целью достичь стратегических целей без длительной кампании или масштабного наращивания сил. RDO может быть успешной как сама по себе, так и, если необходимо, подготовить условия для перехода к действиям в ходе масштабного регионального конфликта с применением тяжелого вооружения.

Основой «быстрых решающих действий» является концепция сетецентрической войны (Network-Centric Warfare — NCW). Концепция сетецентрической войны представляет собой мощный набор способов и форм противоборства, которые позволяют ВС получить полное преимущество над противником, используя всю доступную информацию об окружающем пространстве, о противнике и о собственных силах.

По мнению авторов концепции «быстрых решающих действий», сегодня даже среди традиционных государственных игроков различие между враждебностью и невраждебностью практически нивелируется, поскольку новые способы воздействий (типа вторжений в компьютерные сети) мешают точно определить, когда была пересечена линия враждебности [2].

Аналитики Пентагона отмечают, что сегодня, несмотря на существенное технологическое, экономическое и военное превосходство, целый ряд региональных держав и межнациональных коалиций имеют потенциал, позволяющий угрожать национальным интересам высокоразвитых государств. Противники будут искать возможности достичь цели прежде, чем высокоразвитые государства смогут ответить на вызов. При этом противник не будет пытаться наносить поражение американским силам в симметричной открытой конфронтации, а скорее будет пытаться наносить поражение американской воле, используя асимметричные нападения, блокируя возможность доступа и, если необходимо, втягивая их в длительный, вялотекущий и изматывающий конфликт [2].

Также предполагается, что противник будет пытаться блокировать доступ ВС к ТВД, используя широко доступные современные системы вооружений. Цель противника в этом случае будет состоять в том, чтобы заставить армию высокоразвитого государства сомневаться в своей способности победить в пределах приемлемых затрат. Противник будет пытаться противостоять высокотехнологичным способностям войны за счет применения маскировки, хитрости и рассредоточения своих сил. Он также будет использовать сложные информационные действия, чтобы воздействовать на волю к победе [2].

На этом фоне произошедшие глубокие изменения в информатике, биологии, космических исследованиях, а также в ряде других областей науки позволяют с принципиально новых позиций подойти к развитию военной науки. Парирование новых угроз, созданных новейшими технологиями, может быть весьма трудной задачей для традиционных вооруженных сил. Сегодня, в эру информационной глобализации, не может быть ясных линий между враждебным и невраждебным или политическим и военным действиями. Действия противника будут простираться далеко за пределы открытых военных действий и могут включить террористические акты и атаки на компьютерные сети. При этом исполнителей таких акций будет очень тяжело обнаружить. Даже после их обнаружения они могут смешаться с мирным населением, делая сложным нанесение ответного удара. В этих условиях необходимо оперировать в континууме многомерного политического, военного, экономического, социального и информационного пространства, в котором как сами цели, так и интенсивность взаимодействия с потенциальными противниками могут быстро меняться [2].

В этой связи эксперты Пентагона отмечают, что существующие сегодня вооруженные силы высокоразвитых государств, с их подавляющим превосходством в обычном военном конфликте с равным по силе противником, не обладают средствами, с помощью которых возможно полностью доминировать над новой оперативной средой — информационным пространством. Американскими военными отмечается, что, начиная с развала СССР, США изменили численность ВС времен «холодной войны» и создали их уменьшенную копию. Однако большинство доктрин времен «холодной войны», принципы действий, планирование и строительство вооруженных сил остаются неизменными. США удалось увеличить эффективность отдельных компонентов вооруженных сил с появлением преимуществ «революции в военном деле», но не удалось повысить эффективности применения военной силы в целом [2].

По мнению ряда экспертов, ограничения «традиционных» ВС включают [2]:

- 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 и др.

Кроме этого, отмечается, что сегодня ВС США имеют непревзойденную способность собирать информацию об окружающем пространстве, о противнике и о собственных ВС, но испытывают недостаток в совместном планировании и управлении, чтобы использовать эту информацию для достижения превосходства в принятии решений. Также отмечается, что армия США, имея системы ВТО, которые способны поразить цель с большой точностью, испытывает сложности в способности последовательно производить желательные оперативные эффекты и заставлять противника принимать выгодные США решения [2].

Сегодня армия должна быть готова к быстрому переходу от относительно

мирного процесса противостояния до интенсивных боевых действий. И при этом быстро и решительно достигать стратегических целей. Считается, что военная мощь США в соединении с другими инструментами национальной мощи должна развивать способность ответить быстро и решительно разрешать конфликты в возможно более короткое время. При этом США планируют делать это, не теряя способности побеждать в случае развязывания крупномасштабного регионального конфликта с применением тяжелого вооружения [2].

Военные эксперты армии США считают, что для ответа на изменения, произошедшие в геостратегичесом пространстве в начале XXI века, США должны преобразовать путь, которым сегодня проводятся объединенные операции. Сегодня важно знать, как провести военные операции совместно с другими инструментами национальной мощи. Аналитиками отмечается, что базовыми характеристиками, которые описывают фундаментальные различия между будущими и сегодняшними объединенными действиями, является опора на знания и на эффекты [2].

Опора на знания. Информационное превосходство, основанное на превосходящих знаниях и лучшей информированности лиц, принимающих решения, позволит военным изменить будущие военные действия. Мощь сложных информационных систем обеспечит возможность беспрецедентного моделирования действий врага, собственных способностей армии, учета факторов окружающей среды и боевого пространства. Улучшенное ситуативное планирование позволит достичь превосходства в сроках и качестве принимаемых решений и 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 желательных эффектов [2].

Опора на эффекты. Действия на основе эффектов (Effect-based Operations, EBO) — концепция войны, которая сосредотачивается на получении желательного стратегического результата (эффекта) в поведении врага, через применение диапазона военных и невоенных мер на тактическом, оперативном и стратегическом уровнях [2].

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 концепции высокоточных ударов, доминирующих маневров и информационных операций на всём боевом пространстве с целью вызвать изменения в поведении противника [2].

Существенное значение в ходе военных действий будущего отводится информационным операциям. По мнению экспертов Пентагона, информационная операция — это информационный эквивалент маневра и огня. Информационная операция особенно эффективна, когда она реализуется в своей целевой области (в информационной сфере). Она также может использоваться и для поддержки огня и маневра в других сферах противоборства [2].

Информационные операции планируются к реализации для достижения

двух главных информационных эффектов[2]:

- технических эффектов;
- эффектов влияния.

Технические эффекты достигаются путем радиоэлектронных и информационных атак.

Эффекты влияния достигаются путем психологических операций, дезинформации, связей с общественностью, оперативной безопасности и специальных информационных операций.

При этом информационная операция обладает уникальными характеристиками, позволяющими применять ее как в мирное, так и в военное время. Эти характеристики включают низкий уровень разрушения физической инфраструктуры, низкие требования к развертыванию, высокую своевременность выполнения поставленных задач, низкий уровень риска для персонала [2].

Таким образом, подходы, основанные на информационных операциях, позволят администрации США с принципиально новых позиций подойти к проведению внешней политики США в XXI веке. Основой такой политики станет комплекс, прежде всего невоенных мер, направленных на создание «информационных эффектов», приводящих к изменению поведения конкретного субъекта международных отношений в выгодном для США направлении.

3.3. Основные термины и определения информационного противоборства

Адекватное описание противоборства в информационном пространстве потребовало формирования соответствующего терминологического базиса. В связи с этим в США и странах НАТО еще с 90-х гг. введены руководящие документы, определяющие эту терминологию, и зачастую именно ею руководствуются исследователи в данной области. Кроме того, различными научно-исследовательскими организациями и отдельными специалистами предложены свои варианты терминологии, которые ими широко используются при проведении НИОКР и публикации научных работ. В связи с тем, что всё это сильно затрудняет однозначное понимание процессов противоборства в информационном пространстве, предлагается рассмотреть вопросы терминологии данной предметной области более подробно.

В 1996 г. Министерство обороны США ввело в действие «Доктрину борьбы с системами контроля и управления» [275]. Этот документ впервые определял принципы борьбы с системами контроля и управления за счет применения информационной войны в военных действиях. В этом документе также были определены организационная структура, порядок планирования, обучения и управления ходом операции, а также основные понятия в этой области.

Основные взгляды командования ВС США, касающиеся информационного противоборства и информационной сферы как новой сферы ведения боевых действий, изложены в новой редакции доктрины «Информационные операции», принятой в 2006 г. В ней же определены цели, задачи и принципы информационных операций [95].

В дальнейшем данный документ был дополнен рядом подзаконных актов, что позволило управлению ВС США сформировать устойчивую, непротиворечивую терминологию в области информационной войны. Основы этой терминологии были представлены в руководящих документах ВС США [262–268, 271, 274, 275], международных стандартах ITU-T и ISO [278–280], а также обобщены в работах отечественных специалистов [2, 131, 270, 272, 277, 285, 286, 371].

3.3.1. Информационное пространство

Информационное пространство — область ведения информационной войны [2, 275].

Действия в информационном пространстве разворачиваются в [2, 275]:

- технической сфере;
- психологической сфере.

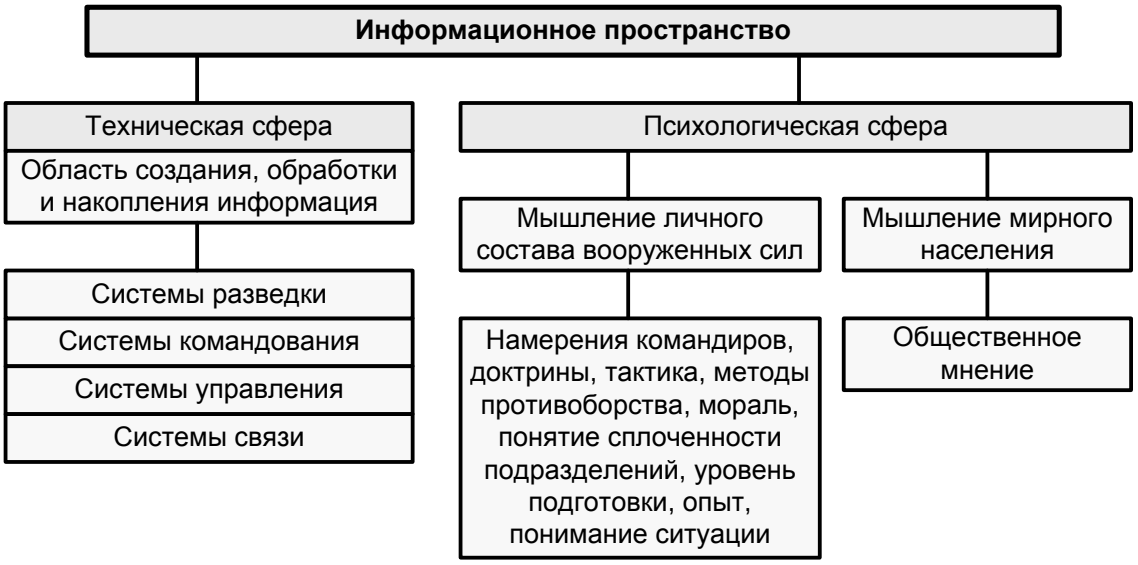


Рис. 3.1. Декомпозиция информационного пространства [2, 275]

Техническая сфера — область информационного пространства, в которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой функционируют системы управления, связи и разведки [2, 275].

В дальнейшем в ряде руководящих документов развитие и уточнение понятия технической сферы информационного пространства привело к созданию понятийного аппарата *киберпространства.*

Психологическая сфера — область информационного пространства, которая объединяет мышление личного состава ВС и мирного населения. Это область, в которой формируются намерения командиров, доктрины, тактика, методы противоборства, мораль, понятие сплоченности подразделений, уровень подготовки, опыт, понимание ситуации и общественное мнение [2, 275].

Ряд экспертов ВС США считают целесообразным исключение участия физических средств поражения в информационных действиях (таких как пора-

жение пунктов управления, разрушение инфраструктуры и др.), поскольку эти действия происходят в физическом пространстве, которое является традиционной областью войны и объединяет традиционные сферы противоборства — землю, море, воздух и космическое пространство. То есть то пространство, в котором функционируют системы вооружения, военной техники и системы коммуникаций [2].

Одним из ключевых понятий, которым оперируют специалисты в области информационного противоборства США, является «информационная обстановка» которое по смысловому контексту созвучно «информационному пространству».

Информационная обстановка — совокупность людей, организаций и систем, собирающих, отрабатывающих, доводящих информацию или действующих на ее основе [284].

Элементы информационной обстановки — руководители, лица, принимающие решения (ЛПР), люди организации и системы [284].

Ресурсы информационной обстановки — материальные средства и системы, используемые для сбора, анализа, применения или доведения информации [284].

Включая понятия ресурса и элементов, можно дать следующее определение информационной обстановки: это сфера, в которой функционируют люди и автоматизированные системы — ведут наблюдение, ориентируются, принимают решения и действуют на основе информации. С этой точки зрения информационная обстановка является «основной обстановкой принятия решений» на земле, на море, в воздухе, в космосе и информационном пространстве.

По взглядам специалистов США, информационная обстановка состоит из трех измерений: физического, информационного, познавательного — рис. 3.2 [284].

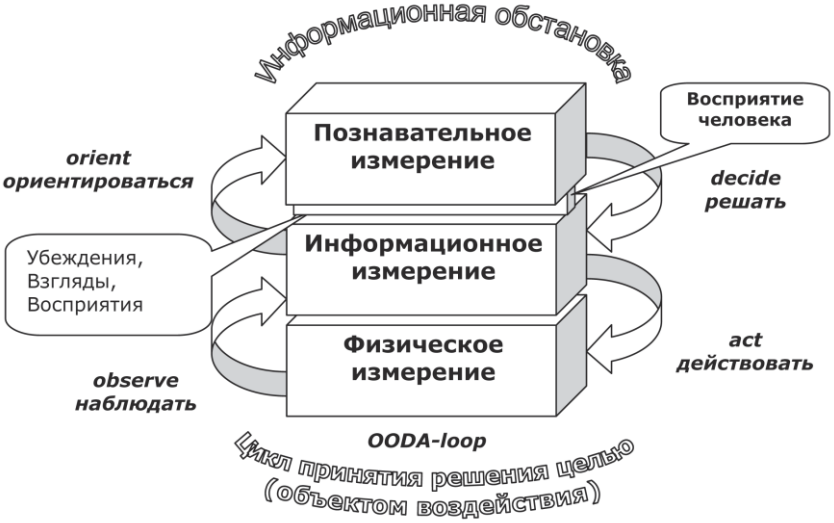


Рис. 3.2. Сферы информационной обстановки [284]

Физическое измерение — традиционная область войны. Эта область объединяет традиционные сферы противоборства — землю, море, воздух и косми-

ческое пространство. Это область, в которой функционируют физические платформы вооружений и технические системы управления и связи. Поэтому элементы этой области проще всего идентифицируемы. Боевая мощь в этой области традиционно измеряется эффектами физического поражения [2, 284].

Информационное измерение — область, в которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой существует логика функционирования систем управления, связи и разведки. В битве за информационное превосходство эта область является самой чувствительной к информационным воздействиям, так как именно это измерение связывает реальный физический мир с логикой функционирования технических систем сбора, передачи и обработки информации, а через них — с сознанием человека, функционирующим в познавательном измерении [2, 284].

Познавательное измерение — область мышления бойца и мирного населения. Это область, в которой формируются намерения командиров, доктрины, тактика, методы противоборства. Нематериальные активы лидерства, морали, сплоченности подразделений, уровень подготовки, опыта, понимания ситуации и общественного мнения — это всё элементы этой области. Познавательное измерение существует в сознании лица, принимающего решение. Это та область, где человек обрабатывает полученную информацию в соответствии с присущим ему комплексом норм, морали, убеждений, культуры и ценностей. Последние действуют в качестве «окна» для восприятия лица, принимающего решение при фильтровании информации и получении сознания значимости и взаимосвязи. Информация оценивается и анализируется, чтобы сформировать решения, которые передаются через информационное измерение в область физического мира [284].

Каждая из составляющих информационной обстановки может быть подвергнута определенному воздействию и являться объектом, который в определенных обстоятельствах может оказать решающее влияние на исход операции (войны) с учетом их концептуальной взаимосвязи в цикле принятия решения.

3.3.2. Киберпространство и кибербезопасность

С развитием понятийного аппарата информационного противоборства назрела объективная необходимость выделить часть терминологии, относящуюся непосредственно к противоборству в технической сфере информационного пространства. В Вооруженных силах США и НАТО такой терминологический базис введен через множество так называемых «киберпонятий».

Общее определение киберпространства впервые введено исследовательской службой конгресса США.

Киберпространство — всеохватывающее множество связей между людьми, созданное на основе компьютеров и телекоммуникаций вне зависимости от физического и географического положения [287].

В Министерстве обороны США, в Едином уставе комитета начальников штабов Вооруженных сил США [266] киберпространство определено следующим образом.

Киберпространство — сфера (область), в которой применяются различные РЭС (связи, радиолокации, разведки, навигации, автоматизации, управления и наведения) для приема, передачи, обработки, хранения, видоизменения (трансформации) информации и связанная с ними информационная инфраструктура ВС [266, 287].

В международном стандарте по кибербезопасности ISO/IEC 27032:2012 [278] киберпространство определено с учетом тенденций развития глобальной сети Интернет.

Киберпространство — среда, которая представляет собой следствие результата взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологий устройств и сетей, подключенных к ней, которых не существует в какой-либо физической форме [278, 287].

В стандарте по кибербезопасности ISO/IEC 27032:2012 [278] понятие *кибербезопасность* определено через понятие *киберпространство*.

Кибербезопасность — это безопасность в киберпространстве [278, 287].

Стандарт ISO/IEC 27032:2012 [278] определяет связи термина *кибербезопасность* с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур. В стандарте приводится визуализация связи этих различных терминов (рис. 3.3). С точки зрения международных экспертов все эти термины объединяет понятие *информационная безопасность*.

Рис. 3.3. Связь термина «кибербезопасность» с терминологическим базисом стандарта ISO/IEC 27032:2012 [278]

В рекомендации X.1205 МСЭ-Т [279] кибербезопасность определена через понятие киберпространства и систему управления рисками.

Кибербезопасность — набор средств, стратегий, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологий, которые могут быть использованы для защиты киберпространства, ресурсов организации и пользователя [279, 280, 287].

3.3.3. Информационная война

Проектом Конвенции [289] об обеспечении информационной безопасности ООН информационной войне дано следующее определение.

Информационная война — межгосударственное противоборство в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам; для подрыва политической, экономической и социальной систем; массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны [287].

В качестве основных определений в руководящих документах ВС США сформулировано следующее определение информационной войны.

Информационная война — широкомасштабная информационная борьба с применением способов и средств информационного воздействия на противника в интересах достижения целей воздействующей стороны [2, 275].

По направленности информационных воздействий информационная война, как правило, подразделяется на два основных вида [2, 275]:

- психологическая война (в ее составе некоторые специалисты выделяют информационно-психологическую войну);
- информационно-техническая война.

Ряд специалистов дает информационно-технической войне новое определение — ***техносферная война*** [62, 63].

Эксперты ВС США считают, что информационная война может проводиться во всех сферах общественной жизни — в экономике, политике, в военном деле, в социальных отношениях, в сфере духовной жизни и особенно в идеологии. При этом рядом специалистов США введены определения, расширяющие суть данного понятия относительно изложенного в документе [275].

Информационная война — комплексное воздействие на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника [2, 256].

Информационная война — соперничество и организованные действия (информационные операции) конфликтующих сторон в области информационных потенциалов, проводимые с целью снижения возможностей по использованию имеющегося государственного, военного и боевого потенциала противника и сохранения (повышения) возможностей по использованию собственного потенциала [2, 131, 293].

Информационный потенциал — совокупность информации, зафиксированной на материальных носителях или в любой другой форме, обеспечивающей ее передачу во времени и пространстве потребителям для решения широкого спектра задач, связанных с деятельностью государственных институтов, военно-промышленного комплекса и ВС; а также силы и средства, используе-

мые для получения, обработки, хранения и представления информации; умонастроения людей, использующих эту информацию и способных запускать и контролировать вещественно-энергетические процессы [131, 138].

Цель информационной войны — такое воздействие на противника, в результате которого он самостоятельно, без принуждения принимает благоприятные для атакующей стороны решения [2, 131, 275].

Объекты ведения информационной войны — информационные системы и сети обмена информацией (включая соответствующие линии передач, обрабатывающие центры и человеческие факторы этих систем), а также информационные технологии, используемые в системах вооружений [131].

Современное понимание информационной войны возникло в том числе и за счет развития работ американского специалиста Дж. Бойда. В этих работах обосновывается, что любая война включает в себя три элемента [13]:

1. ***моральную войну*** — разрушение воли противника к достижению победы путем его отделения от союзников (или потенциальных союзников) и внутреннего «раздробления», подрывая общую веру и общие взгляды;
2. ***ментальную войну*** — деформацию и искажение восприятия противником реальности на основе дезинформации и создания неправильных представлений о ситуации;
3. ***физическую войну*** — разрушение физических ресурсов противника (в случае информационной войны это — разрушение (подавление) инфраструктуры государственного и военного управления, информационных и телекоммуникационных систем и др.).

Информационная война состоит из совокупности информационных операций, проводимых в информационном пространстве в интересах достижения информационного превосходства.

При этом следует отличать информационную войну от компьютерной преступности. Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, может быть составной частью обширного плана атаки. Однако ведение войны никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации в качестве оружия для ведения боевых действий [131].

Как показано в работе [284], с течением времени содержательная часть понятия «информационная война» применительно к действиям ВС изменилась и в настоящее время в руководящих документах США и НАТО в основном используется термин «информационная операция». В то же время область применения термина «информационной войны» сместилась в сферу описаний глобальных противоречий между государствами и стратегического информационного противоборства.

3.3.4. Информационные операции

Информационные операции — действия, предпринимаемые для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры [2, 256, 270, 275].

Цель информационных операций — достижение информационного превосходства над противником.

Информационное превосходство — способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое [2, 275].

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

Информационное превосходство — способность обеспечивать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во всё время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных действиях [2, 270, 275].

Основные объекты воздействия в ходе информационных операций (рис. 3.4) [256, 270]:

- органы управления государства и его вооруженных сил;
- информационно-управляющие системы гражданской инфраструктуры (телекоммуникационные, включая средства массовой информации, транспортные, энергетического комплекса, финансового и промышленного секторов);
- информационно-управляющие элементы военной инфраструктуры (системы связи, разведки, боевого управления, тылового обеспечения, управления оружием);
- линии, каналы связи и передачи данных;
- информация, циркулирующая или хранящаяся в системах управления;
- общество в целом (как гражданское население, так и личный состав вооруженных сил), его государственные, экономические и социальные институты;
- средства массовой информации (в первую очередь электронные);
- руководящий состав и персонал автоматизированных систем управления, участвующий в процессе принятия решений.

В период проведения миротворческих операций объектами воздействия могут быть также военизированные, партизанские и политические организации, религиозные и социальные группы, отдельные лица, открыто или тайно выступающие против присутствия ВС или союзников и препятствующие выполнению ими своей миссии [270].

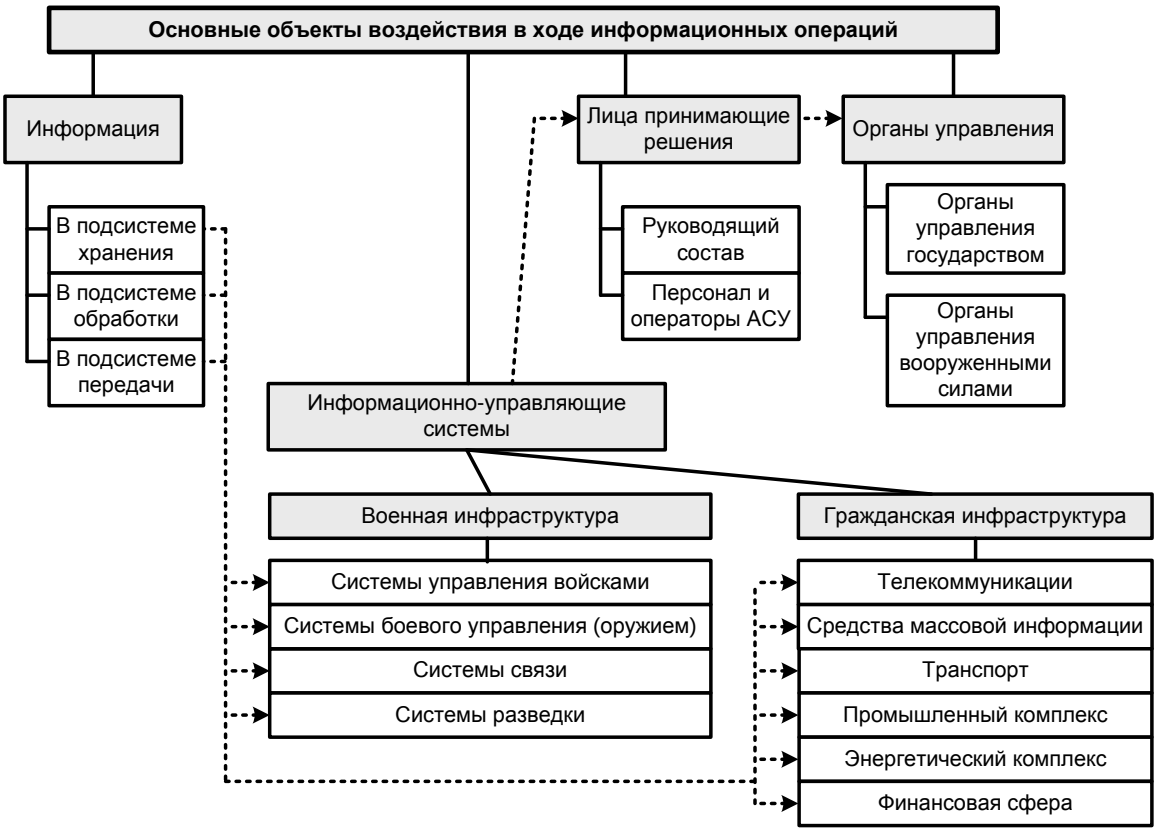


Рис. 3.4. Основные объекты воздействия в ходе информационных операций [256, 270]

Поскольку информационные операции связаны с использованием информации и информационных технологий для воздействия на военные и гражданские системы с целью достижения информационного превосходства над противником, ряд специалистов дают следующее определение информационным операциям [270].

Информационная операция — это комплекс взаимосвязанных по цели, месту и времени мероприятий и акций, направленных на инициализацию и управление процессами манипулирования информацией, с целью достижения и удержания информационного превосходства путем воздействия на информационные процессы в информационных системах противника [2, 256].

При этом информационные системы рассматриваются в широком смысле, т. е. не только автоматические и автоматизированные технические системы, но и государство и общество, которые тоже рассматриваются как информационные системы.

Информационная операция — действия, предпринимаемые с целью оказать влияние на информацию и информационные системы противника и защитить свои собственные информацию и информационные системы [284].

Информационные операции, по сути, являются основой ведения информационной войны. Информационные операции являются самостоятельным видом оперативного обеспечения, который реализует на поле боя концепцию информационной войны.

Анализ зарубежных материалов, проведенный в работе [95], позволяет выделить следующие ***ключевые особенности информационных операций***:

- сравнительно низкая стоимость создания средств информационного противоборства и информационного оружия, а соответственно — низкие финансовые и материальные затраты на проведение информационных операций;
- ликвидация статуса традиционных государственных границ при подготовке и проведении информационных операций;
- усиление роли управления восприятием ситуации путем манипулирования информацией по ее описанию и контексту;
- изменение приоритетов в деятельности стратегической разведки, которые смещаются в область завоевания и удержания информационного превосходства;
- усложнение задачи обнаружения начала информационной операции;
- сложность создания коалиции против агрессора, проводящего информационную операцию.

Общая классификация информационных операций приведена на рис. 3.5.

По целям и уровню управления, на которое осуществляется воздействие, информационные операции классифицируются на [95]:

- информационные операции на государственном уровне;
- информационные операции на военном уровне.

На государственном уровне целями информационной операции являются ослабление позиций конкурирующих государств, подрыв их национально-государственных устоев, нарушение системы государственного управления за счет информационного воздействия на политическую, дипломатическую, экономическую и социальную сферы жизни общества, проведения информационно-психологических операций, подрывных и иных деморализующих пропагандистских акций. Кроме этого, информационные операции на государственном уровне могут решать задачи защиты национальных интересов, предупреждения международных конфликтов, пресечения провокационных и террористических акций, а также обеспечения безопасности национальных информационных ресурсов [95].

На военном уровне информационные операции представляют собой комплекс мероприятий, проводимых в масштабах ВС страны, их видов, объединенных командований в зонах и являются составной частью военных кампаний (операций). Они направлены на достижение информационного превосходства над противником (в первую очередь в управлении войсками) и защиту своих систем управления. Для этого могут использоваться любые военные и технические силы и средства, имеющиеся в распоряжении, при формальном соблюдении правовых, моральных, дипломатических, политических и военных норм [95].

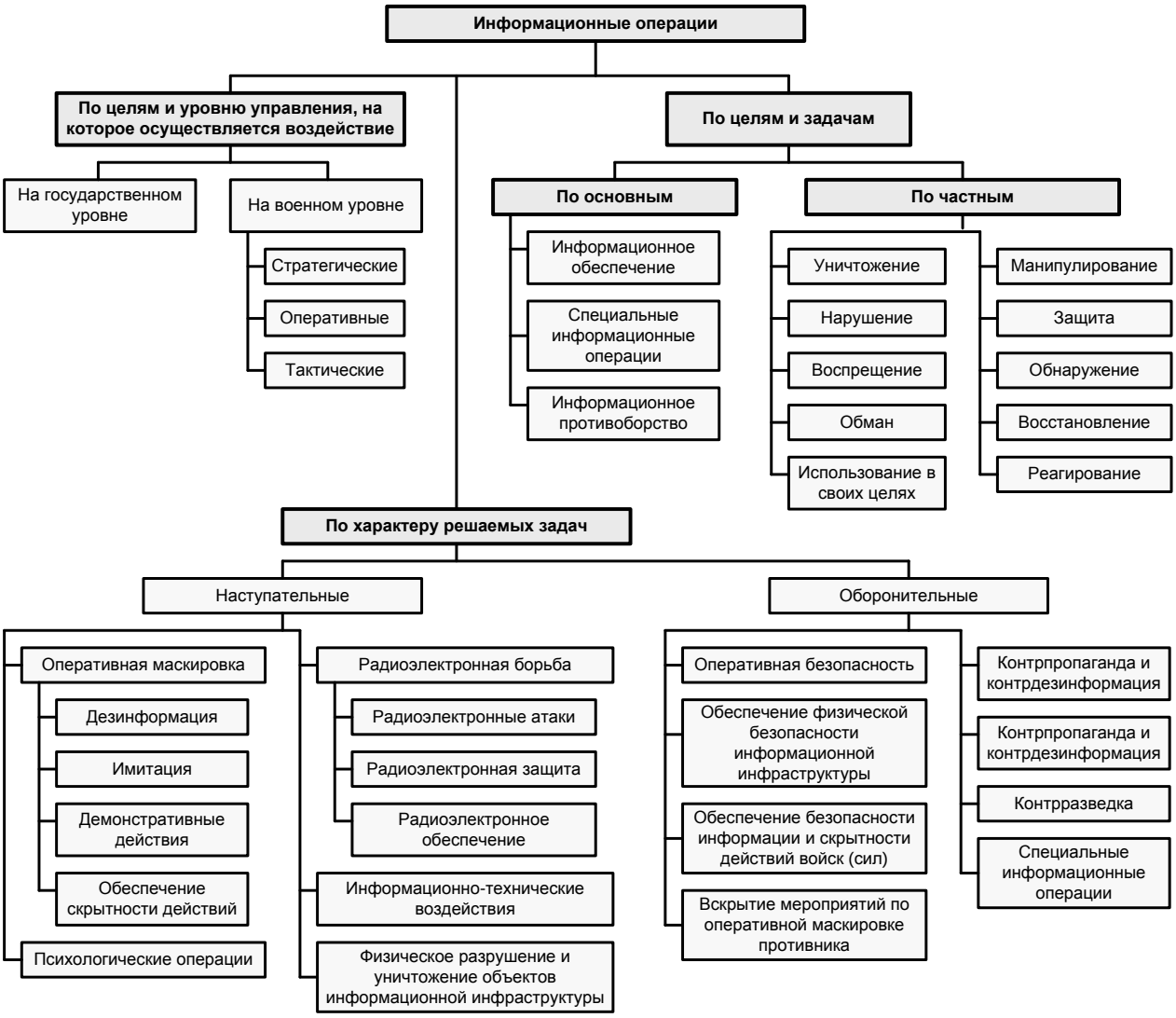


Рис. 3.5. Классификация информационных операций

На военном уровне информационные операции представляют собой комплекс мероприятий, проводимых в масштабах ВС страны, их видов, объединенных командований в зонах и являются составной частью военных кампаний (операций). Они направлены на достижение информационного превосходства над противником (в первую очередь в управлении войсками) и защиту своих систем управления. Для этого могут использоваться любые военные и технические силы и средства, имеющиеся в распоряжении, при формальном соблюдении правовых, моральных, дипломатических, политических и военных норм [95].

По уровню военного управления, на которое осуществляется воздействие, и масштабу воздействия информационные операции на военном уровне могут быть классифицированы следующим образом [253, 270]:

- ***стратегические информационные операции*** проводятся по решению военно-политического руководства страны, являются воздействием на элементы государственного устройства потенциальных противников (политические, военные, экономические и информационные) при

одновременной защите своих государственных структур и призваны обеспечить достижение национальных стратегических целей;

- ***оперативные информационные операции*** проводятся для обеспечения успешного хода военной операции или кампании в целом или решения ее главных задач, являются воздействием на линии связи, системы тылового обеспечения и боевого управления ВС противника при одновременной защите аналогичных собственных систем как своих ВС, так и союзников.
- ***тактические информационные операции*** проводятся с целью обеспечения решения тактических военных задач и сосредоточены на воздействии на информацию и информационные системы, такие как системы связи, боевого управления, разведки и другие, непосредственно обеспечивающие ведение боевых действий соединениями и частями противника при одновременной защите своих систем.

При этом перед ВС при проведении информационных операций впервые ставится задача воздействия на противника еще в угрожаемый период (до начала активных боевых действий), с тем чтобы обеспечить выгодную для своей стороны направленность процессов управления и принятия решений противостоящей стороной [95].

По целям и задачам информационные операции классифицируются следующим образом [2, 270]:

- информационное обеспечение;
- специальные информационные операции;
- информационное противоборство.

При этом выделяются **частные задачи информационной операции**, решение которых в ходе ее проведения будет способствовать достижению ее цели [266, 284]:

- *уничтожение* — причинение такого ущерба системе (или объекту), что она не сможет выполнять ни одну из своих функций, не может быть восстановлена до приемлемого уровня без ее полного воссоздания;
- *нарушение* — прерывание информационных потоков;
- *подавление* — снижение эффективности или работоспособности систем управления или связи противника и его средств сбора и обработки информации;
- *воспрещение* — лишение противника возможности доступа к необходимой для принятия решений и управления информации, использования систем, средств служб и сервисов;
- *обман* — введение в заблуждение лица, принимающего решение, формирование уверенности в том, чего нет в действительности, путем искажения его восприятия;
- *использование в своих целях* — получение доступа к системам управления противника с целью добывания информации или внедрения ложной или дезориентирующей информации;

- *манипулирование* — вынуждение противника принимать решения и совершать действия, выгодные своим войскам;
- *защита* — принятие мер противодействия разведке противника, захвату важного оборудования и информации;
- *обнаружение* — выявление фактов вторжения в информационные системы или вскрытие их уязвимостей, создающих предпосылки или предоставляющих потенциальные возможности для вторжения;
- *восстановление* — возвращение информационных систем в их предшествующее состояние и восстановление информации;
- *реагирование* — своевременный ответ на информационную атаку или вторжение противника или других субъектов в информационные системы.

По характеру решаемых задач информационные операции классифицируются следующим образом [2]:

- оборонительные;
- наступательные.

Цель оборонительных информационных операций — обеспечение выполнения целевых задач информационными и управляющими системами в условиях ведения информационной войны, а также обеспечение сохранности информационных ресурсов и предотвращения утечки, искажения, утраты или хищения информации в результате несанкционированного доступа к ней со стороны противника [2, 253].

Оборонительные информационные операции — взаимосвязанные процессы по защите информационной среды, вскрытию признаков нападения, восстановлению боеспособности и организации ответных действий на агрессию (нападение) [253].

Оборонительные информационные операции включают в себя следующие мероприятия по обеспечению безопасности собственных информационных ресурсов [2, 253]:

- оперативная безопасность;
- обеспечение физической безопасности информационной инфраструктуры;
- обеспечение безопасности информации и скрытности действий своих войск (сил);
- вскрытие мероприятий по оперативной маскировке противника;
- контрпропаганда и контрдезинформация;
- контрразведка;
- радиоэлектронная защита;
- специальные информационные операции.

Оборонительные информационные операции должны обеспечивать своевременность и точность передачи данных, гарантированный доступ к ним пользователей в условиях информационного воздействия противника. В ходе них предусматривается проведение мероприятий по восстановлению боеспособности информационных систем.

Цель наступательных информационных операций — достижение и удержание информационного превосходства в информационной войне [2, 256].

Наступательные информационные операции представляют собой комплексное проведение по единому замыслу и плану мероприятий по оперативной маскировке, радиоэлектронной борьбе, программно-математическому воздействию на информационно-управляющие системы, физическому уничтожению (или выводу из строя) объектов информационной инфраструктуры [256].

В ходе таких операций принимаются меры, оказывающие воздействие на сознание людей и направленные на срыв процесса принятия решений, а также действия с целью нарушения работы или уничтожения элементов информационной инфраструктуры.

Наступательные информационные операции включают следующие мероприятия по достижению и удержанию информационного превосходства [2, 256, 284].

1. Оперативная маскировка:
   - дезинформация;
   - имитация;
   - демонстративные действия;
   - обеспечение скрытности действий.
2. Психологические операции.
3. Радиоэлектронная борьба:
   - радиоэлектронные атаки;
   - радиоэлектронная защита;
   - радиоэлектронное обеспечение.
4. Физическое разрушение и уничтожение объектов информационной инфраструктуры.
5. Информационно-технические воздействия.

При проведении наступательных информационных операций основными традиционными методами являются психологические операции и мероприятия по оперативной маскировке, традиционно применявшиеся для оказания влияния на сознание людей в процессе принятия ими решений, а также такие действия, как радиоэлектронное подавление и использование средств физического уничтожения, направленные на нарушение функционирования или уничтожение элементов информационной инфраструктуры. К достаточно новым методам в данном случае можно отнести специальные программно-математические воздействия на компьютерные сети противника и специальные информационные операции.

Оперативная маскировка — мероприятия, проводящиеся под руководством командующих объединенными группировками войск (сил), в интересах оказания воздействий на органы принятия решений противника через его системы сбора, анализа и распределения информации путем предоставления им заведомо ложной информации и скрытия признаков реальной деятельности войск (сил). Цель этих мероприятий состоит в том, чтобы запутать, дезинформировать разведывательные органы противника, заставить их делать неправильные выводы и, как следствие, добиться от военного руководства против-

ника неверных действий. Эти мероприятия позволяют также опередить противника в принятии решения [253].

Оперативная маскировка предполагает применение следующих способов [253]:

- *дезинформация* — распространение заведомо ложной информации о составе, состоянии, дислокации, боеготовности своих войск, их группировках, характере и способах решения задач, планах, предназначении и состоянии военной техники и объектов;
- *имитация* — воспроизведение правдоподобных демаскирующих признаков, характерных для реальной деятельности войск (объектов), создание радиоэлектронной обстановки с использованием имитаторов, радиотехнических устройств, ложных сооружений и объектов, макетов военной техники и т. д.;
- *демонстративные действия* — преднамеренный показ противнику специально выделенными силами и средствами активной деятельности в целях его дезориентации и скрытия истинных намерений организаторов;
- *обеспечение скрытности действий* — определение признаков, распознаваемых разведывательными системами противника и позволяющих ему на основе их анализа получать особо важную и своевременную информацию; выбор и проведение мероприятий, которые обеспечивали бы скрытие этих признаков и тем самым снижали бы до приемлемого уровня уязвимость союзников от действий разведки противника.

Успех проведения мероприятий по оперативной маскировке в большой степени зависит от эффективности разведывательного обеспечения. Разведка в этом случае осуществляет вскрытие объектов противника, в отношении которых замышляются эти действия, оказывает помощь в разработке правдоподобной версии, предлагаемой для дезинформации, выборе наиболее перспективных объектов для реализации дезинформации, а также оценивает эффективность проведенных мероприятий.

Психологические операции — мероприятия по распространению специально подготовленной информации с целью оказания воздействия на эмоциональное состояние, мотивацию и аргументацию действий, принимаемые решения и поведение отдельных руководителей, организаций, социальных или национальных групп и отдельных личностей противника в благоприятном для государства и его союзников направлении [253].

Психологические операции по своим масштабам классифицируются следующим образом [253]:

- стратегические;
- оперативные;
- тактические.

Проведение психологических операций может обеспечиваться мероприятиями оперативной маскировки [253].

На стратегическом уровне психологические операции могут проводиться в форме пропаганды определенных политических или дипломатических позиций, официальных заявлений либо сообщений руководителей государства [253].

На оперативном уровне такие операции могут проводиться в виде распространения листовок, с помощью радио- и телевещания, вещания с использованием средств громкоговорящей связи, а также других средств для передачи информации, содержащей призывы, побуждающие личный состав вооруженных сил противника к массовому саботажу, дезертирству, бегству или капитуляции [253].

На тактическом уровне проведение психологических операций предполагает использование громкоговорящей связи и других средств для нагнетания страха, разжигания разногласий и роста неповиновения в рядах противника [253].

Радиоэлектронная борьба подразделяется на следующие составные элементы [253]:

- радиоэлектронные атаки;
- радиоэлектронную защиту;
- радиоэлектронное обеспечение.

Радиоэлектронные атаки — действия наступательного характера, предпринимаемые с целью дезорганизовать, нейтрализовать или снизить возможности противника по эффективному использованию им радиоэлектронных систем в различных звеньях управления ВС [253].

Радиоэлектронная защита — такие действия, как защита своих РЭС от помех, создаваемых противником, и осуществление контроля (наблюдения) за работой РЭС союзников с целью исключения их взаимного влияния друг на друга [253].

Радиоэлектронное обеспечение — действия, направленные на обнаружение, идентификацию и определение местоположения РЭС противника, которые могут являться как источниками получения разведданных, так и источниками информационных угроз [253].

Более подробно радиоэлектронная борьба как составной элемент информационных операций рассмотрена в разделе 2 «Радиоэлектронная борьба».

Физическое уничтожение элементов информационной инфраструктуры рассматривается как проводимые в ходе информационной операции действия по применению средств огневого поражения и физического уничтожения с целью вывода из строя ключевых элементов системы управления и связи противника [253].

Информационно-технические воздействия определяются как действия с применением аппаратно-программных средств, направленные на использование, искажение, подмену или уничтожение информации, содержащейся в базах данных компьютеров и информационных сетей, а также на снижение эффективности функционирования либо вывод из строя самих компьютеров и компьютерных сетей [253].

С учетом расширения субъекта и объекта воздействия, а также учитывая то что, воздействие может быть не только прямым, но и опосредованным, можно дать более широкое определение.

Информационно-технические воздействия — воздействия на информационный ресурс, информационную систему, информационную инфраструктуру, на технические средства или на программы решающие задачи сбора, передачи, обработки, хранения и воспроизведения информации, с целью вызвать заданные структурные или функциональные изменения.

Также среди наступательных информационных операций выделяют борьбу с системами управления как самостоятельный вид боевого обеспечения. При организации информационных операций действия по борьбе с системами управления централизованно интегрируются в них и становятся их неотъемлемыми элементами.

Борьба с системами управления — деструктивное воздействие на информационные системы противника и циркулирующую в них информацию или уничтожение их. При этом целевыми объектами воздействия являются системы управления и связи противника [253].

3.3.5. Информационное воздействие

Информационное воздействие представляет собой наступательную составляющую информационной войны и реализуется посредством наступательных информационных операций.

Информационное воздействие — основной поражающий фактор информационной войны, представляющий собой воздействие информационным потоком на объект атаки — информационную систему или ее компонент — с целью вызвать в нём в результате приема и обработки данного потока заданные структурные или функциональные изменения [2, 275].

Объект информационного воздействия — множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе, но выгодных противнику [2, 275].

Объекты воздействия и защиты в психологической сфере — психика личного состава ВС и населения противостоящих сторон, системы формирования общественного мнения и принятия решений [2, 275].

Объекты воздействия и защиты в технической сфере — информационно-технические системы (системы связи и управления, телекоммуникационные системы, радиоэлектронные средства, компьютерные сети и т. д.) [2, 275].

Для каждой информационной сферы характерны свои объекты воздействия и средства поражения.

Различают следующие **виды информационного воздействия** [2, 275]:

- одиночные (например, отдельные военно-политические лидеры и др.);
- групповые (например, народные массы и личный состав вооруженных сил).

Средства информационного воздействия классифицируют по характеру поражающих свойств [2, 275]:

- высокоточное воздействие (на определенных лиц, на избранный социальный срез общества, на определенный ресурс в информационно-вычислительной сети);
- комплексное воздействие (всё население некоторого региона, а также вся его информационно-телекоммуникационная инфраструктура).

При этом **тип информационного воздействия** может быть [2, 275]:

- разрушающим;
- манипулирующим;
- блокирующим.

Степень поражения информационным воздействием — емкость той части объекта информационного воздействия, которая либо уничтожена или блокирована, либо работает на цели, чуждые собственной системе, но выгодные противнику [2].

Возможны следующие **основные способы информационного воздействия** [2, 253]:

- подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);
- радиоэлектронное воздействие на элементы информационных и телекоммуникационных систем (радиоэлектронная борьба);
- получение разведывательной информации путем перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счет внедрения специальных технических средств перехвата информации;
- осуществление несанкционированного доступа к информационным ресурсам (путем использования программно-аппаратных средств, прорыва систем защиты информационных и телекоммуникационных систем противника) с последующим их искажением, уничтожением или хищением либо нарушение нормального функционирования этих систем;
- формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения;
- получение интересующей информации путем перехвата и обработки открытой информации, передаваемой по незащищенным каналам связи, циркулирующей в информационных системах, а также публикуемой в открытой печати и средствах массовой информации.

3.4. Общие понятия об информационном оружии

3.4.1. Определение информационного оружия

В настоящее время к информационному оружию 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, 275].

В соответствии со сферами, в которых ведется информационное противоборство, информационное оружие классифицируется на два основных вида [2, 275]:

1. информационно-техническое оружие;
2. информационно-психологическое оружие.

Главными объектами воздействия 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. 3.6).

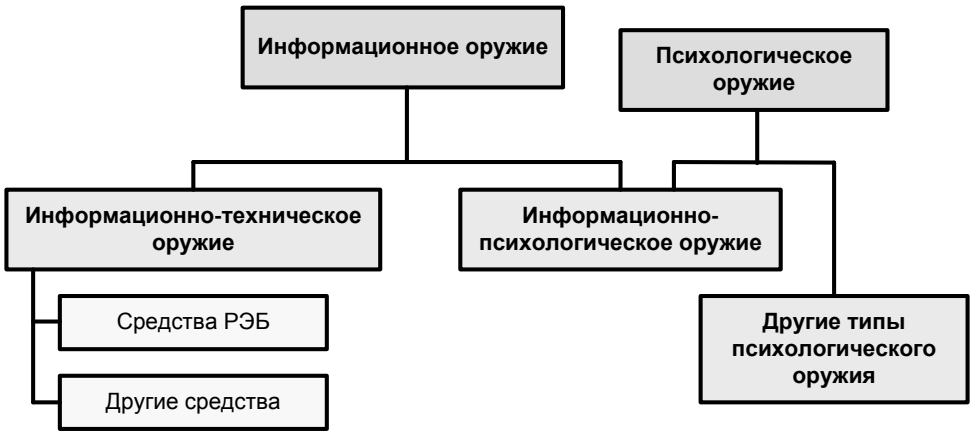


Рис. 3.6. Два основных вида информационного оружия

Фактически информационное оружие является технологией, включающей в себя [2, 277]:

- анализ способов и механизмов активизации у конкретной системы противника (технической, психологической, социальной, экономической и т.д.) характерных в нее возможностей самоуничтожения;
- поиск программы самоуничтожения;
- разработка конкретного информационного оружия;
- применение информационного оружия по заданному объекту.

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].

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 [304]. В соответствии с этой работой дано следующее определение информационному оружию.

Информационное оружие — различные средства поражения: высокоточное оружие для поражения органов управления или отдельных РЭС, средства РЭБ, источники мощного ЭМИ, программные средства и т. д., эффективно решающие задачи информационной войны [304].

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 РЭС противника.

В работах [307] и [312] приводятся близкие по смыслу определения информационного оружия.

Информационное оружие — совокупность информационных технологий, способов и средств информационного воздействия, предназначенных для ведения информационной войны [307].

Информационное оружие — оружие, наиболее эффективно решающее задачи информационной войны, основной задачей которой является достижение информационного превосходства [312].

Указывая на недостаток двух приведенных выше определений информационного оружия, заключающийся в привязке данного понятия к неоднозначно трактуемому в различных источниках понятию «информационная война», автор монографии [303] 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 [303].

Это определение, а также определение, представленное в работах [2, 275], на взгляд автора, 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.

В работе [13] авторами сделана другая попытка обобщения и конкретизации вышеуказанных определений информационного оружия.

Информационное оружие — это совокупность способов и средств [13]:

- подавления элементов инфраструктуры государственного и военного управления противника;
- радиоэлектронного влияния на элементы информационных и телекоммуникационных систем;
- несанкционированного доступа к информационным ресурсам с последующей их деформацией, уничтожением или хищением;
- информационно-психологического воздействия на военнослужащих и гражданское население противоборствующей стороны.

Современная стратегия применения информационного оружия основана на модели «пяти колец» Дж. Вардена. Под пятью «центрами тяжести» в данном случае понимаются 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 несколько отличительных качественных характеристик, которыми оно концептуально отличается от других видов оружия.

К концептуальным отличительным характеристикам информационного оружия относятся [319]:

- *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 эффекту воздействия сопоставимо с оружием массового поражения;
- *внезапность применения* — не требуется его длительная подготовка;
- *экономическая эффективность* — разработка информационного оружия и его применение требуют существенно меньших затрат по сравнению с другими видами оружия;
- *масштабность применения* — оно может применяться 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 всей системы в целом;
- *сложность осуществления контроля за созданием, испытанием, применением и распространением 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].

3.4.2. Общая классификация информационного оружия

В соответствии со сферой своего применения информационное оружие классифицируется на [13]:

- информационно-техническое оружие;
- информационно-психологическое оружие.

Подробно особенности этих типов информационного оружия рассмотрены в других разделах данной работы: 4.2 «Информационно-техническое оружие: определение и классификация»; 5.2 «Психологическое оружие»; 5.3 «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 противника путем поражения наиболее критичных из входящих в нее компонентов (как в технической, так и в психологической сфере) [13].

Наступательное информационное оружие. 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 других технических средств 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 (таблица 3.1) [13, 303, 312, 313, 315]. 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 3.1 — 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.); - 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

Вид информационного оружия	Используемые средства	Тип технологии
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 ПО информационной системы; - средства скрытого частичного изменения алгоритма функционирования ПО; - средства сбора данных, циркулирующих в ИС противника; - средства доставки и внедрения определенных алгоритмов в конкретное место информационной системы; - средства воздействия на системы охраны объектов	На основе информационных технологий
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 процесс передачи информации	- 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

Вид информационного оружия	Используемые средства	Тип технологии
Средства психологического воздействия, дезинформации и пропаганды	- воздействие посредством СМИ; средства пропаганды; средства создания или модификации виртуальной реальности; - средства имитации голосов операторов систем управления (например, ЛПР) и видеоизображения конкретных людей с их голосом (руководителей государств, лидеров партий и др.); - 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.	На основе информационных технологий
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	На основе информационных технологий

3.4.3. Классификация технологий информационного противоборства, обеспечивающих разработку и применение информационного оружия

В основу классификации технологий информационного противоборства положена приведенная выше классификация информационного оружия, которое по своему целевому назначению подразделяется на: оборонительное и наступательное. Классификацию технологий информационного противоборства можно представить в виде двенадцати укрупненных групп [13].

Группы технологий, обеспечивающих разработку и применение наступательного информационного оружия [13]:

- технологии программных воздействий;
- технологии информационно-психологических воздействий на личный состав;

- технологии воздействия на информацию, распространяемую СМИ (печатные, электронные, в том числе в сети Интернет);
- технологии воздействия на информацию в системах управления;
- технологии радиоэлектронного воздействия;
- технологии психологической борьбы, агитации и пропаганды среди военнослужащих противоборствующей стороны и гражданского населения.

Группы технологий, обеспечивающих разработку и применение оборонительного информационного оружия [13]:

- технологии защиты от программного воздействия;
- технологии защиты от специальных информационно-психологических воздействий;
- технологии защиты от деструктивного воздействия информации, распространяемой СМИ, а также от программных, лингвистических и иных негативных воздействий на людей;
- технологии защиты информации в системах управления;
- технологии защиты от радиоэлектронного воздействия и технических средств разведки;
- технологии морально-психологического обеспечения войск и гражданского населения.

В ходе дальнейшей декомпозиции каждая из перечисленных групп технологий может быть конкретизирована. Например, технологии программных воздействий классифицировать на: компьютерные вирусы, удаленные сетевые атаки, нейтрализаторы тестовых программ и др.

4. Информационное противоборство в технической сфере

4.1. Современные взгляды на роль и способы ведения информационного противоборства в технической сфере

4.1.1. Взгляды различных стран на разработку принципов и доктрин информационного противоборства в технической сфере (на примере ВС США, НАТО и Китая)

4.1.1.1. США

Развитие информационных технологий оказывает существенное влияние на характер, формы и способы ведения боевых действий. В этой связи возникли противоречивые взгляды на роль и значение операций в информационной сфере. Это было связано с тем, что информационная сфера не имела аналогий, сопоставленных с опытом ведения боевых действий в других, традиционных сферах [383].

В США, сохраняющих за собой технологическое и военное лидерство, на высшем уровне был принят ряд директив и официальных документов [262–268, 274, 275], регламентирующих политическую и военную деятельность в информационном (кибернетическом) пространстве. Суть стратегии заключается в том, что киберпространство стало рассматриваться Вашингтоном в качестве такого же потенциального поля боя, как земля, воздух, море и космос. Поэтому США приравнивают акты кибератак к традиционным военным действиям и предусматривают возможность «отвечать на серьезные нападения пропорциональными и справедливыми военными мерами», вплоть до применения ядерного оружия.

При этом представители Пентагона отмечают, что разработанная доктрина является лишь первым шагом на пути к освоению киберпространства. В дальнейшем, как отметил заместитель председателя Объединенного комитета начальников штабов ВС США, генерал Дж. Картрайт, Пентагон должен перейти от политики обороны к политике сдерживания угроз, не забывая при этом и о разработке возможных наступательных мер [287].

В своих стратегических документах Пентагон признал киберпространство новым полем возможных боевых действий, а НАТО приравнивает кибератаки на страну — члена-альянса к вооруженному нападению.

Таким образом, США признают кибербезопасность стратегической проблемой государственной важности, затрагивающей все слои общества. Государственная политика кибербезопасности NCSS (National Cyber Security Strategy) служит средством усиления безопасности и надежности информационных систем государства.

В рамках повышения уровня подготовки кадров АНБ США проводит ежегодные учения Cyber Defense Exercise в формате конкурса среди обучающихся в гражданских колледжах и военных академиях страны. Основные цели учения

— вызвать у американских военнослужащих интерес к сфере информационных технологий и повысить уровень их знаний [287].

Некоторые военные специалисты США и НАТО признавали уязвимость гражданских и военных информационных структур, но не верили в возможность появления новой модели потенциальных военных конфликтов. Другие военные специалисты (особенно в ВВС США) считали, что сражения в информационной сфере станут «новой революционной формой военных конфликтов». Основные расхождения во взглядах и предложениях на ведение боевых действий в информационной сфере возникли при разработке в ВС США согласованной со всеми видами ВС и учреждениями МО стратегии боевых действий в информационной сфере. В последующем было принято военно-политическое решение о необходимости ведения боевых действий в информационной сфере. В разработанной стратегии они были определены как фактор, повышающий боевой потенциал США в операциях объединенных сил. Впоследствии эти положения были закреплены в наставлении Объединенного штаба Комитета начальников штабов (ОШ КНШ) Вооруженных сил США JP 3-13 от 2006 г., а 27 ноября 2012 г. уточнены в новой редакции JP 3-13 [275]. По сути, эти документы в юридическом аспекте зафиксировали создание единой системы и общей для всех видов ВС США военной стратегии ведения боевых действий в информационной сфере, дополняющей и равнозначной другим сферам ведения боевых действий [383].

Возглавлявший в тот период Объединенное стратегическое командование ВС США генерал К. Чилтон выдвинул новую стратегическую категорию, которая была им определена как «доктрина объединенного устрашения, базирующаяся на использовании ядерного оружия, ракетных систем и боевых возможностей кибервойны» [383].

На рубеже XX и XXI вв. в ВС США появились новые оперативно-стратегические категории, такие как «информационная война», «наступательная, оборонительная и специальная информационная операция», «информационное превосходство» и другие. В изданном в 2006 г. едином наставлении ОШ КНШ JP 3-13 «Информационные операции» американцы отказались от термина «информационная война» и от деления подразделений «информационных операций» на три вида; определили состав сил и задачи «информационных операций» в операциях единых сил США и операциях многонациональных сил [383].

В настоящее время группой по развитию комплексных возможностей ICDT (Integrated Capabilities Development Team) Командования по боевой подготовке и доктринам сухопутных войск США (TRADOC) разработаны базовые документы, определяющие спектр задач сухопутных войск США в киберпространстве на период 2010–2024 гг.; в частности, создана концепция проведения операций с полномасштабным использованием киберсредств — Cyber Electronics In Full-Spectrum Operations Concept, а также определены перспективные направления их проведения [288].

В 2012 г. ВС США отказались от разделения сил, участвующих в информационных операциях, на основные и обеспечивающие, определив, что в информационных операциях единых и многонациональных сил могут приме-

няться как летальные, так и нелетальные силы и средства, тесно связанные между собой [383].

В сентябре 2012 г. председатель объединенного штаба КНШ ВС США генерал М. Демпси издал директиву «Единые силы — 2020», излагающую основополагающие концепции ведения совместных операций. Данная директива значительно повысила значение информационных операций в сражениях XXI века, делая упор на глобальные интегрированные операции, основой которых станут «проводимые одновременно или отдельно от сил общего назначения операции сил специальных операций и кибероперациий ВС США».

Задачами таких информационных операций будут являться [383]:

- нарушение работы информационных систем и компьютерных сетей органов военного и государственного управления;
- нейтрализация или снижение возможностей разведки противника;
- когнитивное воздействие на интеллектуальные способности лиц, участвующих в подготовке и принятии военных и политических решений;
- обеспечение ВС США и их союзников возможностью добывать развединформацию и упреждать принятие решений противником.

Базовой основой таких операций должны стать «достижение и удержание информационного превосходства над противником и управление вооруженными силами в сетецентрических операциях в едином информационном пространстве и в реальном режиме времени» [383].

Роль и значение информационных операций в XXI в. профессор национального университета МО США Дж. Куел определил следующим образом: «Обеспечение контроля и превосходства в информационном пространстве имеет такое же решающее значение в операции, как имело место в XX в. значение обеспечения контроля и превосходства в воздушном пространстве. Военной необходимостью такого контроля является потенциальная возможность дезорганизации систем управления, связи и линий снабжения противника, снижения мобильности его ВС, создания благоприятных условий для нанесения ударов по стратегической инфраструктуре противника». Дж. Куела поддерживает и заместитель министра обороны США Г. Ингланд, который заявил: «Важность обеспечения полного преимущественного контроля в информационном пространстве должны понимать военные руководители и специалисты оперативных органов штабов, чтобы обеспечивать в операциях реализацию максимальных боевых возможностей своих ВС, правильно определять границы допустимой уязвимости своих информационных систем и компьютерных сетей, обеспечивать успешное применение систем оружия, ракет, танков, в целом средств и систем управления ВС и их радиолокационного обеспечения». Начальник управления систем связи объединенного штаба КНШ ВС США (J-6) вице-адмирал Н. Браун добавила, что «если мы не сможем понять и оценить роль и значение угроз в информационной сфере, мы никогда не сможем добиться успеха в операции». А старший советник директора Национальной разведки США М. Хэтвей заявила, что информация сегодня стала стратегическим ресурсом, она определяет качество бизнеса и успешность ведения любых

дел и операций с использованием информационных систем и компьютерных сетей в США и во всём мире» [383].

В декабре 2012 г. командованием ВВС США был представлен документ Cyber Vision 2025. Этот документ является важной составной частью единого комплекта оперативно-стратегических документов и определяет направление, динамику и основные тенденции развития военно-стратегической обстановки в глобальном информационном пространстве [3].

Согласно представленным в Cyber Vision 2025 оценкам, на рубеже 2025 г. ВВС США прогнозируют осложнение ситуации в киберпространстве для действий американских вооруженных сил. Оценка обстановки, лежащая в основе документа, исходит из того, что в ближайшие годы ситуация в киберпространстве будет характеризоваться ростом напряженности и «конкурентности» [3].

Вырастет число стран, обладающих соответствующими технологиями, одновременно существенно возрастает капиталоемкость работ в области безопасности, а финансирование ряда проектов уменьшится вслед за общим ухудшением глобальной экономической ситуации. В предстоящие годы США продолжат терять влияние на ряд регионов мира (прежде всего на Азию), и многополярный мир станет фактической реальностью. США в экономической мощи будут противостоять Китай (который всё еще будет находиться на второй позиции) и Индия (на третьей). Помимо традиционных государств, аналитики ВВС США прогнозируют появление «гибридных противников», которые, помимо использования иррегулярной тактики действий, будут обладать и высокотехнологичными системами вооружения, что потребует от ВС высокой гибкости и мобильности для адекватного ответа на новую угрозу [3].

В качестве серьезной угрозы, значительно обострившейся к 2025 г., называют проблему утраты контроля США над производством микроэлектроники и компонентов микропроцессорной техники, а также взрывной рост оффшорного программирования (т. е. за пределами США). Отсутствие надежных средств верификации программного обеспечения, а также выявления закладок в микрокристаллах процессоров сделает эту проблему одной из наиболее значимых для США в следующие 10 лет [3].

Подчеркивается, что развитие технологий подстегнет и трансформацию угроз в информационном пространстве. Среди значимых технологических новшеств выделяют глубокий анализ социальных сетей, которые позволят прогнозировать социальное поведение и управлять социальными группами [3].

Также указывается, что уже сегодня обозначился дефицит специалистов в области компьютерной безопасности, и их недостаток будет только расти. В США к 2025 г. прогнозируется появление около 3800 молодых специалистов с докторской степенью Ph.D. в области информационных технологий. Из них менее половины будут гражданами США. В то время как в Китае эта цифра будет выше 8500 [3].

Существенное ограничение на эффективную оборону от кибератак накладывается высокой скоростью развития обстановки в информационном пространстве. Это не позволяет использовать весь доступный потенциал для орга-

низации адекватного ответа. Отмечается всё большее проникновение эффектов от воздействия информационного оружия в физическое пространство — операции в киберпространстве могут повлечь физическое разрушение критической инфраструктуры и даже массовую гибель людей [3].

Вместе с тем, наряду с негативной оценкой ситуации в средне- и долгосрочной перспективе американские ВВС исходят из потребности гарантированного обеспечения информационного превосходства США. Под «гарантированным превосходством» понимается информационное превосходство, обеспеченное в условиях противодействия противника, при этом основное внимание уделяется обеспечению боевой устойчивости систем управления на разных уровнях. Признаётся, что обеспечить гарантированное превосходство в жестких условиях возможно лишь при эффективной системе заблаговременного оповещения еще на ранних стадиях подготовки противником акций в информационном пространстве (это обусловливает сосредоточение внимания на вопросах глобального сбора информации, далеко за пределами потенциальных объектов атаки), наличием высококлассных специалистов (в документе введен термин «киберспецназ» — Air Force Cyberspace Elite), и надежной информационной инфраструктуры, способной выполнять задачи даже в жестких условиях информационных атак противника. Успех в киберпространстве определяется балансом усилий человека и автоматических процедур. Дефицит времени в условиях атак потребует увеличения уровня автоматизации действий. Вместе с тем рост сложности атак требует наличия высококлассных специалистов, способных относительно быстро разгадать замысел противника. Существенную помощь здесь могут оказать средства визуализации обстановки в киберпространстве. Кроме технических средств анализа и отображения, для этого требуется специальное обучение персонала, отвечающего наиболее высоким требованиям [3].

Обеспечение устойчивости в киберпространстве потребует эффективного сочетания резервирования, разнообразия вариантов решений и декомпозиции (распределения в сети) функциональных возможностей системы командования и управления. Это может быть отчасти достигнуто созданием систем раннего обнаружения вторжений, самовосстановленем после атак, а также реагированием на угрозы в реальном масштабе времени. Основу здесь будет играть так называемая «активная оборона», заключающаяся в оперативном автоматическом реконфигурировании атакованного сегмента сети, изменения паролей, IP-адресов, частот и др. (например, по случайному закону для увеличения сложности и затруднения действий противника). Для обозначения указанных действий в материалах Cyber Vision 2025 использован термин «оперативный киберманевр» (rapid cyber maneuver) [3].

В целом Cyber Vision 2025 является очередным доктринальным документом, отражающим эволюционный процесс развития возможностей ВВС США по организации и ведению информационного противоборства. Указанные в документе особенности развития обстановки в информационном пространстве в средне- и долгосрочной перспективе адекватны общей позиции американских военных экспертов по оценкам развития киберпространства. Наряду с

этим обращает на себя внимание и больший акцент на вопросы обеспечения боевой устойчивости систем, что подтверждает информацию о том, что в ВС США серьезно относятся к возможностям потенциальных противников нанести ущерб критической инфраструктуре США [3].

За последние 15 лет расходы США на разработку и приобретение средств информационного противоборства выросли в 4 раза и ныне занимают первое место среди расходов на все военные программы. США ежегодно расходуют на информационные технологии только из федерального бюджета около 38 млрд долларов, из которых около 20 млрд (более 50%) составляют расходы военного ведомства. И это без учета десятков миллиардов долларов, затрачиваемых на бортовые системы управления спутников, ракет, самолетов, танков и кораблей [292]. Также к работам в области информационного противоборства Министерство обороны США активно привлекает коммерческие структуры. В связи с чем объемы госзаказов в области кибербезопасности в период с 2010 по 2013 г. выросли примерно на 44%, до 10,7 млрд долларов [37].

Вслед за США руководящие документы и стратегии кибербезопасности приняты в Канаде, Японии, Индии, Австралии, Новой Зеландии, Колумбии и некоторых других государствах [287].

4.1.1.2. Другие страны НАТО: Великобритания, Германия, Франция

В настоящее время страны — члены Евросоюза (особенно входящие в блок НАТО) в большинстве разработали и приняли стратегии кибербезопасности: Швеция (2008 г.), Эстония (2008 г.), Финляндия (2013 г.), Словакия (2008 г.), Чехия (2011 г.), Франция (2011 г.), Германия (2011 г.), Литва (2011 г.), Люксембург (2011 г.), Голландия (2011 г.), Великобритания (2011 г.) [287].

Над созданием единой концепции коллективной кибероборонs начали работать и в НАТО.

С 2008 г. НАТО проводит ежегодные киберучения с отработкой взаимодействия международных сил альянса в области информационной безопасности. Так, в апреле 2013 г. на учениях под названием «Locked Shields — 2013» отрабатывались мероприятия отражения кибератак компьютерных сетей. Организатор учений — центр изучения передового опыта НАТО в области кибербезопасности, совместно с министерствами обороны Эстонии и Финляндии. В мероприятии приняли участие около 250 специалистов из 9 стран: Эстонии, Финляндии, Литвы, Германии, Польши, Нидерландов, Италии, Словакии и Испании [287].

В ноябре 2010 г. на саммите НАТО было решено разработать «План действий в области кибероборонs». Важное место в нём будет отведено созданию центра НАТО по реагированию на киберинциденты. Изначально его предполагалось запустить в 2015 г., но по настоянию США срок сократили на 3 года [288].

Европейское агентство по сетевой и информационной безопасности ENISA (European Network and Information Security Agency) в октябре 2012 г. провело киберучения «European Cyber Exercise» с целью определения готовности орга-

низаций государственного и частного секторов к отражению кибератак. В учениях приняли участие более 300 специалистов по компьютерной безопасности из банков, интернет-провайдеров и государственных учреждений 25 государств. Это уже вторые учения в киберпространстве, проведенные под эгидой ЕС с ноября 2010 г. [287].

Великобритания

Британское представление об информационной войне во многом подобно таковому в США. Оно определяет информационную войну как действия по оказанию влияния на информационные системы противника при одновременной защите собственных информационных систем. «Свобода слова» в Великобритании регулируется, по крайней мере, десятком законов и множеством подзаконных актов. В настоящее время там действует более 10 государственных и независимых учреждений и организаций, занимающихся регулированием в сфере массовой информации. В Великобритании основные направления государственной информационной политики разрабатывает Британский совет совместно с Центральным бюро информации. Совет находится в непосредственном подчинении МИД Великобритании [2].

Организация связи с общественностью в структуре Министерства обороны Великобритании возложена на аппарат пресс-секретаря — начальника службы информации Минобороны. Руководитель этой службы (гражданское лицо) имеет ранг государственного чиновника. Кроме того, в Великобритании в 2000 г. введен в действие комплекс законодательных актов, который в значительной степени может применяться к расследованию преступлений в киберпространстве. Он предполагает, что нападения на информационные системы могут рассматриваться как обычное уголовное преступление со всеми вытекающими последствиями. Данный акт позволяет британскому правительству перехватывать и читать электронную почту, а также требовать расшифровки личных файлов по требованию государственных чиновников [2].

Германия

Представление об информационной войне в ФРГ совпадает с таким представлением принятым в США и Великобритании. Оно включает ведение наступательной и оборонительной информационной войны для достижения целей национальной политики. Вместе с тем ФРГ имеет тенденцию оставаться более системной в подходах к обеспечению информационной безопасности, чем США.

При определении угроз и возможных ответов иностранные государства рассматриваются отдельно от негосударственных организаций (типа политических партий, международных организаций и средств массовой информации). Также отдельно выделяются преступные сообщества (организованные преступные группы, хакеры и т. д.) и отдельные индивидуумы (религиозные фанатики и др.) [2].

Однако в двух аспектах представление ФРГ об информационной войне отличается от американского. ФРГ рассматривает управление средствами мас-

совой информации как элемент информационной войны. Кроме того, Германия отдельно вводит определение для экономической информационной войны, подобно французам.

Причинами такого подхода является следующее [2]:

- Германия оценила потенциал возможного экономического ущерба, который может быть нанесен немецкому бизнесу и экономике;
- Германия, возможно, испытала существенные экономические потери от Франции в операциях индустриального шпионажа в киберпространстве;
- Германия может искать пути смягчения последствий от потенциальных вторжений.

В ФРГ система органов связи с общественностью бундесвера предназначена для освещения в СМИ вопросов военной политики, взглядов руководства ФРГ и НАТО на перспективы строительства и развития вооруженных сил, ведения информационно-пропагандистской работы с общественными и молодежными организациями, а также для изучения общественного мнения по вопросам военного строительства. В Германии базовой структурой формирования информационной политики государства является Федеральное ведомство печати и информации, имеющее статус высшего федерального ведомства. Его статс-секретарь принимает участие в заседаниях кабинета министров [2].

Франция

Французские военные эксперты рассматривают концепцию информационной войны, состоящую из двух главных элементов: военной и экономической (или гражданской). Военная концепция предполагает несколько ограниченную роль информационных операций. Военная концепция определяет место информационных действий в основном в контексте конфликтов малой интенсивности или в миротворческих операциях. В этом контексте союзники не рассматриваются как противники.

Напротив, экономическая или гражданская концепция включает более широкий диапазон потенциального применения информационных операций. Французское представление принимает намного более широкое и более глубокое представление для конфликта в экономической сфере. В этом случае французы не видят себя связанными рамками НАТО, ООН или согласием США на проведение операций. Такой подход к экономическому конфликту учитывает возможность быть и союзником, и противником одновременно.

В ВС Франции вопросами взаимодействия с общественностью занимается служба информации и общественных связей (SIRPA). Современная структура этой службы определена в 1990 г., одновременно были уточнены и значительно расширены ее задачи и функции. SIRPA находится в непосредственном подчинении Министра обороны и возглавляется бригадным генералом.

Франция активно формирует структуры по контролю за своими гражданами в киберпространстве. В ряде средств массовой информации отмечалось, что французы создали собственную версию системы Eshelon (по сообщениям американской прессы, система направлена на перехват фактически всех частных глобальных коммуникаций). «Frenchelon» — так некоторые назвали

эту систему, которая по сообщениям СМИ используется для контроля и анализа коммуникаций, особенно в районе Парижа.

В последнее время правительство Франции, изучив опыт работы арабских телеканалов по освещению агрессии против Ирака, приступило к формированию собственного новостного спутникового канала, предназначенного для организации вещания на ряд азиатских стран, в которых позиции Франции традиционно сильны.

4.1.1.3. Китай

Китай уже давно включил термин «информационная война» в тезаурус своих военных специалистов [384]. Сегодня он неуклонно движется к формированию единой доктрины информационной войны. Фактически, если революция в военном деле определяется как существенное изменение в технологии, дающее преимущество в военном обучении, организации, стратегии и тактике военных действий, то, возможно, Китай из всех стран сегодня испытывает истинную революцию в киберпространстве.

Китайская концепция информационной войны включает уникальные сугубо китайские представления о войне вообще. Эти представления основаны на концепции «народной войны», стратегемах великого Сун Цзы, а также на местных представлениях о том, как воевать на стратегическом, оперативном и тактическом уровнях. Многое из этого подхода делает акцент на обмане, войне знаний и поиске асимметричных преимуществ над противником. Информационная война определена как «переход от механизированной войны индустриального возраста к ... войне решений и стиля управления, войне за знания и войне интеллекта» [2].

Китай развивает концепцию «сетевых сил» (воинские подразделения численностью до батальона), которые будут состоять из высококлассных компьютерных экспертов, подготовленных в ряде государственных университетов, академий и учебных центров. Предполагается, что основной акцент будет сделан на привлечение активной молодежи [2].

На сегодняшний момент в Китае было проведено уже несколько крупномасштабных учений этих сил по отработке концепции информационной войны.

По утверждению ряда американских экспертов [384–386], усилия Китая сегодня направлены главным образом на укрепление его экономического состояния, поддержания национального единства, значительного улучшения технологических и военных способностей, а также на увеличение регионального и глобального влияния.

Основным условием решения стоящих задач является минимальное или полностью отсутствующее явное и открытое противоборство, которое может привлечь внимание стран Запада к Китаю и к региону в целом. Поставленная цель достигается реализацией уникальной формы информационной войны, эффективно использующей тактику обмана, маскировки и введения в заблуждение противника. Эта теория поддерживается различными источниками, которые имеют непосредственное отношение к «Великой китайской стратегии» и

стратегическому наследию Китая и во многом ведет к пересмотру границ западного определения понятия информационной войны [2].

Особо следует отметить, что подобная трактовка развития китайского подхода к информационной войне существенно отличается от результатов, которые высказывались американскими экспертами всего несколько лет назад. Так, еще в 2001 г. результат идентификации китайской доктрины информационной войны рассматривался ими как «разочаровывающе неуловимый». Однако существенное переосмысление произошло после опубликования книги китайских военных специалистов «Неограниченное противоборство» (Unrestricted Warfare) [2].

Ранее американские эксперты отмечали, что в открытой литературе китайские специалисты используют определения, практически полностью повторяющие американское видение информационной войны, а часто просто занимаются плагиатом. Вместе с тем бóльшая часть экспертов обращает внимание на то, что копирование действительно может иметь место. Однако бóльшая часть дебатов в Китае по рассматриваемой проблеме могла быть организована с целью сокрытия реальных намерений и способностей Китая, что заставляет воспринимать ее как масштабную кампанию по дезинформации. Некоторые эксперты предупреждают, что США должны быть осторожны, чтобы не полагать, будто Китай всецело рассматривает информационную войну через призму открытых американских публикаций [2].

Как отмечается в ряде прогнозных исследований, выполненных за последние годы в аналитических центрах США, Китай становится главным экономическим и военным конкурентом США в XXI столетии. Однако, несмотря на наличие такого серьезного противника, американское понимание стратегического наследия Китая, его «Великой стратегии» и роли информационной войны в поддержке этой стратегии, по мнению американских экспертов, серьезно недооценены. Существующий сегодня в США уровень развития приемов и методов анализа и прогнозирования не позволяет полностью постичь то сильное и глубокое воздействие, которое восточное стратегическое наследие имеет в действиях Китая [2].

Вместе с тем недостаток любой официальной информации, закрытость китайского общества, ряд существенных разрывов между теорией и практикой в китайских открытых публикациях в области информационной войны, продолжающиеся дебаты и отсутствие единого мнения по ряду вопросов, а также уникальное влияние китайской стратегической традиции ставят перед американскими специалистами со стороны Китая всё более и более непредсказуемые вызовы в информационном пространстве [2].

По мнению аналитиков, сегодня американская военная доктрина, основанная на всеобъемлющем высокотехнологичном превосходстве, должна включать и совершенную оценку ситуации в различных областях, в первую очередь в военной и информационной. Однако, как показали результаты ряда последних конфликтов, в которых приняли участие американские войска, США пренебрегают детальным изучением и осознанием стратегической культуры потенциальных противников. Например, результаты последних военных кампаний

США и их союзников в Ираке показали, что наличие технически превосходящей мощи недостаточно для победы над противником. Необходимо помнить, что цель любой войны состоит прежде всего в сломе воли противника к сопротивлению. Сегодня это ключевой аспект информационной войны [2].

Эксперты отмечают, что, учитывая складывающуюся военно-стратегическую обстановку, а также продолжающееся размывание границ между войной и миром, область информационной войны требует еще более внимательного изучения всех аспектов, связанных с выработкой и принятием решений противником, а главное — его стратегической концепции [2].

Исследуя стратегию действий Китая, а также роль и место в ней средств и методов информационной войны, американские аналитики столкнулись с рядом фундаментальных отличий, корни которых лежат в культурном различии Западной и Восточной цивилизаций [2].

Суть восточной стратегии противоборства заключается в том, что в стратегии нужно стремиться к большему влиянию при минимальных затратах, при этом не уничтожать противника и собственную нацию в бесконечной борьбе, а использовать ресурс и возможности противника для собственного роста. Важным является также и то, что главной целью остается не победа над противником любой ценой, даже ценой его полного истребления, но, избегая непосредственных столкновений и стратегических перемещений сил, достижение господства, выживания и процветания собственного народа. Этот подход оставляет жизнеспособной нацию, позволяя ей доминировать над процветающим миром, а не над миром разрухи, негодования и бедности [2].

В качестве еще одного подтверждения культурных различий американские эксперты отмечают следующее: Китай официально не опубликовал свою «великую стратегию», однако анализ различных источников позволил американским специалистам идентифицировать две стратегические цели Китая [2]:

1. развитие «всесторонней национальной мощи»;
2. максимизация «стратегической конфигурации силы», названной китайскими специалистами «ши», с целью поддержания независимости и создания импульса для усиления национальной мощи.

Полная стратегия Китая остается закрытой от широкой публики, однако наибольший интерес, по мнению экспертов, представляет именно англоязычная интерпретация китайского «ши», так как в отношении этого термина отсутствует какой-либо западный эквивалент. Лингвисты трактуют его как «выравнивание сил», «склонность вещей» или «потенциал, рожденный диспозицией», который в руках высококлассных стратегов может гарантировать победу над превосходящей силой [2].

Осознание базовых принципов китайской стратегии позволяет американским аналитикам утверждать, что сегодня в Китае может превалировать совсем иное представление о США как о глобальном противнике. Наиболее вероятно, что, базируясь на культурных различиях, Китай видит США как препятствие к достижению контроля и влияния в регионе и в мире в целом, однако победа Китая над этим противником невозможна без использования ресурса самого противника. Учитывая безусловные выгоды от взаимодействия с США — пре-

жде всего в вопросах торговли и технологий, — Пекин, очевидно, полагает, что США представляют существенный долгосрочный вызов. Руководство Китая утверждает, что США стремятся поддерживать доминирующее геостратегическое положение, сдерживая рост китайской мощи, и в конечном счете их стремление будет направлено на расчленение и «вестернизацию» Китая, одновременно не допуская возрождения России. Кроме этого, Китай отрицательно относится к взаимоотношениям США с Японией и Тайванем [2].

В целом же аналитики предполагают, что в ближайшей перспективе Китай будет стремиться уменьшить влияние США в Азиатско-Тихоокеанском регионе, не предпринимая при этом резких конфронтационных действий, с тем чтобы не допустить открытого противостояния с превосходящими силами [2].

Между тем современная американская военная доктрина стремится к достижению информационного превосходства над противником путем массированного использования высокотехнологичных систем вооружения и военной техники, поддержанных разветвленной инфраструктурой командования, управления, систем связи и разведки, а также широким использованием высокоточного оружия для уничтожения ключевых целей. Основной задачей является при этом разрушение способностей противника по управлению войсками. Информационные действия ведутся американскими войсками в поддержку традиционного кинетического оружия. Основываясь на подобной доктрине, цель американских военачальников сегодня заключается в том, чтобы быть на несколько шагов впереди противника, находясь внутри его цикла принятия решений и обладая актуальной информацией не допускать противника к пониманию характера действий своих войск, а также быстро и с высокой точностью наносить по нему удары [2].

Основной вывод экспертов сводится к тому, что существующая сегодня в Китае концепция информационной войны не есть борьба в традиционном, западном смысле этого слова. Информационные действия Китая сегодня идут вне военной области, которая более традиционна для Запада. Они главным образом базируются на достижении благоприятного для Китая развития событий и их положительного исхода вместо наращивания мощи технических средств или использования текущей уязвимости американской инфраструктуры. Цели информационных действий Китая, вероятнее всего, удалены во времени на десятилетия в противоположность существующей американской тенденции к немедленным, но краткосрочным успехам [2].

Эксперты полагают, что версия о том, что Китай в настоящее время ведет информационную войну «незападной» формы, получает достаточно много подтверждений. Так, в последнее время Китай стремится накапливать как можно больше значащей информации (особенно в области экономики и обороны), защищать собственную информацию, а также лиц, принимающих решения, и свое национальное единство. Китайцы стремятся эксплуатировать информационные системы их противника, создают общественные структуры, пытаясь влиять на процесс принятия решений их противником. При этом Китай пробует скрыть свои собственные намерения от Запада, потому что китайские стратеги

осознают преимущества такого положения: возможность эксплуатации намного больше, когда цель предпринимаемых действий не осознаётся противником [2].

По мнению американских экспертов, если Китай намеревается победить, не вступая в открытое противоборство, то он в ближайшие годы будет тщательно придерживаться выбранной линии подкупа, запугивания и заимствования каждого возможного преимущества, но не противопоставляя при этом себя Западу и не идя с ним на открытую конфронтацию [2].

В докладе «Возможности КНР вести кибервойну и использовать компьютерные сети», подготовленном в октябре 2009 г. для конгресса США группой Northrop Grumman, указывается, что в рамках Народно-освободительной армии Китая существует детально разработанная доктрина о применении средств нападения на компьютерную инфраструктуру противника [288].

Анализ открытой китайской литературы позволил американским экспертам выделить ряд базовых положений китайской концепции информационной войны. К основным способам ведения информационной войны относят [2]:

- атаки на компьютерные сети;
- информационные операции;
- экономические операции;
- высокоточные удары;
- направленные акции.

Наиболее часто описываемыми целями возможной информационной войны являются [2]:

- преимущество национальной безопасности;
- экономическое преимущество;
- финансовая выгода;
- политическое влияние;
- изменение политики.

В перспективе при ведении информационной войны можно ожидать тесного переплетения всех четырех «инструментов национальной мощи Китая» [2]:

- вооруженных сил (преимущество национальной безопасности);
- экономики (финансовая выгода);
- дипломатии/политики (изменение политики);
- информации (политическое влияние).

Таким образом, любые средства, которые увеличивают национальную мощь, рассматриваются китайскими стратегами в качестве средства информационного противоборства.

Понимание американскими экспертами китайского подхода к концепции информационной войны в академических кругах и сообществах экспертов остается сегодня недостаточным для построения адекватной стратегии противодействия Китаю в информационной сфере в ближайшие годы [2].

На основе детального анализа доступных источников американскими специалистами делается вывод о том, что уязвимость инфраструктуры Америки сегодня, безусловно, очень высока, и угроза «электронного Перл-Харбора», особенно со стороны негосударственной организации, ответные действия про-

тив которой были бы весьма затруднены, не должна игнорироваться. Однако в случае с Китаем, за исключением его возможного нападения на Тайвань, следует особенно внимательно относиться к долгосрочным целям его концепции информационной войны, которые гораздо больше сосредотачиваются на экономике и региональном влиянии. Эксперты подчеркивают, что экономическое развитие остается для Китая самым высоким национальным приоритетом [2].

4.1.2. Силы информационного противоборства в технической сфере (на примере ВС США, НАТО и Китая)

Широкое распространение информационных технологий создало реальную угрозу их использования для вмешательства в процесс функционирования систем государственного и военного управления. В наиболее технически развитых государствах, имеющих обширную информационную и телекоммуникационную инфраструктуру, начали создавать специализированные подразделения. Основными задачами таких подразделений является защита критической информационной государственной и военной инфраструктуры, а также практическая отработка способов ведения войны в киберпространстве. В мирное время на такие подразделения возлагаются задачи ведения разведки и шпионажа, а также диверсионной деятельности в киберпространстве.

4.1.2.1. США

Осознавая важность целей и задач информационного противоборства в технической сфере, США первыми выдели силы операций в киберпространстве в отдельный род войск.

Приказом министра обороны от 23 июня 2009 г. в США сформировано новое командование боевых действий в киберпространстве USCYBERCOM, которое 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 истребителя 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 агентством 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 киберкомандования родов ВС, 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].

Общая численность командования USCYBERCOM на начало 2012 г. составила около 1000 человек. Бюджет USCYBERCOM на 2011 г. превысил 150 млн долларов [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;
- воздушная армия боевых действий в киберпространстве ВВС — 24-я воздушная армия;
- командование боевых действий в киберпространстве морской пехоты;

- командование боевых действий в киберпространстве береговой охраны США.

Командование боевых действий в киберпространстве сухопутных войск ВС США. Общая численность командования составляет около 21 000 военнослужащих и гражданских специалистов, а численность его штаба — около 200 человек. Командование боевых действий в кибернетическом пространстве является функциональным командованием сухопутных войск страны. По административной организации оно подчинено штабу армии США, а по оперативной — командованию USCYBERCOM и является его сухопутным компонентом [281, 282].

Основными задачами командования боевых действий в кибернетическом пространстве сухопутных войск США являются [281]:

- защита компьютерных сетей и автоматизированных систем управления сухопутных войск от несанкционированного доступа;
- организация и проведение кибернетических операций в интересах сухопутных войск и ВС США в целом;
- обеспечение безопасности информации в средствах вычислительной техники сухопутных войск;
- реализация проектов по совершенствованию функционирования компьютерных систем и сетей сухопутных войск.

Основу командования боевых действий в кибернетическом пространстве составляет командование компьютерных сетей и технологий (9-е командование связи). Кроме того, при выполнении задач в оперативное подчинение командованию передаются силы и средства 1-го командования информационных операций и батальона защиты информационных сетей, административно входящих в состав командования разведки и безопасности сухопутных войск США [281].

9-е командование связи организационно включает: штаб, четыре (5-е и 7-е, 311-е и 335-е) командования связи, три (11-ю, 21-ю и 35-ю) бригады связи, батальон спутниковой связи, центр управления глобальными сетевыми операциями и обеспечения безопасности [281].

Командования связи применяются по территориальному принципу. Так, в зоне Северной Америки выполнение задач в кибернетическом пространстве возложено на 7-е командование связи, в Европейской зоне — на 5-е, в зоне Тихого океана — на 311-е, в зоне объединенного центрального командования — на 335-е командование связи, в зоне Центральной и Южной Америки — на 35-ю бригаду связи. Общая численность командования около 17 000 военнослужащих и гражданских специалистов [281].

Командование боевых действий в кибернетическом пространстве ВМС — 10-й оперативный флот ВМС США — сформировано в январе 2010 г. из имевшихся в ВМС профильных сил и средств, а к выполнению возложенных на него задач в полном объеме приступило в октябре 2010 г. Оно относится к категории основных командований ВМС и по административной организации подчиняется начальнику штаба американского флота через его заместителя по разведке и информационному превосходству. По оперативной организации оно подчинено командованию USCYBERCOM и является его

военно-морским компонентом. Численность личного состава данного командования ВМС США — около 10 000 военнослужащих и гражданских специалистов, более 130 человек из которых числятся в штабе [281].

Ключевыми функциями командования являются [281]:

- управление силами радиоэлектронной разведки и РЭБ ВМС;
- организация связи и обеспечение безопасности коммуникационных сетей;
- криптографическое обеспечение деятельности ВМС.

Основу командования боевых действий в кибернетическом пространстве ВМС составляют десять береговых оперативных соединений, объединенных в пять функциональных групп [281]:

- дешифрования и криптографического обеспечения ВМС;
- боевого использования и защиты коммуникационных сетей;
- информационных операций;
- радиоэлектронной разведки;
- научно-исследовательских и опытно-конструкторских работ (НИОКР).

24-я воздушная армия боевых действий в кибернетическом пространстве ВВС США сформирована в феврале 2009 г. путем реорганизации и объединения имевшихся в американских ВВС профильных сил и средств в новую командно-штабную структуру [281, 282].

По административной организации 24-я воздушная армия является компонентом космического командования ВВС США, а в оперативном отношении подчинена командованию USCYBERCOM. С октября 2010 г. армия приступила к выполнению задач по предназначению в полном объеме. Общая ее численность составляет около 5500 военнослужащих и гражданских специалистов [281].

Основными задачами 24-й воздушной армии являются [281]:

- организация и ведение боевых действий в кибернетическом пространстве в интересах как ВВС, так и ВС в целом;
- защита компьютерных сетей и глобальных систем связи ВС США от несанкционированного доступа;
- обеспечение безопасности информации и целостности компьютерных сетей американских ВС;
- подготовка специалистов для действий в киберпространстве;
- подготовка предложений по оснащению подразделений ВВС США новыми аппаратно-программными средствами;
- разработка и реализация проектов по совершенствованию функционирования компьютерных систем и сетей ВВС страны.

24-я воздушная армия ВВС США организационно включает [281]:

- штаб с 624-м оперативным центром (отвечает за организацию и управление операциями в кибернетическом пространстве в интересах как ВВС, так и ВС в целом);
- 67-е крыло боевого применения информационных систем (занимается следующими вопросами: комплектование, оснащение и подготовка подразделений кибернетических операций; отслеживание состояния и

обеспечение защиты информационных сетей ВВС; проведение кибернетических атак на информационно-управляющие сети противника; ведение разведки и РЭБ в кибернетическом пространстве);

- 688-е крыло информационных операций (отвечает за планирование, техническое обеспечение и проведение информационных операций, а также за исследования в области кибернетических технологий и разработку вооружения нового поколения для осуществления кибернетических операций);
- 689-е крыло связи (обеспечивает подготовку, развертывание и функционирование систем управления и связи, а также систем управления воздушным движением на ТВД).

Кроме того, к обеспечению решения задач в интересах этой армии привлекается служба радиоконтроля и распределения частотных диапазонов ВВС, административно подчиненная штабу космического командования ВВС страны [281].

Командование боевых действий в кибернетическом пространстве морской пехоты США сформировано в январе 2010 г. Общая численность около 1000 человек. По линии административного управления командование боевых действий в киберпространстве морской пехоты подчинено коменданту морской пехоты США. По линии оперативного управления оно подчинено командованию USCYBERCOM [281].

Основные функции данного командования [281]:

- ведение боевых действий в кибернетическом пространстве под оперативным руководством командования USCYBERCOM в интересах решения задач оперативных формирований морской пехоты США;
- обеспечение защиты и безопасного функционирования единой компьютерной сети морской пехоты;
- интеграция возможностей глобальной информационной сети национальных ВС в интересах решения задач оперативных формирований морской пехоты;
- криптографическое обеспечение деятельности морской пехоты.

Командование боевых действий в кибернетическом пространстве береговой охраны. На это командование возложено решение следующих основных задач [281]:

- защита компьютерных сетей и автоматизированных систем управления от несанкционированного доступа;
- проведение информационных операций различного масштаба;
- обеспечение безопасности информации;
- реализация проектов по совершенствованию функционирования компьютерных систем и сетей.

В дальнейшем, в соответствии с планами Пентагона, в штабах объединенных командований ВС США с географическими зонами ответственности намечается создать **зональные центры по обеспечению действий в киберпространстве**. Их основной задачей будет организация взаимодействия с центром совместных операций в киберпространстве командования USCYBERCOM в

интересах планирования и проведения совместных кибернетических операций на оперативно-стратегическом уровне в пределах зоны ответственности определенного зонального командования.

Создание USCYBERCOM в США активизировало деятельность других стран в этой сфере. В декабре 2009 г. Южная Корея объявила о создании подразделения кибервойск в ответ на создание аналогичного подразделения в КНДР. Подготовка к созданию кибервойск ведется и в Великобритании. В 2010 г. Китай создал подразделение, занимающееся вопросами кибервойны и информационной безопасности. В 2013 г. о создании войск информационных операций заявило Министерство обороны РФ.

4.1.2.2. Другие страны НАТО: Германия, Великобритания, Нидерланды

Германия

В 2013 г. Германия объявила о наличии подразделения кибероперации численностью 60 человек [122]. Помимо этого, разведывательная служба Германии BND объявила о наборе 130 сотрудников для работы в Национальном центре кибербезопасности. В марте 2013 г. глава BND Г. Шиндлер заявил, что его ведомство ежедневно регистрирует до пяти кибератак на компьютерные системы государственных органов, которые предположительно идут из Китая, и выразил обеспокоенность тем, что похищенная информация может быть использована для будущих диверсий против производителей оружия, телекоммуникационных компаний, правительства и военного ведомства [123].

Вскоре после публикаций разоблачений бывшего сотрудника АНБ Э. Сноудена министр МВД Германии Х.-П. Фридрих заявил, что BND будет выделен дополнительный бюджет в размере 100 млн евро для расширения возможности слежения за киберпространством от 5% до 20% от общего объема Интернет-трафика (максимальная сумма, разрешенная законодательством Германии) [124, 125].

Великобритания

В январе 2015 г. Великобритания и США достигли договоренности о сотрудничестве в сфере кибербезопасности. В ходе встречи Президента США Б. Обамы и британского Премьер-министра Д. Кэмерона лидеры двух стран договорились о создании совместных подразделений по борьбе с киберпреступностью, а также о проведении киберучений, в которых будут использоваться учебные кибератаки друг против друга [126].

Нидерланды

В Нидерландах мероприятия в сфере кибероборонына общенациональном уровне координируются Национальным центром компьютерной безопасности (NCSC). Министерство обороны Нидерландов изложило свою стратегию кибервойн в 2011 г., основной акцент в ней делается на киберзащиту, возложенную на объединенное ИТ-подразделение JIVC (Joint IT branch). Помимо

этого, министерство обороны создает подразделение для ведения кибероперации — DCC (Defensie Cyber Command), которое начало функционировать в конце 2014 года [114, 115].

4.1.2.3. Китай

В структуре народно-освободительной армии Китая (НОАК) имеются специальные подразделения 61398 и 61046, численностью около 2000 человек, предназначенные для проведения кибероперации. Подразделение 61398 подчинено 3-му управлению Генерального штаба НОАК, которое считается аналогом американского АНБ. Подразделение 61398 отвечает за ведение разведки против США и Канады, в то время как подразделение 61046 специализируется на разведке против стран Европы. Точная дата создания подразделения 61398 неизвестна, однако известно, что оно уже в 2004 г. вело набор выпускников Чжэцзянского университета, являющихся специалистами по информационным технологиям [103, 104].

Кроме специальных подразделений НОАК, китайское руководство использует для проведения кибершпионажа и кибератак также группы хакеров, крупнейшей из которых является так называемый «Альянс красных хакеров» (англ. Red Hacker Alliance), численность которого оценивается примерно в 80 000 человек [108, 109].

По оценкам экспертов, в сфере информационной безопасности «Альянс красных хакеров» является неформальной, но управляемой властями Китая сетью, включающей хакеров из всей китайской диаспоры во всём мире, тесно взаимодействующей с 3-м и 4-м управлениями Генерального штаба НОАК [378].

Документы, ставшие доступными широкой общественности после утечки дипломатических источников США в 2010 г., содержат опасения американских специалистов, что Китай использует доступ к исходному коду программных продуктов компании Microsoft для выявления уязвимостей и проведения бескомпроматных кибератак на государственные и научные учреждения США [110].

Дж. Фриц в своей статье 2008 г. [111] утверждает, что китайское правительство с 1995 по 2008 г. было замешано в ряде громких скандалов, связанных со шпионажем и использованием в целях шпионажа «децентрализованной сети студентов, бизнесменов, ученых, дипломатов и инженеров из китайской диаспоры». Шпионаж Китая в США преследует такие цели, как «программы аэрокосмической промышленности, перспективные военные технологии, технологические данные системы C4ISR, высокопроизводительные компьютеры, технологии создания и производства ядерного оружия и крылатых ракет, конструкторская документация полупроводниковых приборов и интегральных схем».

Информацию о деятельности подразделений кибероперации НОАК в основном удалось получить за счет анализа, проведенного американским частным предприятием Mandiant. Эта компания изучила ситуацию с уязвимостью компьютерных сетей в сотнях организаций по всему миру и в 2006 г. выявила группу хакеров, которую обозначила как APT1, а также более двух десятков

аналогичных групп, которые проводили кибероперации из Китая). 18 февраля 2013 г. компания Mandiant выпустила отчет [103], содержавший развернутый анализ деятельности группы APT1 (также именуемой Comment Crew или Shanghai Group), основанный на непосредственных наблюдениях сотрудников компании за последние 7 лет, а также на информации из открытых Интернет-источников.

По данным компании Mandiant, группа APT1 (Shanghai Group) с 2006 по 2013 г. систематически похищала большие объемы данных по меньшей мере в 141 организации, проникая одновременно в компьютерные сети нескольких десятков компаний. Похищенная информация охватывает широкий спектр конфиденциальных данных, касающихся стратегий (внутренние служебные записки, повестки, протоколы), продуктов компаний (технологии, дизайн, результаты испытаний), промышленных процессов (стандарты и т. д.), бизнес-информации (бизнес-планы, переговоры по контрактам, прайс-листы, приобретения или партнерство), содержание переписки по электронной почте и пароли доступа к сетям. Shanghai Group удавалось сохранять незаконный доступ к компьютерным сетям компаний в среднем в течение года (356 дней). В одном случае этой группе удалось сохранять свой доступ к внутренней сети компании 1764 дней (почти 5 лет) [103].

Согласно представленному отчету, Shanghai Group вела шпионаж в основном против организаций англоязычных стран: 87% из 141 компании имеют штаб-квартиры в странах, где английский язык является основным (США, Канада и Великобритания), и только одна компания является французской. Деятельность Shanghai Group велась в глобальном масштабе с использованием приблизительно тысячи серверов, размещенных на отдельных IP-адресах в 13 странах. Из этих 849 уникальных IP-адресов 709 были зарегистрированы в Китае, и 109 — в США. Кроме того, в 97% всех случаев была выявлена принадлежность хакеров к IP-адресам, локализованным в районе Шанхая. Компания Mandiant определила 2551 доменное имя, приписываемое Shanghai Group [103].

По оценкам экспертов компании Mandiant, с высокой степенью вероятности можно считать, что группа APT1, или Shanghai Group, является не чем иным, как подразделением 61398 НОАК. В подтверждение данного вывода компанией Mandiant приводятся следующие факты [103]:

- масштаб операций кибершпионажа, которые вела эта группа на протяжении длительного времени, требует такого объема финансовых, людских и материальных ресурсов, который способно обеспечить только государство;
- технические и языковые навыки, необходимые для проведения кибероперациий, которые вела Shanghai Group, идентичны соответствующим компетенциям подразделения 61398 (шпионаж против США и Канады);
- тактика и способы кибероперациий носили чисто разведывательный характер — не выявлено случаев уничтожения данных или осуществления финансовых махинаций, что характерно для действий обычных хакеров или организованной преступности;

- анализ 20 отраслей экономики, к которым принадлежит 141 организация, которая подверглась кибершпионажу, показывает четкую корреляцию со стратегическими целями двенадцатой пятилетки Китая на 2011–2015 гг.;
- используемые Shanghai Group на протяжении более 7 лет IP-адреса, расположение серверов, характеристики используемых операционных систем указывают на местоположение группы в районе Шанхая.

Китайское правительство, со своей стороны, официально отрицает свою причастность к кибероперациям, заявляя, что Китай является не агрессором, а скорее жертвой растущего числа кибератак. Несмотря на это, эксперты по компьютерной безопасности именно на Китай возлагают ответственность за ряд кибероперациий, направленных на ряд государственных учреждений и предприятий в США, Великобритании, Индии, России, Канаде и Франции [388].

В 2015 г. в новой военной доктрине Китая впервые были упомянуты подразделения, предназначенные для проведения кибероперациий. В соответствии с этим документом в НОАК формируются 3 типа подразделений, которые можно рассматривать как силы кибероперациий [116]:

1. специализированные военные силы для сетевой борьбы — призваны вести оборонительные и наступательные операции в киберпространстве;
2. группы специалистов из гражданских организаций, уполномоченные военным руководством вести сетевые операции. Среди «гражданских организаций» — министерство государственной безопасности и министерство общественной безопасности;
3. «внешние субъекты», которые могут быть организованы и мобилизованы для сетевых операций.

4.1.2.4. Другие страны: Израиль, КНДР, Корея

Израиль

По имеющимся оценкам, ведение операций в киберпространстве в армии Израиля возложено на входящее в структуру военной разведки подразделение 8200, которое по своим функциям является аналогом американского АНБ и насчитывает несколько тысяч человек личного состава [119]. По данным газеты The Telegraph 2012 г. [120], в ближайшие 5 лет израильские ВС намерены увеличить численность и вооружение своих кибервойск, на что выделяется около 500 млн долларов. Согласно заявлению израильского эксперта по вопросам кибероперациий генерал-майора И.Б. Исраэля, готовность Израиля к военным действиям в киберпространстве как в наступательной, так и в оборонительной ее составляющей является одним из ключевых аспектов их новой военной доктрины [120].

КНДР

По сообщению агентства Reuters, в структуру Разведывательного управления Генштаба Корейской народной армии входят подразделения, специализи-

рующиеся на проведении кибероперaций, одним из которых является подразделение 121, известное также как Dark Seoul Gang [105]. Численность подразделения 121 составляет порядка 1800 человек, многие из которых являются выпускниками Пхеньянского университета автоматики [106].

Ранее деятельность подразделения 121 была направлена главным образом против Южной Кореи. По некоторым оценкам, только в 2013 г. подразделение 121 атаковало более 30 000 компьютеров в Южной Корее, включая сервера банков и телекомпаний, а также веб-сайт Президента Южной Кореи. Также подразделение 121 обвиняют в заражении в 2013 г. тысяч смартфонов в Южной Корее вредоносным игровым приложением [105].

Деятельность подразделения 121 оказалась в центре внимания общественности в декабре 2014 г., когда компания Sony Pictures отменила премьеру своего фильма «Интервью», в котором показана попытка покушения на лидера Северной Кореи Ким Чен Ына, после того как компьютерная сеть компании была взломана. Власти США назвали эту кибератаку против кинокомпании Sony Pictures крупнейшей хакерской атакой, когда-либо проводившейся против интересов США, при этом директор ФБР Дж. Коми заявил об уверенности властей США в том, что за этой кибератакой стоят подразделения кибероперaций из КНДР [107]. Власти КНДР официально опровергли все эти обвинения.

Корея

В марте 2013 г. Южная Корея подверглась самой мощной за всю свою историю кибератаке. Были взломаны компьютерные сети ряда крупных банков — Shinhan Bank, Woori Bank и Nonghyup Bank, а также многих телерадиокомпаний (KBS, YTN и MBC). В общей сложности, кибератака затронула более 30 000 компьютеров. Организатор этой атаки не был выявлен, но многие эксперты высказали предположение, что за атакой стоит Северная Корея, поскольку руководство КНДР неоднократно выступало с угрозами в адрес Южной Кореи в ответ на санкции, предпринятые в связи с ядерными испытаниями КНДР, а также ежегодные совместные военные учения Южной Кореи и США [101].

Министерство обороны Республики Корея заявило, что Южная Корея намерена усовершенствовать стратегию кибероборoны страны и укрепить соответствующее подразделение — Cyber Warfare Command, чтобы успешно противостоять возможным новым кибератакам. В связи с этим Южная Корея ведет консультации с США по выработке адекватных мероприятий по комплектованию подразделений в сфере киберзащиты [102].

Создание отдельных родов войск для проведения операций в киберпространстве потребовало развития теории и технологий создания информационно-технического оружия. Особенности терминологии, теории и технологий применения такого оружия рассмотрены далее.

4.2. Информационно-техническое оружие: определение и классификация

Особенностью информационно-технического оружия является его ориентированность на поражение аппаратно-программных средств и систем сбора, передачи, хранения, обработки и представления информации, функционирующих в технической сфере информационного пространства (в киберпространстве).

В работах [2, 269, 292] даны различные определения информационного оружия в технической сфере. Взяв эти термины за основу можно сформулировать 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, применяемое 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. 4.1).

1. По цели использования информационно-техническое оружие классифицируют на [2]:

- обеспечивающее;
- атакующее;
- комбинированное.

Рассматривая данную классификацию, надо отметить, что традиционно средства оборонительных информационно-технических воздействий не рассматриваются в качестве оборонительного информационно-технического оружия. В настоящее время сложился подход, в котором оборонительные средства (средства антивирусной защиты, системы обнаружения и предотвращения вторжений, средства криптографической защиты и т. д.) рассматриваются как элемент обеспечения информационной безопасности и противодействия несанкционированному доступу со стороны некоторых отдельных нарушителей. Вместе с тем в условиях, когда будет вестись информационное противо-

борство в технической сфере, такой подход может вызвать путаницу в определениях и потребует введения категории «*оборонительное информационно-техническое оружие*».

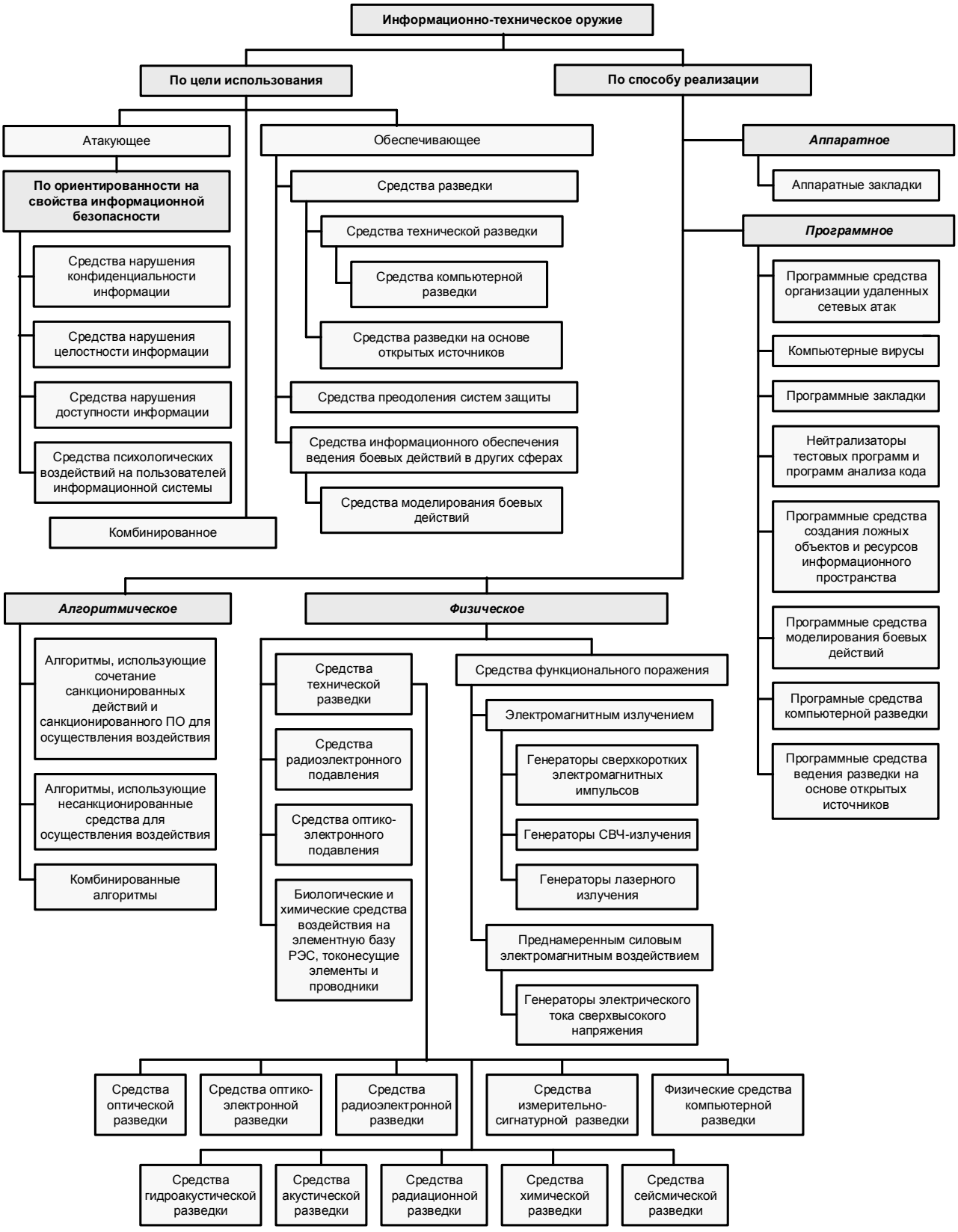


Рис. 4.1. Классификация информационно-технического оружия

Обеспечивающее информационно-техническое оружие — средства и системы, которые применяются для сбора данных, обеспечивающих эффективное применение оборонительного или атакующего информационно-технического и другого оружия, а также против средств защиты атакуемой системы [2].

Обеспечивающее информационно-техническое оружие можно классифицировать следующим образом.

1. Средства разведки:
   - традиционные средства технической разведки, классифицированные по физическим средам, в которых ведется добывание информации;
   - средства компьютерной разведки (как программные средства, так и средства доступа к физической инфраструктуре);
   - средства ведения разведки на основе открытых источников.
2. Средства преодоления систем защиты.
3. Средства информационного обеспечения ведения боевых действий в других сферах.

Необходимо отметить, что средства разведки почти всегда выступают в качестве обеспечивающего оружия. Они 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.

Успешное применение средств преодоления систем защиты позволяет осуществлять эффективные воздействия на хранимую, обрабатываемую и передаваемую в системе информацию с использованием атакующего информационно-технического оружия. Средства разведки позволяют получить информацию об атакующих средствах информационно-технического оружия противника и способах его применения, что позволяет рационально сконфигурировать собственные средства информационно-технической защиты.

Отдельно стоит выделить средства информационного обеспечения ведения боевых действий в других сферах. Под такими средствами понимаются не АСУ и КСА управления вооружением, а комплексы для моделирования боевых действий, которые позволяют путем многократного прогона модели найти рациональный состав сил и средств, а также оптимальную стратегию их действий при любом вероятном сценарии действий противника.

Атакующее информационно-техническое оружие — средства и системы, с помощью которых осуществляется воздействие на информацию, системы ее сбора, передачи, хранения, обработки и представления, а также на используемые в этих системах информационные технологии.

Применение атакующего информационно-технического оружия направлено на срыв выполнения информационной системой целевых задач.

Как правило, атакующее информационно-техническое оружие включает в себя следующие компоненты, объединенные в единую систему [381]:

- средство доставки оружия;
- средство преодоления подсистемы защиты атакуемой системы;
- полезная нагрузка.

Атакующее информационно-техническое оружие, в зависимости от его ориентированности на нарушение конкретного свойства информационной безопасности, можно классифицировать на четыре основных вида [2]:

- средства нарушения конфиденциальности информации;
- средства нарушения целостности информации;
- средства нарушения доступности информации;
- средства психологических воздействий на пользователей информационной системы.

2. По способу реализации информационно-техническое оружие можно подразделить на следующие классы [2, 292]:

- алгоритмическое;
- программное;
- аппаратное;
- физическое.

Информационно-техническое оружие, относящееся к разным классам, может применяться совместно. Кроме того, некоторые виды информационно-технического оружия могут одновременно нести в себе черты нескольких классов.

К **алгоритмическому информационно-техническому оружию относятся** [2]:

- алгоритмы, использующие сочетание санкционированных действий и санкционированного (легального) программного обеспечения для осуществления несанкционированного воздействия на информационные ресурсы;
- алгоритмы использования несанкционированных средств (другого информационно-технического оружия — программного, аппаратного, физического) для осуществления несанкционированного воздействия на информационные ресурсы;
- комбинированные алгоритмы, состоящие из алгоритмов предыдущих двух типов.

Разновидностью алгоритмического оружия являются ***эксплойт*** (exploit) — потенциально невредоносный набор данных (например, санкционированная последовательность команд, графический файл или сетевой пакет нестандартного размера, запрос на установление соединения), который некорректно обрабатывается информационной системой, работающей с такими данными, вследствие ошибок в ней. Результатом некорректной обработки такого набора данных может быть перевод информационной системы в уязвимое состояние.

Примером алгоритмического оружия является DOS-атака (Denial of Service — отказ в обслуживании), заключающаяся в том, что на атакуемую сис-

тему с высокой интенсивностью посылаются корректные запросы на использование ее информационных ресурсов. Это ведет к тому, что возможности информационной системы по обслуживанию таких запросов быстро исчерпываются, и она отказывает в обслуживании всем своим пользователям.

К **программному информационно-техническому оружию** относится ПО, которое может быть использовано для проведения атак на информационные системы противника и позволяющее в процессе своей работы производить несанкционированное воздействие на ее информационные ресурсы. К такому ПО можно отнести:

- программные средства организации удаленных сетевых атак;
- компьютерные вирусы;
- программные закладки;
- нейтрализаторы тестовых программ и программ анализа кода.

Кроме того, к программному информационно-техническому оружию можно отнести ряд программных средств, решающих обеспечивающие задачи как в информационном пространстве, так и в традиционных сферах применения оружия (воздух, земля, море):

- программные средства создания ложных объектов и ресурсов информационного пространства (виртуальные машины);
- программные средства моделирования боевых действий;
- программные средства компьютерной разведки;
- программные средства ведения разведки по открытым источникам в семантической части информационного пространства.

К **аппаратному информационному оружию** могут быть отнесены аппаратные средства, которые изначально встроены в информационную систему или несанкционированно внедренные в нее, а также санкционированные аппаратные средства, обладающие недекларируемыми возможностями, которые позволяют в процессе своей работы производить несанкционированное воздействие на информационные ресурсы системы. К наиболее распространенному типу аппаратного информационно-технического оружия относятся аппаратные закладки.

К **физическому информационно-техническому оружию** могут быть отнесены средства добывания информации путем доступа к физической инфраструктуре информационного пространства, анализу генерируемых этой инфраструктурой физических полей, а также средства радиоэлектронного и огневого поражения ее физических элементов. При этом некоторые специалисты считают более корректным отнесение к физическому информационно-техническому оружию только средств, предназначенных исключительно для воздействия на технические элементы информационной системы.

Обобщение сведений, представленных в работе [292], показало, что классификация физического информационно-технического оружия может иметь следующий вид:

- средства технической разведки, классифицированные по физическим средам, в которых ведется добывание информации;
- средства РЭП;

- средства оптико-электронного подавления;
- средства функционального поражения электромагнитным излучением (генераторы электромагнитных импульсов, генераторы СВЧ-излучения, генераторы лазерного излучения);
- средства функционального поражения преднамеренными силовыми электромагнитными воздействиями (генераторы электрического тока сверхвысокого напряжения);
- биологические и химические средства воздействия на элементную базу РЭС, токонесущие элементы и проводники (например, графитовые бомбы).

4.3. Использование информационно-технического оружия для борьбы с системами военного управления

Борьба с системами управления выделяется в ВС США как вид боевых действий (в рамках информационных операций при проведении военных действий), предусматривающий физическое уничтожение и отсечение командных структур ВС противника от воинских частей с целью нарушить стабильность боевого управления и руководства. Рассмотрим основные особенности подготовки и проведения таких информационных операций, взяв за основу взгляды специалистов ВС США, опубликованные в работах [16, 268, 386, 387].

Данная цель достигается за счет [16, 268]:

- уничтожения командных структур противника (так называемая стратегия «обезглавливания»);
- разрушения коммуникаций системы военного управления (стратегия «удушения»).

При этом выбор метода борьбы во многом определяется характером поставленных тактических и стратегических задач.

4.3.1. Уничтожение командных структур

Уничтожение командных структур противника является хорошо испытанным тактическим и стратегическим приемом ведения войны, однако возможности для этого в разные исторические периоды были разными. Если в прошлом командование войсками размещалось непосредственно на поле боя или вблизи от него, то с появлением технических средств электросвязи (телефония, радиосвязь и т. п.) командные структуры стали располагать на значительном расстоянии от районов ведения боевых действий.

Важной особенностью современной системы управления войсками является разветвленная внутренняя система командных центров (пришедших на смену относительно компактным штабным структурам), которая включает в себя не только объекты штабной инфраструктуры и собственно командование, но и сложную информационную составляющую (оборудование, внутренние и внешние информационные потоки), эффективность функционирования которой напрямую определяет эффективность военного управления.

Грамотно проведенная и надлежащим образом скоординированная информационная атака на такой командный центр способна привести к срыву планов противника даже без физического уничтожения командования.

Более того, вопреки общепризнанным недостаткам тактики узконаправленного воздействия на противника даже изолированная атака на системы контроля и управления может иметь стратегический успех. Это связано с тем, что критически важная информация обычно хранится лишь в определенных и относительно легко выявляемых местах. Это, как правило, командные пункты, центры связи, системы энергоснабжения и т. п. Выявление и последующая ликвидация таких узлов могут привести к полной потере противником возможности управлять задействованными в операции силами.

Таким образом, атака с использованием обычного и высокоточного вооружения в физической сфере с целью уничтожения командных центров более не является единственным способом выполнения поставленной задачи. Их можно вывести из строя также путем нарушения системы электроснабжения, воздействия мощным электромагнитным импульсом (для электронных систем), а также путем внедрения компьютерных вирусов (для баз данных и ПО).

Противник при применении подобного воздействия, как правило, не всегда и не сразу способен обнаружить факт атаки на свою информационную инфраструктуру. К тому же такое воздействие можно провести с максимальной эффективностью еще до начала традиционных боевых действий. Это можно отнести к числу несомненных достоинств информационного оружия, хотя его направленное использование потребует предварительной работы, связанной с обнаружением целей — ключевых командных центров противника, выявлением их уязвимых мест и тщательным выбором способа атаки.

При этом у противника со своей стороны возникает проблема защиты командных центров от подобных атак. В случае традиционных боевых действий их безопасность обеспечивают защитные сооружения, повышение мобильности и маскировка либо совокупность этих методов. Таким образом, возможность проведения противником информационной атаки требует учета ряда новых аспектов, к которым принято относить [16, 386, 387]:

- максимальное снижение рассеянного электромагнитного излучения информационных систем либо генерирование фонового маскирующего излучения;
- отключение неиспользуемых электротехнических систем и коммуникаций, связывающих центры управления с внешними системами;
- обязательное дублирование электропитания информационных систем через независимые генераторы, расположенные в командном центре;
- децентрализация информационных сетей, создание замкнутых, невзаимосвязанных функциональных и информационных контуров;
- создание минимально необходимой информационной инфраструктуры MEII (Minimum Essential Information Infrastructure), состоящей из как можно меньшего набора информационных систем, обеспечиваю-

щих устойчивое функционирование управления в целом и легко восстанавливаемых в случае их повреждения в результате атаки;
- резервирование информационных систем и создание резервных копий критической информации;
- децентрализация управляющих структур в угрожаемый период, а также ограничение личных контактов персонала командного центра (вместо этого предлагается проводить телеконференции и другие легко протоколируемые мероприятия).

В общем виде перечисленные меры противодействия могут быть обобщенны в виде трех основных способов [16, 386, 387]:

1. децентрализация;
2. сокращение числа избыточных каналов связи командных центров с внешним миром;
3. создание дублирующих и резервных систем, которые могут стать целью информационной атаки.

Реализация таких мер потребует значительных финансовых затрат, времени на их разработку и внедрение, а значит существенно усложнит общую архитектуру всей системы командования и боевого управления противника.

4.3.2. Разрушение коммуникаций системы военного управления

Стратегия «удушения», в отличие от стратегии «обезглавливания», предусматривает поражение в первую очередь не командных и управляющих центров, а внешних линий связи и особенно тех узлов связи, в которых концентрируются потоки критически важной информации. Их разрушение приведет к тому, что системы управления в целом оказываются не способными надлежащим образом выполнять функции управления вооружениями и воинскими подразделениями.

В рамках стратегии «удушения» успех операции в основном зависит от следующих факторов [16]:

- точности и достоверности определения структуры подсистемы связи системы управления;
- общего построения и знания принципов организации информационной инфраструктуры противника.

В тех случаях, когда в основе информационной инфраструктуры противника лежит спутниковая связь, нарушить работу системы управления можно не только за счет физического уничтожения спутников связи (что нецелесообразно, так как сделает невозможным использование в дальнейшем этой орбиты из-за рассеивания осколков), но и подавив их средствами РЭП, а также исказив поступающую по соответствующим каналам связи информацию (особенно если противник использует орбитальную группировку, принадлежащую какой-либо другой стране).

Результативность информационных операций на коммуникационные системы противника в значительной мере зависит от масштабов использования

в них современных информационных технологий. Причем зависимость эта носит двоякий характер.

С одной стороны, при широком использовании новых информационных технологий в системах управления имеются избыточные резервные каналы связи и вычислительные ресурсы, подавить которые значительно сложнее, чем при редуцированной системе. Причем одновременно такие резервные каналы выполняют функцию своего рода маскировки действительно значимых линий связи, обслуживающих командные центры.

Например, использование высокотехнологичной системы коммуникаций в Югославии привело к тому, что в ходе воздушных бомбардировок данные НАТО о потерях и разрушениях югославских линий связи оказались сильно завышенными, в то время как в действительности югославская система управления сохранила свою эффективность [16].

С другой же стороны, менее разветвленная и неизбыточная система коммуникаций менее уязвима, хотя сами системы контроля и управления менее эффективны.

В работе [16] подчеркивается, что степень избыточности коммуникационных систем должна планироваться, а не являться результатом их хаотического роста.

Например, дублирование информационного трафика дает определенную гарантию сохранности поступающей критической информации, тогда как дублирование информационных потоков в редуцированных сетях, особенно при их хаотическом построении, способно вызвать перегрузку вычислительных мощностей системы и привести к прекращению обработки информации.

Таким образом, устойчивость и живучесть коммуникационных систем в более высокой степени зависит от принципа их организационного построения, чем от самого факта использования новейших информационных технологий.

Несмотря на то, что информационные операции по борьбе с системами контроля и управления стали весьма существенным аспектом современных представлений о ведении информационной войны, они никоим образом не подменяют собой традиционные способы ведения боевых действий. Особая ценность информационных операций против систем управления состоит в том, что они могут оказаться весьма эффективными на ранних стадиях развития конфликта и, кроме того, создают предпосылки для бескровной победы над противником.

Однако эти преимущества могут быть сведены противником «на нет» путем децентрализации своих командных систем, а также посредством ведения войны на основе сетецентрических принципов.

4.4. Информационно-технические воздействия: определение и классификация

Информационно-техническое воздействие **(ИТВ)** — основной поражающий фактор информационно-технического оружия, представляющий собой воздействие либо на информационный ресурс, либо на информационную сис-

тему 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.

Различают следующие **виды информационно-технических воздействий:**

- одиночные;
- групповые.

Информационно-технические воздействия также классифицируют по характеру поражающих свойств [2, 275]:

- высокоточные воздействия (например, на определенный ресурс в информационно-вычислительной сети);
- комплексные воздействия (например, вся информационно-телекоммуникационная инфраструктура).

По типу воздействий на информацию или информационный ресурс информационно-технические воздействия могут быть:

- пассивными:
  - перехват;
  - несанкционированный доступ;
- активными:
  - разрушающие воздействия;
  - манипулирующие воздействия;
  - блокирующие воздействия;
  - отвлекающие воздействия.

Пассивные воздействия не оказывают непосредственного влияния на работу информационной системы, но могут нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на функционирование информационной системы приводит к тому, что пассивное воздействие трудно обнаружить. Примером пассивного воздействия является разведка параметров информационной системы.

Активные воздействия оказывает непосредственное влияние на функционирование информационной системы (изменение конфигурации системы, нарушение работоспособности и т. д.) и нарушает принятую в ней политику безопасности. Очевидной особенностью активного воздействия, в отличие от пассивного, является принципиальная возможность его обнаружения, так как в результате его осуществления в информационной системе происходят определенные деструктивные изменения.

По цели использования информационно-технические воздействия могут быть классифицированы следующим образом:

- обеспечивающие;
- атакующие;
- оборонительные;
- комбинированные.

По способу реализации информационно-технические воздействия могут быть подразделены на:

- алгоритмические;
- программные;
- аппаратные;
- физические:
    - электромагнитные (среди них отдельно можно выделить воздействия на основе различных электромагнитных волн: радиоэлектронные; оптико-электронные; оптические; силовые);
    - акустические;
    - гидроакустические;
    - радиационные;
    - химические;
    - биологические;
    - на основе новых и других физических принципах.

Классификация информационно-технических воздействий в общем случае по смыслу совпадает с классификацией информационно-технического оружия, за исключением оборонительных воздействий.

Оборонительные информационно-технические воздействия ориентированы на противодействие информационно-техническому оружию противника. 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 собственной защиты.

Средства оборонительных информационно-технических воздействий 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.

Общая схема классификации информационно-технических воздействий представлена на рис. 4.2.

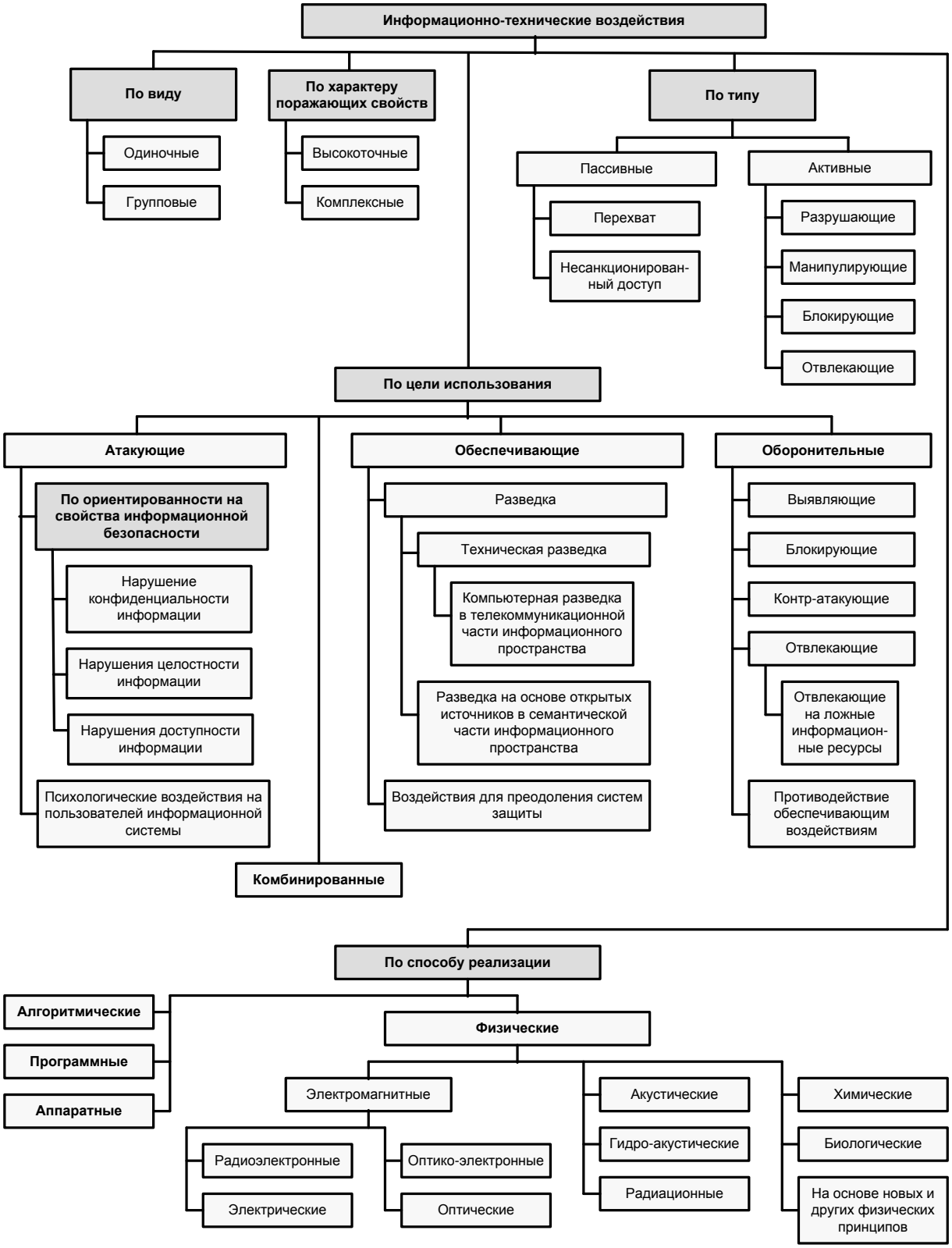


Рис. 4.2. Классификация информационно-технических воздействий

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 воздействий 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 так называемые **оборонительные средства информационно-технического воздействия**, к которым 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 ПО 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, способные выполнить любое подмножество перечисленных ниже функций [2, 320]:

- 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 в 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.

При этом под самокопированием понимается процесс воспроизведения своего собственного кода (в том числе и в модифицированном виде) в оперативной или внешней памяти системы с последующим его внедрением. Под ассоциированием с другой программой понимается интеграция своего кода либо его части в код другой программы таким образом, чтобы при некоторых условиях управление передавалось на код программы с потенциально опасными последствиями [2, 30].

Основные средства информационно-технического воздействия можно классифицировать по способу реализации.

1. Алгоритмические (атакующие):
- эксплойты, ориентированные на управляющую программу информационной системы (ядро или модули операционной системы, драйвера, BIOS);
- эксплойты, ориентированные на прикладные программы информационной системы (пользовательские приложения, серверные приложения, сетевые приложения, браузеры);
- эксплойты, ориентированные на сетевые протоколы информационной системы;
- эксплойты, ориентированные на перевод информационной системы или управляемой ею технологической системы в нештатные или технологически опасные режимы функционирования (например, вирус Stuxnet, внедренный в АСУ технологическим процессом обогащения урана, за счет перехвата и модификации команд от промышленного контролера, в течение длительного времени задавал для центрифуг нештатный режим работы, что привело к отказу более 1000 центрифуг на иранском заводе по обогащению урана).
2. Программные:
   - атакующие:
     - компьютерные вирусы;
     - программные закладки;
     - нейтрализаторы тестовых программ и программ анализа кода;
   - обеспечивающие:
     - программные средства для моделирования боевых действий;
     - программные средства компьютерной разведки в телекоммуникационной части информационного пространства;
     - программные средства ведения разведки на основе открытых источников в семантической части информационного пространства;

- оборонительные:
    - программные средства антивирусной защиты;
    - системы обнаружения и предотвращения вторжений;
    - программные средства криптографической защиты;
    - программные стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
    - средства тестирования ПО и анализа кода для выявления программных закладок и недекларируемых возможностей;
    - средства создания ложных объектов и ресурсов в информационном пространстве.

3. Аппаратные:
    - атакующие:
        - аппаратные закладки;
    - оборонительные:
        - средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей.
4. Физические:
    - атакующие:
        - средства РЭП;
        - средства оптико-электронного подавления;
        - средства функционального поражения электромагнитным излучением (генераторы электромагнитных импульсов, генераторы СВЧ-излучения, генераторы лазерного излучения);
        - средства и комплексы функционального поражения преднамеренными силовыми электромагнитными воздействиями (генераторы электрического тока сверхвысокого напряжения);
        - биологические и химические средства воздействия на элементную базу РЭС, токонесущие элементы и проводники (например, графитовые бомбы).
    - обеспечивающие:
        - средства технической разведки (в том числе и средства компьютерной разведки).

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, связанно с нарушением ее конфиденциальности, так и путем активных действий (атак), направленных на создание условий, которые благоприятствуют добыванию информации.

Общая схема классификации средств информационно-технических воздействий представлена на рис. 4.3.

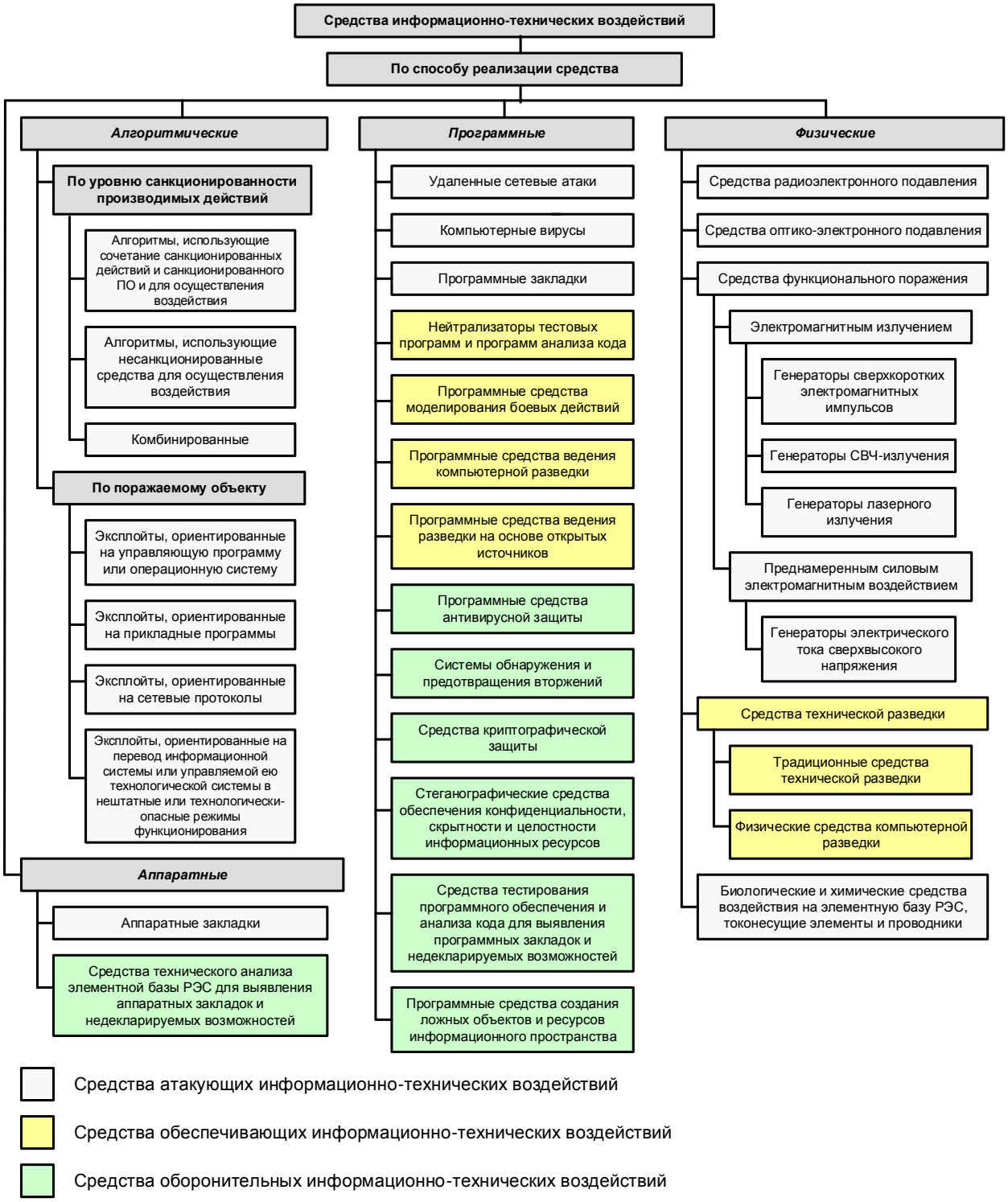


Рис. 4.3. Классификация средств
информационно-технических воздействий

Рассмотрим более подробно наиболее распространенные средства информационно-технического воздействия из представленных на рис. 4.3.

Ввиду того, что антивирусные средства защиты, системы обнаружения и предотвращения вторжений, а также криптографические и стеганографические средства защиты довольно подробно рассмотрены в известной литературе,

основное внимание уделим следующим информационно-техническим воздействиям и средствам их проведения:

- 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.

4.5. Удаленные сетевые атаки

4.5.1. Определение и классификация удаленных сетевых атак

С учетом определения и классификации удаленных воздействий на распределенные вычислительные системы, представленных в работе [380], 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.

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 [322, 380]:

- открытость информационной системы, свободный доступ к информации по организации сетевого взаимодействия и способам защиты, применяемым в системе;
- наличие ошибок в операционных системах, в прикладном ПО и в протоколах сетевого обмена;
- разнородность используемых версий ПО 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 ПО;
- «экономия» на средствах и системах обеспечения безопасности или игнорирование их.

Удаленные сетевые атаки можно классифицировать в соответствии с различными основаниями. Общая схема классификации удаленных сетевых атак представлена на рис. 4.4.

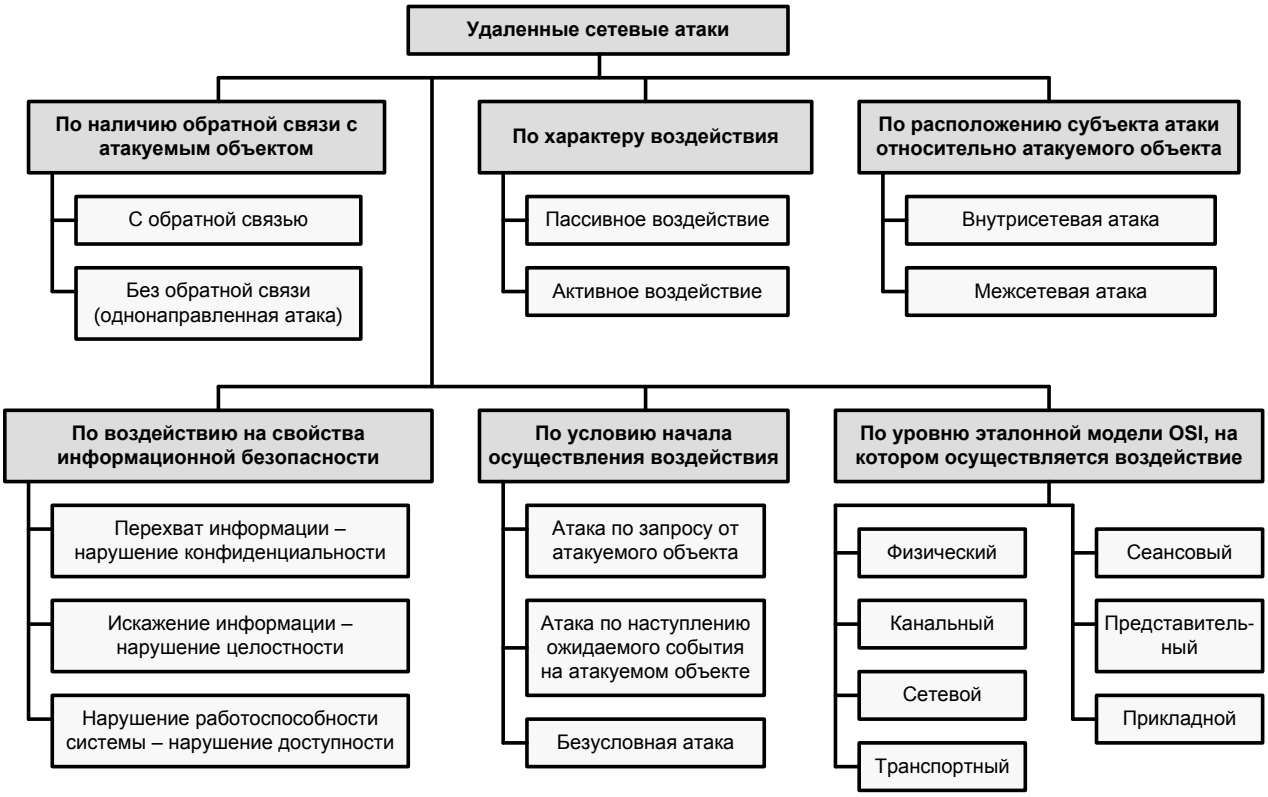


Рис. 4.4. Классификация удаленных сетевых атак

1. По характеру воздействия [322, 380]:

- пассивное воздействие;
- активное воздействие.

Пассивное воздействие не оказывает непосредственного влияния на работу информационной системы, но может нарушать ее политику безопасности. Отсутствие непосредственного влияния на функционирование атакуемой системы приводит к тому, что пассивную сетевую атаку практически невозможно обнаружить. Примером типовой пассивной удаленной сетевой атаки является прослушивание канала связи.

Активное воздействие оказывает непосредственное влияние на функционирование информационной системы (изменение конфигурации системы, нарушение работоспособности и т. д.) и нарушает принятую в ней политику безопасности. Практически все типы удаленных сетевых атак относятся к активным воздействиям. Очевидной особенностью активного воздействия, по сравнению с пассивным, является принципиальная возможность его обнаружения, так как в информационной системе происходят определенные деструктивные изменения.

2. По воздействию на свойства информационной безопасности ресурсов системы [322, 380]:

- перехват информации — нарушение конфиденциальности;
- искажение информации — нарушение целостности;
- нарушение работоспособности системы — нарушение доступности.

Перехват информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. В этом случае осуществляется несанкционированный доступ к информации без возможности ее искажения. Также очевидно, что нарушение конфиденциальности информации является пассивной сетевой атакой. Примером такой атаки, связанной с перехватом информации, может служить прослушивание канала связи в сети.

Искажение информации означает либо полный контроль над информационным потоком между объектами информационной системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, искажение информации ведет к нарушению целостности информационных ресурсов системы. Примером удаленной сетевой атаки, целью которой является нарушение целостности информационных ресурсов, может служить атака, связанная с внедрением ложного сетевого объекта в систему, например внедрения ложного DNS-сервера.

При нарушении работоспособности системы атакующей стороной не предполагается получение несанкционированного доступа к информации. Ее основная цель — добиться, чтобы элементы распределенной информационной системы на атакуемом объекте вышли из строя, а для всех остальных объектов системы доступ к информационным ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить DoS-атака.

3. По условию начала осуществления воздействия [322, 380]:

- атака по запросу от атакуемого объекта;
- атака по наступлению ожидаемого события на атакуемом объекте;
- безусловная атака.

При атаке по запросу от атакуемого объекта атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов могут служить DNS- и ARP-запросы. Важно отметить, что данный тип удаленных атак наиболее характерен для распределенных сетевых информационных систем.

При атаке по условию наступления ожидаемого события атакующий осуществляет наблюдение за состоянием информационной системы, которая является целью атаки. При возникновении определенного события в этой системе атакующий начинает воздействие на нее. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сама атакуемая система. Такие сетевые атаки довольно распространены. Примером такой атаки может быть атака, связанная с несанкционированным доступом к информационным ресурсам компьютера по сети после факта его успешного заражения backdoor-

вирусом, который создает дополнительные уязвимости в подсистеме защиты компьютера.

При безусловной атаке она осуществляется немедленно и безотносительно к состоянию информационной системы и атакуемого объекта. Следовательно, в этом случае атакующий является инициатором начала осуществления атаки.

4. По наличию обратной связи с атакуемым объектом [322, 380]:

- с обратной связью;
- без обратной связи (однонаправленная атака).

Удаленная сетевая атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ. Следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адаптивно реагировать на все изменения, происходящие на атакуемом объекте. Подобные удаленные атаки наиболее характерны для распределенных сетевых информационных систем.

В отличие от атак с обратной связью, удаленным сетевым атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную сетевую атаку можно называть однонаправленной удаленной атакой. Примером такой однонаправленной атаки может служить DoS-атака.

5. По расположению субъекта атаки относительно атакуемого объекта [322, 380]:

- внутрисетевая атака;
- межсетевая атака.

В случае внутрисетевой атаки субъект и объект атаки находятся в одной сети. При межсетевой атаке субъект и объект атаки находятся в разных сетях. Важно отметить, что межсетевая удаленная атака представляет гораздо бóльшую опасность, чем внутрисетевая. Это связано с тем, что в случае межсетевой атаки ее объект и непосредственно атакующий могут находиться на значительном расстоянии друг от друга, что может существенно воспрепятствовать мерам по отражению атаки.

6. По уровню эталонной модели OSI, на котором осуществляется воздействие [322, 380]:

- физический;
- канальный;
- сетевой;
- транспортный;
- сеансовый;
- представительный;
- прикладной.

Удаленные атаки могут быть ориентированы на сетевые протоколы, функционирующие на различных уровнях модели OSI. При этом надо отме-

тить, что атаки, ориентированные на физический, канальный, сетевой и транспортный уровни, как правило, направлены против сетевой инфраструктуры — оборудования узлов сети и каналы связи. Атаки, ориентированные на сеансовый, представительный и прикладной уровни, как правило, направлены против оконечных терминалов сети. В связи с этим, в зависимости от уровня OSI, на который ориентирована атака, конкретный вид используемого воздействия может значительно меняться. Это может быть воздействие средств РЭП или ЭМИ при атаке, ориентированной на физический уровень, при этом эффекты от такого воздействия отображаются на более верхних уровнях модели OSI. Либо DoS-атака на узловое оборудование сети, либо вирус, поражающий операционную систему конечного терминального оборудования.

4.5.2. Примеры способов информационно-технических воздействий на основе удаленных сетевых атак

В связи с тем, что удаленные сетевые атаки совместно с воздействием вирусных средств составляют подавляющее большинство всех информационно-технических воздействий, рассмотрим их более подробно.

Общая классификация способов информационно-технического воздействия на основе удаленных сетевых атак представлена на рис. 4.5.

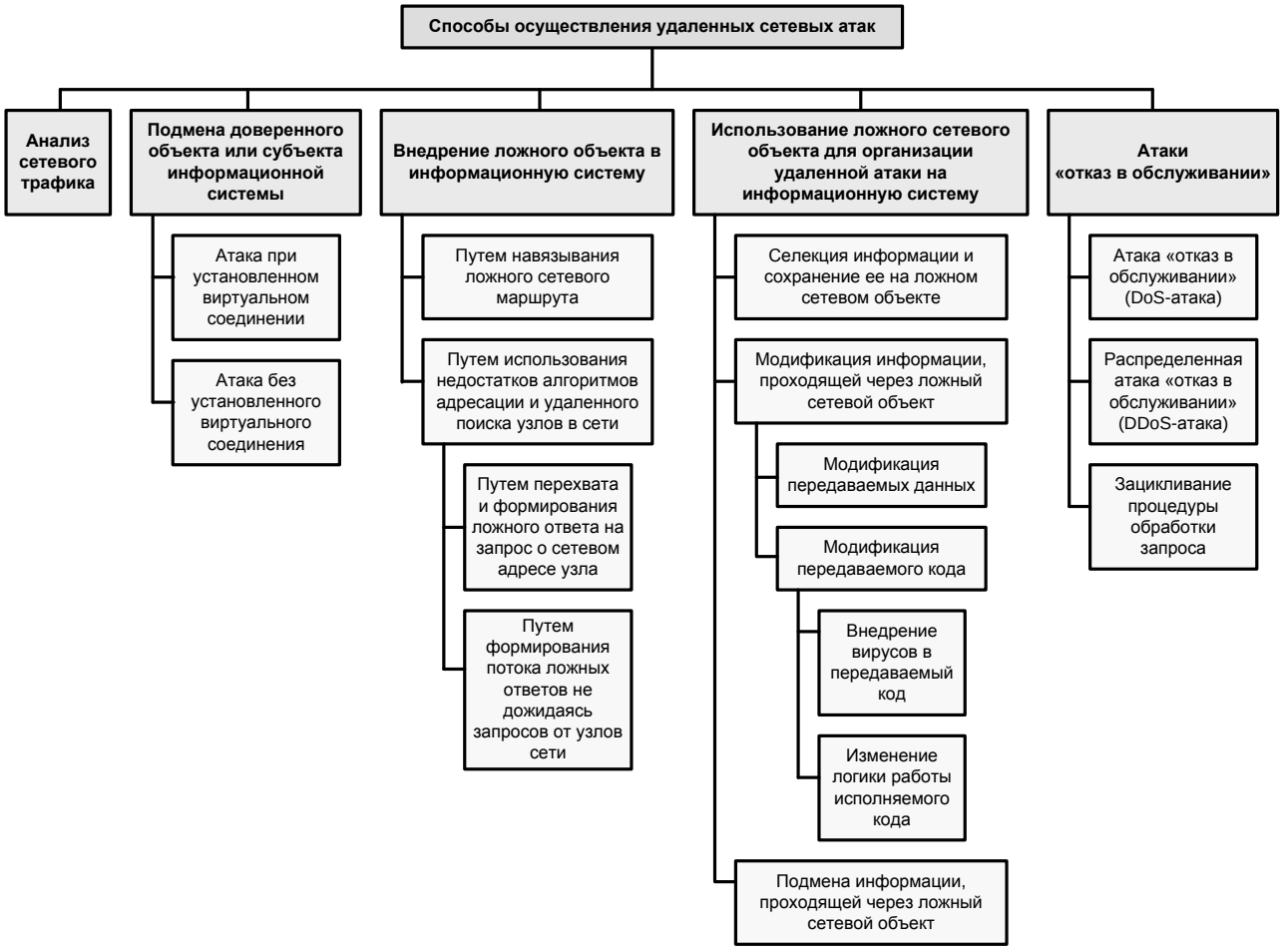


Рис. 4.5. Классификация способов осуществления удаленных сетевых атак

К основным способам информационно-технического воздействия, которые можно отнести к удаленным сетевым атакам, относятся [322, 380]:

- анализ сетевого трафика;
- подмена доверенного объекта или субъекта информационной системы;
- внедрение ложного объекта в информационную систему:
    - внедрение ложного объекта путем навязывания ложного сетевого маршрута;
    - внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети;
        - путем перехвата и формирования ложного ответа на запрос о сетевом адресе узла;
        - путем формирования потока ложных ответов, не дожидаясь запросов от узлов сети;
- использование ложного сетевого объекта для организации удаленной атаки на информационную систему:
    - селекция информации и сохранение ее на ложном сетевом объекте;
    - модификация информации, проходящей через ложный сетевой объект;
    - подмена информации, проходящей через ложный сетевой объект;
- атаки типа «отказ в обслуживании»:
    - отказ в обслуживании (DoS-атака);
    - распределенная атака «отказ в обслуживании» (DDoS-атака);
    - зацикливание процедуры обработки запроса.

4.5.2.1. 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 воздействия, заключающегося в прослушивании канала связи. Данное воздействие называется *анализом сетевого трафика*.

Анализ сетевого трафика позволяет [322, 380]:

- изучить логику работы сетевой информационной системы, то есть получить взаимно однозначное соответствие событий, происходящих в системе, команд и данных, пересылаемых друг другу ее объектами, в момент появления этих событий. Это достигается путем перехвата и анализа пакетов сетевого трафика. Знание логики работы информационной системы позволяет смоделировать и осуществлять другие удаленные сетевые атаки;

- перехватить поток данных, которыми обмениваются объекты сетевой информационной системы. Таким образом, эта атака заключается в получении на удаленном объекте несанкционированного доступа к информации, которой обмениваются два сетевых абонента. Отметим, что при этом отсутствует возможность модификации трафика и сам анализ возможен только внутри одного сегмента сети. Примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети.

В соответствии с выше представленной классификацией анализ сетевого трафика является пассивным воздействием. Осуществление данной атаки без обратной связи ведет к нарушению конфиденциальности информации внутри одного сегмента сети на канальном или сетевом уровне OSI. При этом начало атаки является безусловной по отношению к цели атаки [322, 380].

4.5.2.2. Подмена доверенного объекта или субъекта информационной системы

Одной из проблем безопасности сетевой информационной системы является недостаточная идентификация и аутентификация ее объектов, удаленных друг от друга. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами сетевого взаимодействия. Обычно в сетевых информационных системах эта проблема решается следующим образом: в процессе создания виртуального канала объекты системы обмениваются определенной информацией, уникально идентифицирующей данный канал. Однако такой обмен производится не всегда. Зачастую, особенно при передаче служебной и адресной информации, в сети используются одиночные сообщения, не требующие подтверждения. Так как сетевой адрес достаточно просто подделывается, его можно использовать для виртуальной подмены доверенного объекта или субъекта информационной системы. Таким образом, в том случае, когда в сети используются нестойкие алгоритмы идентификации удаленных объектов, оказывается возможной удаленная атака *подмена доверенного объекта или субъекта информационной системы*, заключающаяся в передаче по сети сообщений от имени произвольного объекта или субъекта информационной системы [322, 380].

Существуют две разновидности этой сетевой атаки, в зависимости от принятой в системе политики информационной безопасности и подхода к защите сетевых соединений [322, 380]:

- атака при установленном виртуальном соединении;
- атака без установленного виртуального соединения.

В случае если в сети для сеанса обмена данными устанавливаются виртуальные соединения, атака будет заключаться в присвоении прав доверенного субъекта сетевого взаимодействия, легально подключившегося к объекту системы. Это позволит атакующему вести сеанс работы с объектом информационной системы от имени доверенного субъекта. Реализация таких удаленных атак обычно состоит в передаче пакетов обмена с атакующего объекта на цель атаки

от имени доверенного субъекта взаимодействия (при этом переданные сообщения будут восприняты системой как корректные). Однако для осуществления атаки данного типа необходимо преодолеть систему идентификации и аутентификации сетевых сообщений [322, 380].

Атаки на информационную систему, в которой не используются виртуальные соединения, заключаются в передаче служебных сообщений от имени сетевых управляющих устройств, например от имени маршрутизаторов. В этом случае возможна подделка сетевого адреса отправителя. Например, так реализуется удаленная атака, использующая навязывание ложного маршрута путем посылки ложных адресных сообщений [322, 380].

Подмена доверенного объекта или субъекта информационной системы может быть классифицирована как активное воздействие, совершаемое с целью нарушения конфиденциальности и целостности информации по наступлению на атакуемом объекте определенного события. Такая удаленная атака может являться как внутрисетевой, так и межсетевой, как с обратной связью, так и без обратной связи с атакуемым объектом и осуществляться на сетевом или транспортном уровнях модели OSI [322, 380].

4.5.2.3. Внедрение ложного объекта в информационную систему

Зачастую в распределенной информационной системе бывают недостаточно надежно решены проблемы идентификации сетевых управляющих устройств (например, маршрутизаторов) при их взаимодействии с объектами системы. В этом случае такая распределенная система может подвергнуться сетевой атаке, связанной с изменением параметров маршрутизации и внедрением в сеть ложного объекта. В том случае, если настройки сети таковы, что для взаимодействия объектов необходимо использовать алгоритмы удаленного поиска узлов, то это также может быть использовано для внедрения в систему ложного объекта. Таким образом, существуют два принципиально разных способа проведения атаки «внедрение ложного объекта в информационную систему» [322, 380]:

- внедрение ложного объекта путем навязывания ложного сетевого маршрута;
- внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети:
    - путем перехвата и формирования ложного ответа на запрос о сетевом адресе узла;
    - путем формирования потока ложных ответов не дожидаясь запросов от узлов сети.

Современные глобальные сети представляют собой совокупность сетевых сегментов, связанных между собой через узлы-маршрутизаторы. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждой пары адресатов сети указывается оптимальный маршрут. Основная цель атаки, связанной с внедрением ложного объекта путем навязыванием ложного маршрута, состоит в том, чтобы изменить исходную маршрутизацию на объекте сетевой информационной системы так, чтобы

новый маршрут проходил через ложный объект сети — узел атакующего. Реализация этой атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. Данная атака проходит в две стадии [322, 380].

- Атакующему необходимо от имени сетевых управляющих устройств (например, маршрутизаторов) произвести рассылку по сети специальных служебных сообщений, что приведет к изменению маршрутизации в сети. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, который будет проходить через его узел.
- Атакующий наращивает количество трафика, перенаправленного через свой узел, и получает возможность вести прием, анализ и передачу сообщений, передаваемых по сети.

Внедрение ложного объекта путем навязывания ложного сетевого маршрута — активное воздействие безусловное по отношению к цели атаки. Данная удаленная атака может осуществляться как внутри одного сегмента сети, так и межсетевым образом, как с обратной связью, так и без обратной связи с атакуемым объектом на сетевом, транспортном и прикладном уровне модели OSI [322, 380].

В распределенной информационной системе часто оказывается, что ее удаленные объекты изначально не имеют достаточно информации, необходимой для адресации передаваемых сообщений. Обычно такой информацией являются аппаратные и логические адреса объектов системы. Для получения подобной информации в распределенных системах используются различные алгоритмы удаленного поиска, заключающиеся в передаче по сети специальных поисковых запросов. После получения ответа на запрос запросивший субъект системы обладает всеми необходимыми данными для адресации. Руководствуясь полученными из ответа сведениями об искомом объекте, запросивший субъект системы начинает передачу информации. Примером подобных запросов, на которых базируются алгоритмы удаленного поиска, могут служить ARP- и DNS-запросы в сети Интернет [322, 380].

В случае использования в распределенной информационной системе механизмов удаленного поиска существует возможность на атакующем объекте перехватить посланный запрос и послать на него ложный ответ, где указать данные, использование которых приведет к адресации на атакующий ложный узел. В дальнейшем весь поток информации между субъектом и объектом взаимодействия будет проходить через этот ложный объект информационной системы [322, 380].

Другой вариант внедрения в распределенную информационную систему ложного объекта использует недостатки алгоритма удаленного сетевого поиска и состоит в периодической передаче на атакуемый объект заранее подготовленного ложного ответа без приема поискового запроса. При этом атакующий может спровоцировать атакуемый объект на передачу поискового запроса — и тогда его ложный ответ будет немедленно принят и обработан. Такая удаленная атака чрезвычайно распространена в глобальных сетях, когда у атакующего

из-за нахождения его в другом сетевом сегменте относительно цели атаки просто нет возможности перехватить поисковый запрос [322, 380].

Внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети — активное воздействие, совершаемое с целью нарушения конфиденциальности и целостности информации, которое может являться атакой по запросу от атакуемого объекта, а также безусловной атакой. Данная удаленная атака может быть как внутрисетевой, так и межсетевой, имеет обратную связь с атакуемым объектом и осуществляется на канальном, сетевом и прикладном уровнях модели OSI [322, 380].

4.5.2.4. Использование ложного объекта для организации удаленной атаки на систему

После внедрения ложного объекта в сеть и получения контроля над проходящим потоком информации в сети ложный объект может применяться для различных способов воздействия на перехваченную информацию. Выделяют следующие основные воздействия на информацию, перехваченную ложным объектом [322, 380]:

- селекция информации и сохранение ее на ложном сетевом объекте;
- модификация информации, проходящей через ложный сетевой объект;
- подмена информации, проходящей через ложный сетевой объект.

Селекция информации и сохранение ее на ложном сетевом объекте являются пассивной сетевой атакой, сходной с атакой «анализ сетевого трафика», которая дополнена динамическим семантическим анализом, производимым на ложном объекте. Вместе с тем наибольший интерес представляет возможность использования ложного объекта для модификации или подмены информации.

Рассматривают два основных вида модификации информации [322, 380]:

- модификация передаваемых данных;
- модификация передаваемого кода:
    - внедрение вирусов в передаваемый код;
    - изменение логики работы исполняемого кода.

Для модификации передаваемых данных на внедренном объекте производятся селекция потока перехваченной информации и его анализ. При этом может быть распознан тип передаваемых файлов (исполняемый или файл, содержащий данные). При обнаружении файла данных появляется возможность модифицировать эти данные, проходящие через ложный объект. При этом, если модификация данных является достаточно стандартным воздействием, то на модификации передаваемого кода стоит остановиться отдельно.

Ложный объект, проводя семантический анализ информации, проходящей через него, может выделять среди потока информации файлы, содержащие исполняемый код. Для того чтобы определить, что передается по сети — код или данные, — необходимо распознавать определенные особенности, свойственные конкретным типам исполняемых файлов. При этом можно выделить два различных по цели вида модификации кода [322, 380]:

- внедрение вирусов в передаваемый код;
- изменение логики работы исполняемого кода.

При внедрении вирусов в передаваемый код к исполняемому файлу дописывается тело вируса, а также изменяется точка начала исполнения кода так, чтобы она указывала на начало кода внедренного вируса. Описанный способ, в принципе, ничем не отличается от стандартного заражения исполняемого файла вирусом, за исключением того, что файл оказывается заражен вирусом в момент передачи его по сети. Такое возможно лишь при использовании воздействия «внедрение ложного объекта» [322, 380].

При изменении логики работы исполняемого файла при передаче его по сети происходит похожая модификация исполняемого кода. Однако ее цель — алгоритмическое воздействие, ориентированное на внедрение программных закладок, внесение в исполняемый файл дополнительных уязвимостей или эксплойтов. Сложностью такого воздействия является то, что для него, как правило, требуется предварительное исследование логики функционирования исполняемого файла [322, 380].

Внедрение ложного объекта позволяет не только модифицировать, но и подменять перехваченную им информацию. При возникновении в сети определенного контролируемого ложным объектом события одному из участников обмена посылается заранее подготовленная дезинформация. При этом такая дезинформация, в зависимости от контролируемого события, может быть как исполняемым кодом, так и данными.

4.5.2.5. Атаки типа «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 запускаются 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 он 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.

1. **Отказ в обслуживании (DoS-атака)** — передача с одного адреса такого количества запросов на атакуемый объект, которое позволяет передать пропускная способность канала связи. В данном случае, 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.

2. **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.
3. **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.

Удаленная сетевая атака «отказ в обслуживании» классифицируется как активное воздействие, осуществляемое с целью нарушения работоспособности системы, безусловное относительно цели атаки. Данная атака является однонаправленным воздействием, осуществляемым как межсетевым, так и внутрисетевым образом, осуществляемым на сетевом, транспортном и прикладном уровнях модели OSI [322, 380].

Схема классификации основных способов осуществления атаки «отказ в обслуживании» представлена на рис. 4.6.

Рис. 4.6. Наиболее распространенные способы осуществления атаки «отказ в обслуживании»

Наиболее распространенными способами осуществления атаки «отказ в обслуживании» являются следующие.

1. Способы, основанные на насыщении полосы пропускания системы, — атаки, связанные с большим количеством, как правило, бессмысленных или сформированных в неправильном формате запросов к информационной системе или ее сетевому оборудованию, с целью обеспечить отказ в работе системы из-за исчерпания ее системных ресурсов (процессорного времени, памяти или пропускной способности каналов связи). К наиболее распространенным таким способам относятся [382]:

- атаки типа HTTP-flood и ping-flood;
- Smurf-атака (ICMP-flood);
- атака с помощью переполнения пакетами SYN в TCP соединении (SYN-flood).

2. Способы, основанные на недостатке ресурсов системы, — атаки, связанные с захватом или избыточным использованием ресурсов информационной системы. К наиболее распространенным таким способам относятся [382]:

- отправка «тяжелых» или «сложных» пакетов;
- переполнение сервера log-файлами;
- использование уязвимостей неправильно настроенной подсистемы управления квотами использования системных ресурсов;
- использование уязвимостей недостаточной проверки данных пользователей;
- атаки, вызывающие ложные срабатывания подсистемы защиты информационной системы.

3. Способы, основанные на удаленном несанкционированном доступе за счет использования эксплойтов в ПО атакуемой системы. К наиболее распространенным таким способам относятся [382]:

- удаленное использование уязвимостей в программном коде операционной системы и прикладного ПО информационной системы;
- удаленное использование переполнения буфера программы;
- удаленное использование ошибок в разделении памяти между программами в защищенном режиме операционной системы.

4. Способы, основанные на использовании эксплойтов сетевых протоколов атакуемой системы. К наиболее распространенным таким способам относятся [382]:

- DoS-атаки, использующие уязвимости в ПО DNS-серверов;
- DDoS-атаки на DNS-серверы.

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 [382].

4.6. Компьютерные вирусы

Несмотря на долгую историю компьютерной вирусологии, использование вирусов в качестве боевых средств информационно-технического воздействия начато сравнительно недавно. К первому случаю такого использования относится использование в 2010 г. вируса Stuxnet с целью срыва ядерной программы Ирана за счет инфицирования АСУ технологическим процессом обогащения урана [323].

Особенностью современных боевых вирусов является то, что они, как правило, являются комплексными продуктами и состоят из различных модулей, которые относятся к различным типам и 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).

В отличие от своих «непрофессиональных собратьев», средства информационно-технического воздействия на основе вирусов обладают следующими особенностями функционирования [323]:

- избирательность цели и действий;
- использование уязвимостей, в том числе уязвимостей 0-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.

Компьютерные вирусы в соответствии со способами распространения и вредоносной нагрузкой можно классифицировать по четырем основным типам [322]:

1. классические вирусы;
2. программы типа «червь»;
3. программы типа «троян»;
4. другие вредоносные программы.

По способу хранения в памяти информационной системы компьютерные вирусы можно классифицировать на [321]:

- резидентные;
- нерезидентные.

Резидентные вирусы после активации хранят свои копии в оперативной памяти системы, способны перехватывать события операционной системы и программ (например, обращения к файлам или дискам) и инициировать при этом процедуры заражения обнаруженных объектов. Поэтому резидентные вирусы опасны не только во время работы инфицированной программы, но и после ее окончания. Резидентные копии таких вирусов остаются жизнеспособными вплоть до выключения или перезагрузки информационной системы [321].

Нерезидентные вирусы, напротив, активны на довольно непродолжительных интервалах времени — пока функционирует инфицированная вирусом программа [321].

Для защиты от обнаружения со стороны антивирусов и средств защиты информационной системы в вирусах могут применяться следующие технологии [322]:

- *шифрование* — вирус состоит из двух функциональных элементов: собственно вирус и шифратор. При этом каждая конкретная копия вируса состоит из шифратора, собственного случайного ключа и собственно вируса, зашифрованного этим ключом;
- *метаморфизм* — создание различных копий вируса путем замены блоков команд на эквивалентные, путем перестановки местами участков кода, вставки между значащими участками кода незначащих команд и др.;
- *перехват управления* при обращении операционной системы или системы защиты к инфицированным элементам информационной системы.

Использование этих технологий маскировки вирусов привело к появлению следующих типов вирусов, которые классифицируются по технологии защиты от обнаружения [322]:

- ***шифрованный вирус*** — вирус, использующий простое шифрование своего тела со случайным ключом и неизменный шифратор. Такие вирусы могут быть обнаружены по сигнатуре шифратора;
- ***метаморфный вирус*** — вирус, применяющий метаморфизм ко всему своему телу для создания новых копий;
- ***полиморфный вирус*** — вирус, использующий метаморфный шифратор для шифрования тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора, также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм шифрования;
- ***стелс-вирус*** (stealth virus — вирус-невидимка) — вирус, полностью или частично скрывающий свое присутствие в системе путем перехвата обращений к операционной системе на осуществление чтения или записи в инфицированных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.) и подмены их содержимого с целью демонстрации подсистеме защиты оригинального содержимого объекта до его заражения.

Кроме того, компьютерные вирусы можно классифицировать по способу активации [322].

- *Требующие активного участия пользователя*. Отличительной особенностью таких компьютерных вирусов является использование обманных методов. Это проявляется, например, когда получатель инфицированного файла вводится в заблуждение текстом письма и добро-

вольно открывает вложение с «почтовым червем», тем самым активируя его.

- *Не требующие активного участия пользователя*. Активация компьютерных вирусов без участия пользователя возможна за счет того, что вирус самостоятельно находит и использует уязвимости в безопасности информационной системы.

Классификация компьютерных вирусов представлена на рис. 4.7. Далее представлены особенности основных типов вирусов более подробно.

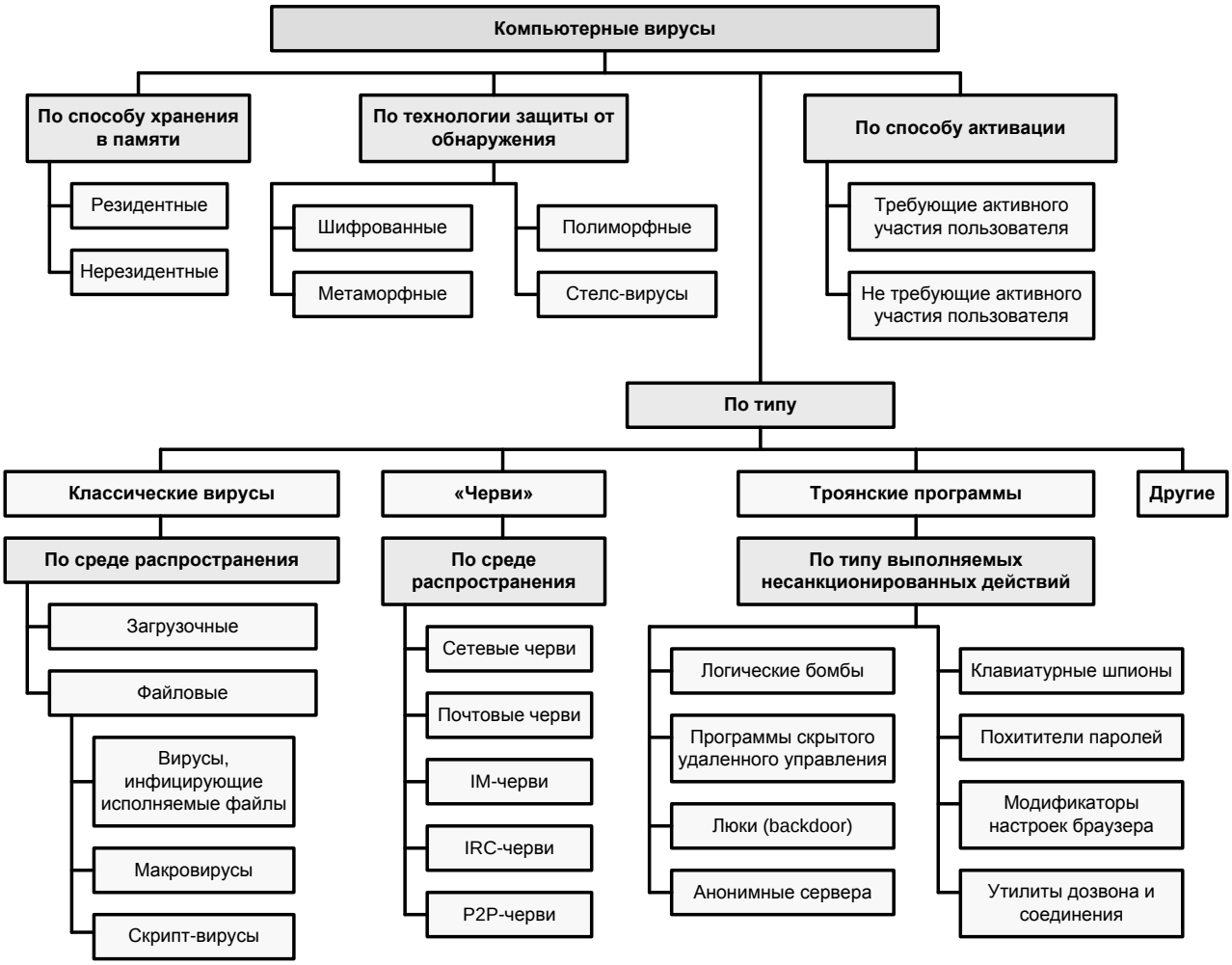


Рис. 4.7. Классификация компьютерных вирусов

4.6.1. Классические вирусы

Основное свойство классического компьютерного вируса — это способность к саморазмножению [322].

Вирус — это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области операционных систем и прочие информационные ресурсы. При этом дубликаты сохраняют способность к дальнейшему распространению [322].

Условно жизненный цикл вируса можно разделить на пять стадий [322]:

1. проникновение на чужой компьютер;
2. активация;
3. поиск объектов для заражения;
4. подготовка копий;
5. внедрение копий;

Путями проникновения вируса могут служить мобильные носители, сетевые соединения, а также любые другие каналы, по которым можно скопировать файл. Однако, в отличие от «червей», вирусы не используют сетевые ресурсы — заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал [322].

После проникновения следует активация вируса. В соответствии с выбранным методом активации вирусы делятся на следующие виды [322]:

- ***загрузочные вирусы*** — заражают загрузочные сектора жестких дисков и мобильных носителей;
- ***файловые вирусы*** — заражают файлы. Отдельно по типу среды обитания в этой группе также выделяют следующие типы вирусов:
    - ***вирусы, инфицирующие исполняемые файлы*** — различными способами внедряются в исполняемые файлы программ (внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы;
    - ***макровирусы*** — инструкции, написанные на внутреннем языке команд заражаемого приложения (на так называемых, макросах);
    - ***скрипт-вирусы*** — инструкции, написанные на внутреннем языке для определенной командной оболочки (скриптов).

Дополнительным отличием вирусов от других вредоносных программ служит их жесткая привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан [322].

Основная цель вируса — распространение на другие ресурсы информационной системы и выполнение деструктивных действий при определенных событиях или действиях пользователя [322].

4.6.2. Черви

В отличие от классических вирусов, программы типа «червь» — это вполне самостоятельные программы, которые также способны к саморазмножению, однако при этом они способны и к самостоятельному распространению с использованием сетевых каналов. Для подчеркивания этого свойства иногда используют термин «сетевой червь» [322].

Программа типа «червь» — это программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению подсистем защиты информационных систем, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом [322].

Жизненный цикл «червей» состоит из следующих стадий [322]:

- проникновение в информационную систему;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- распространение копий.

В зависимости от способа проникновения в систему «черви» классифицируются на следующие типы [322]:

- ***«сетевые черви»*** — используют для распространения локальные сети, каналы в информационно-вычислительных сетях, глобальные сети, в том числе и Интернет;
- ***«почтовые черви»*** — распространяются с помощью почтовых программ;
- ***«IM-черви»*** — используют для распространения системы мгновенного обмена сообщениями типа Internet Massager;
- ***«IRC-черви»*** — распространяются по каналам IRC (Internet Relay Chat) для обмена информацией в чатах и форумах;
- ***«P2P-черви»*** — распространяются при помощи пиринговых файлообменных P2P-сетей .

Сетевые черви могут кооперироваться с вирусами — такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса) [322].

4.6.3. Троянские программы

В отличие от вирусов и червей, в программах типа «троянский конь» не всегда предусмотрен функционал саморазмножения. Довольно большая часть таких программ функцией саморазмножения вообще не обладает [322].

Программа типа «троян» («троянский конь») — программа, основной целью которой является вредоносное воздействие по отношению к информационной системе путем выполнения несанкционированных действий, а именно — кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или несанкционированное использование его ресурсов [322].

Некоторые «трояны» способны к самостоятельному преодолению подсистемы защиты информационной системы с целью проникновения в нее. Однако в большинстве случаев они проникают в систему вместе с вирусом либо с червем. В этом случае вирус или червь следует рассматривать как средство доставки, а «троян» — как средство информационного поражении [322].

Жизненный цикл «троянов» состоит всего из трех стадий [322]:

- проникновение в систему;
- активация;
- выполнение вредоносных действий.

Как уже говорилось выше, проникать в информационную систему «трояны» могут двумя путями — самостоятельно и за счет кооперации с вирусом или «сетевым червем». В первом случае может быть использована маски-

ровка, когда «троян» выдает себя за полезное приложение, которое пользователь самостоятельно копирует и запускает. При этом программа-носитель действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные «трояну» [322].

Для проникновения в информационную систему «трояну» необходима активация, и здесь он похож на «червя»: либо требует активных действий от пользователя, либо самостоятельно заражает его, используя уязвимости в защите информационной системы [322].

Программы типа «троян», как правило, классифицируются по типу выполняемых несанкционированных действий [322].

- ***Логические бомбы*** — характеризуются способностью при выполнении заранее заложенных в них условий (конкретный день, время суток, определенное действие пользователя или команда извне) выполнять несанкционированные действия по уничтожению или искажению информации, воспрещения доступа к тем или иным важным фрагментам информационного ресурса, либо дезорганизации работы технических средств.
- ***Программы скрытого удаленного управления*** — это «трояны», которые обеспечивают несанкционированный удаленный контроль над инфицированной информационной системой. Такие программы предоставляют удаленному пользователю возможность скрытого исполнения программ в информационной системе, поиска, модификации и удаления информации, возможности скрыто загружать или отсылать информацию.
- ***Люки (backdoor)*** — программы, находящие или создающие уязвимости в защите информационной системы с целью дальнейшего предоставления удаленного несанкционированного доступа к ней. От программ удаленного управления этот тип «трояна» отличается более простой функциональностью и ориентированностью не на контроль системы, а на организацию доступа к ней. Как правило, данные «трояны» имеют функционал загрузки и запуска удаленных файлов. Это позволяет при необходимости загрузить на инфицированную систему программу скрытого удаленного управления и получить над информационной системой несанкционированный удаленный контроль.
- ***Анонимные сервера*** — разновидность «троянов», которые используют ресурсы зараженной информационной системы в своих целях, связанных с несанкционированной сетевой активностью: создание bot-сетей и управление ими, выполнение несанкционированных распределенных вычислений, организация и координация DDOS-атак, массовая отправка электронной почты и другие подобные действия.
- ***Клавиатурные шпионы*** — находясь в оперативной памяти, записывают все данные, набираемые на клавиатуре с целью последующей их передачи.

- ***Похитители паролей*** — предназначены для кражи паролей и другой конфиденциальной информации путем поиска на зараженной системе специальных файлов, которые ее содержат.
- ***Модификаторы настроек браузера*** (или других программ просмотра информации в сети) — изменяют настройки браузера таким образом, чтобы стали возможными удаленное исполнение кода в браузере, доступ к хранящейся в нём конфиденциальной информации, подмена сертификатов безопасности, перенаправление на ложные страницы и т. п.
- ***Утилиты дозвона и соединения*** — в скрытом от пользователя режиме инициируют несанкционированное подключение к удаленным сервисам.

Отдельно отметим, что существуют программы из класса «троянов», которые наносят вред другим удаленным информационным системам и сетям, при этом не нарушая работоспособности инфицированной системы. Примером таких программ могут служить анонимные сервера — организаторы DDoS-атак [322].

4.6.4. Примеры средств информационно-технических воздействий на основе компьютерных вирусов

Рассмотрим наиболее известные к настоящему времени средства информационно-технических воздействий на основе вирусов, а также особенности их применения в информационных операциях современности.

Stuxnet. Вирус Stuxnet — компьютерный червь, поражающий компьютеры под управлением операционной системы Microsoft Windows и промышленные системы, управляющие технологическими процессами. Это первое широко известное вирусное программное средство, имеющее точечную целевую функцию инфицирования конкретной АСУ с целью функционального поражения управляемого ею технологического процесса [323].

Вирус Stuxnet, внедренный в АСУ технологическим процессом обогащения урана, за счет перехвата и модификации команд от промышленного контролера марки Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens, в течение длительного времени задавал для центрифуг нештатный режим работы, что привело к отказу более 1000 центрифуг на иранском заводе по обогащению урана. Уникальность программы заключалась в том, что впервые в истории кибератак вирус физически разрушал инфраструктуру [323].

По заявлению бывших сотрудников NSA и JCS DoD, этот вирус был разработан в рамках американо-израильской операции противодействия ядерным планам Ирана. Stuxnet включает десяток выполняемых компонент общим объемом в 1,2 Мбайта, написанных в основном на языках C и C++. Базовой функциональной средой является Win32 [323].

Stuxnet поддерживает как минимум 8 способов саморазмножения, эксплуатацию более десяти уязвимостей, в том числе программной закладки (мастер-пароля), осуществляет контроль и управление через удаленные компьютеры (при обнаружении выхода в Интернет), включает Windows- и

PLC-руткиты и другие способы маскировки и скрытия, а также выполняет обработку ошибочных ситуаций и др. Кроме того, Stuxnet способен внедряться в ряд системных «доверенных» процессов, в том числе инициируемых антивирусными продуктами, такими как: Avira, BitDefender, Computer Associates, Eset, F-Secure, Kaspersky Lab, McAfee, Symantec и Trend Micro [323].

Отличительными особенностями Stuxnet являются [323]:

- использование уязвимостей 0-дня;
- возможность распространения в изолированной среде (без выхода в Интернет), посредством flash-накопителей или собственной локальной p2p-сети;
- наличие компонент, подписанных 2 похищенными электронными цифровыми подписями;
- заражение системы управления технологическими процессами Siemens Simatic Step7;
- выполнение модификации PLC-кода на контроллерах Siemens с целью деструктивного воздействия на физическое оборудование (центрифуг обогащения урана) и дезинформацию операторов завода.

Функциональные клоны Stuxnet, адаптированные под новые цели, могут успешно использоваться для диверсий в АСУ промышленных предприятий, электростанций, управления движением транспорта и т. п.

Flame. Вирус-червь Flame, известный также как Skywiper или Flamer, является примером средства, ориентированного на решение конкретных разведывательных задач на Ближнем Востоке, в первую очередь в Иране. Отмечено около 700 заражений этим вирусом. Активный период действия вируса составлял порядка 6 лет до момента его обнаружения в 2012 г. [323].

Вирус Flame представляет собой комплекс программ объемом около 20 Мбайт (устанавливается поэтапно) и значительно превосходит в этом отношении вирус Stuxnet. В состав Flame входят: криптобиблиотеки, библиотеки архивирования zlib, libbz2, ppmd, СУБД sqlite3, веб-сервер, виртуальная машина Lua. Базовой функциональной средой является Win32 [323].

Ключевыми особенностями Flame являются [323]:

- использование уязвимостей, в том числе 0-дня;
- компрометация ЭЦП в ОС Windows (путем атаки на MD5);
- поиск офисных документов, проектной документации и чертежей (например, pdf и drw файлов), контактной информации, в том числе из соцсетей;
- возможность перехвата аудио и экранной информации;
- поиск и подключение к BIuetooth-устройствам;
- закрытая передача информации на удаленный компьютер;
- наличие инструментария для взлома механизмов защиты.

Что касается последнего, то в составе Flame имеются средства инвентаризации, мониторинга трафика, включая подсистему сбора парольной информации, поиска остаточной информации, анализа файловой системы, архивов и множества типов файлов, кейлогер и т. п. [323].

Flame может распространяться через USB-носители и сеть, также имеет оригинальную возможность обновления путем компрометации обновлений ОС Windows. Работа программы обеспечивается сложной динамичной инфраструктурой — например, известно около сотни доменов, задействованных для передачи данных на командные серверы Flame, попеременно располагавшиеся в различных странах мира. Несмотря на явно разведывательные цели, Flame содержит модуль удаления файлов [323].

Предположительно вирусы Flame и Stuxnet были разработаны одной командой в рамках американо-израильского сотрудничества и использовались совместно. При этом Flame имел разведывательные цели, а Stuxnet — диверсионные.

Duqu — вирус-червь, обнаруженный в 2011 г. Некоторые исследователи полагают, что он связан с червем Stuxnet. Распространение данного вируса происходило через электронную почту. Заражение системы происходит посредством использования уязвимости в ядре Windows, допускающей выполнение вредоносного кода. После заражения системы и установления связи с сервером происходит загрузка и установка дополнительного модуля, предназначенного для сбора сведений о системе, поиска файлов, снятия скриншотов, перехвата паролей и ряда других функций. Особенностью вируса Duqu является то, что он использует объектно-ориентированный фреймворк, написан на чистом C и скомпилирован Microsoft Visual C++ с необычными настройками оптимизации [324].

Специалисты компании Symantec считают, что создатели Duqu имели доступ к исходному тексту Stuxnet и целью Duqu был сбор информации для следующей версии Stuxnet.

Regin — вирус-червь, инфицирующий компьютеры под управлением ОС Windows. Этот вирус обнаружен Лабораторией Касперского и Symantec в 2014 г. Первые сообщения об этом вирусе появились весной 2012 г., а самые ранние выявленные экземпляры датируются 2003 г. Статистика заражений вирусом Regin по странам: 28% — в России; 24% — в Саудовской Аравии; по 9% — в Мексике и Ирландии; и по 5% — в Индии, Афганистане, Иране, Бельгии, Австрии и Пакистане. Статистика по объектам заражений: 28% — телекоммуникационные компании; 48% — частные лица и малый бизнес; остальные 24% — компьютеры государственных, энергетических, финансовых и исследовательских компаний. Regin представляет собой вирус-троянец, использующий модульный подход, который позволяет ему загрузить функции, необходимые для учета индивидуальных особенностей заражаемого компьютера или сети. Структура вируса рассчитана на постоянное, долговременное целевое наблюдение за многочисленными объектами. Regin не хранит данные в файловой системе зараженного компьютера, вместо этого он имеет свою собственную зашифрованную виртуальную файловую систему (EVFS), которая выглядит как единый файл. В качестве метода шифрования EVFS использует вариант блочного шифра RC5. Regin осуществляет коммуникации через Интернет с использованием ICMP/Ping, команд, встраиваемых в HTTP cookie и протоколов TCP и UDP, превращая заражаемую сеть в ботнет [325].

Эксперты по уровню сложности и ресурсоемкости разработки сравнивают Regin с вирусом Stuxnet, в связи с чем высказываются мнения, что вирус мог быть создан на государственном уровне в качестве многоцелевого инструмента сбора данных.

Следует отметить, что для вышеперечисленных вирусных программ: Stuxnet, Flame, Duqu, а также других боевых вирусов (Gauss, MiniFlame, MiniDuqu и др.) эксперты отмечают общие высокотехнологические черты, такие как: библиотеки (в том числе open source), среды, используемые уязвимости, приемы противодействия средствам защиты, а также качество кода. Однако среди вирусных средств встречаются и программы другой архитектуры, уровня технологичности и качества реализации. Наглядным примером может быть троянская программа Sputnik, используемая в рамках разведывательной операции Red October.

Sputnik — троянская программа, предназначения для шпионажа. Целевой функцией программы Sputnik является сбор информации, касающейся деятельности дипломатических, правительственных, научных организаций. Максимальное число заражений пришлось на Россию. Особенностями указанной вредоносной программы являются [323]:

- использование известных уязвимостей Windows-приложений (Word, Excel, Outlook) и механизма социальных атак;
- сбор нескольких десятков типов офисных, графических, почтовых, адресных файлов, в том числе удаленных;
- сбор данных со сменных носителей, дистанционных почтовых серверов и мобильных устройств (iPhone, Nokia, Windows Mobile);
- сбор параметров сетевых устройств;
- сложная распределенная система управления (около 60 доменов).

По отношению к Sputnik отмечают следующие его особенности, такие как поддержка кириллицы и сбор файлов, закрытых с помощью Cryptofiler и PGP. Sputnic использует итерационные атаки с участием людей, когда в очередных атаках используются данные, полученные ранее [323].

Несмотря на то, что Sputnik не так технологически изящен, как вирусы класса Stuxnet, указанный вирус встречается с 2007 г. по сей день [323].

Wanna Crypt — сетевой червь, специализирующийся на шифровании пользовательских данных и требовании денег за расшифровку. Данный вирус не использовался как боевое средство, а использовался злоумышленниками. Однако в основу вируса Wanna Cry был положен код вирусного средства, разработанного АНБ США и украденного у него в результате хакерской атаки. Украденный код использовал эксплойт Eternal Blue в Microsoft Windows [427].

Использование в вирусе Wanna Crypt боевого ядра оказалось весьма впечатляющим. Вирус имел просто сверхвысокую скорость распространения. Во время атаки в мае 2017 г. этот вирус заразил более 75 000 компьютеров в 99 странах, заблокировав работу многих организаций. Среди них — организации национальной службы здравоохранения Великобритании, основной железнодорожный оператор Германии компания Deutsche Bahn, телефонные компании Испании и Португалии, а также различные компании из США, Китая, Италии,

Вьетнама, Тайваня. В России в результате атаки вируса Wanna Crypt были дестабилизирована работа телефонных операторов «Йота», «Мегафон», «Билайн», компаний «Сбербанк», «Связной», «РЖД», нарушена работа информационно-управляющих систем МВД, МЧС и Следственного комитета. Большое количество атак этого вируса именно на государственные учреждения России, в том числе на информационные системы ее силовых ведомств позволило некоторым специалистам сделать вывод, что атака Wanna Crypt является проверкой эффективности воздействия вирусных средств против критической информационной инфраструктуры России, которая проводится спецслужбами США под прикрытием некой «хакерской группировки» [427].

Факты применения представленных выше вирусных средств показывают, что противодействие таким программам не связано исключительно с использованием антивирусных средств. Так, в современных вирусных средствах используются технологии которые позволяет им успешно преодолевать средства антивирусной защиты. К таким технологиям относятся [323]:

- наличие программных закладок, главным образом мастер-паролей;
- наличие уязвимостей 0-дня;
- отсутствие своевременного закрытия известных уязвимостей;
- нарушения политики безопасности;
- другие факторы, связанные с недостаточностью традиционных мер защиты.

4.6.5. Проблемные вопросы использования средств информационно-технических воздействий на основе компьютерных вирусов

Необходимо отметить, что использование вирусных средств не только позволяет решать целевые задачи ВС и органам безопасности, но и требует корректности в их конфигурировании и использовании.

Как показано в работе [326], использование вирусного ПО для целей обеспечения государственной безопасности, которое 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.

Так в Германии для проведения оперативно-розыскных мероприятий правоохранительными органами был использован вирус-троян типа backdoor под названием R2D2. Этот вирус был предназначен для прослушивания телефонных разговоров через Skype и перехвата шифрованных SSL-соединений. При этом троян был способен запускать произвольный код на инфицированном компьютере, к тому же в него были встроены средства для наращивания функциональности путем дополнительной установки компонентов через сеть. Например, можно было добавлять компоненты для дистанционного включения через Интернет микрофона и видеокамеры, встроенных в компьютер, и использовать их для непосредственной слежки. Однако, внедряя широкую функцио-

нальность в области оперативно-розыскных мероприятий, разработчики не снабдили данное вирусное средство элементарными функциями собственной информационной безопасности. Так, шифрование передаваемых данных об итогах работы R2D2 происходит лишь в одну сторону — в зашифрованном виде отсылаются лишь снимки экрана и аудиофайлы перехвата; при этом во всех версиях трояна применяется один и тот же ключ, который жестко встроен в код. Команды управления поступают к трояну в отрытом виде. При этом ни управляющие команды для троянца, ни его ответные сигналы совершенно никак не аутентифицированы и не содержат никакой защиты для обеспечения целостности соединения [326].

Эти факты позволили экспертному сообществу продемонстрировать перехват управления сетью вирусов-троянов R2D2. В результате успешного перехвата управления можно либо использовать получаемые от вирусов-троянов данные по своему усмотрению, либо фальсифицировать их с последующей передачей правоохранительным органам. Кроме этого, возможен сценарий, при котором серверные информационные системы правоохранительных органов могут быть атакованы через слабо защищенный служебный канал управления троянами [326].

Кроме вышесказанных собственных уязвимостей, троян R2D2 отличался тем, что существенно снижал уровень информационной безопасности инфицируемой системы, тем самым делая возможным несанкционированный доступ к ее информационным ресурсам со стороны других нарушителей [326].

Еще одним проблемным вопросом при использовании вирусных средств является контроль над профессиональными способами их создания, применения и распространения со стороны государственных служб.

В мае 2017 г. произошла одна из крупнейших мировых атак вирусом Wanna Crypt. Данный вирус продемонстрировал сверхбыструю скорость распространения и высокую результативность поражения пользовательских данных. За 2 недели своего функционирования Wanna Crypt заразил более 75 000 компьютеров в 99 странах, заблокировав работу многих организаций. Отличительной особенностью вируса Wanna Cry является то, что в его основу был положен код вирусного средства, разработанного АНБ США и украденного у него в результате хакерской атаки [427].

Низкая стоимость разработки и наличие большого количества документации по принципам функционирования критической информационной инфраструктуры делают весьма вероятными 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 [328], в настоящее время уже имеются профессиональные платформы для создания вирусных средств, разработка которых финансируется международной организованной преступностью.

Одним из таких вирусных средств является троян CosmicDuke, собранный на платформе BotGenStudio, которая позволяет индивидуально сконфигурировать трояна-шпиона с учетом особенностей цели, против которой ведется

шпионаж, а также выпускать индивидуальное обновление для этого вируса. В зависимости от настроек троян CosmicDuke может использовать различные способы для маскировки в информационной системе, собирать различные наборы данных и отправлять их несколькими способами. Троян CosmicDuk маскируется под легитимные приложения, которые санкционированно обращаются к Интернету: агенты обновления Java, Acrobat, Chrome и др. Троян CosmicDuke способен копировать документы разных типов, следить за клавиатурой, делать снимки экрана, получать доступ к адресным книгам из почтовых приложений и к паролям, сохраненным в системе и популярных мессенджерах, а также к файлам сертификатов безопасности. Собранная информация передается на управляющие серверы несколькими способами: по FTP и тремя вариантами HTTP-взаимодействия. При этом CosmicDuke использует все возможности для продолжения непрерывного функционирования — к примеру, он даже умеет запускаться через планировщик задач операционной системы [328].

Аналитики Лаборатории Касперского полагают, что платформа BotGen-Studio может быть создана не только для нужд разработавшей ее группы, но и для продажи узкому кругу заказчиков [328].

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.

4.7. Программные закладки

4.7.1. Определение и классификация программных закладок

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 [327]. При этом в большинстве случаев закладка внедряется самим разработчиком ПО 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 играют 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 ПО, является то, что они становятся фактически неотделимы от прикладных или системных программ информационной системы [321].

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 разработкой ПО, 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 [321].

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 ПО. В связи с этим средства маскировки программных закладок преимущественно ориентированы на противодействие отладчикам программ, анализаторам кода и дисассемблерам. В качестве одного из широко применяемых способов маскировки является обфускация (запутывание) программ, в которые внедрена закладка [321].

Классификацию программных закладок можно провести по нескольким основаниям (рис. 4.8).

1. По месту внедрения в информационную систему программные закладки классифицируются на [321]:

- *аппаратно-программные закладки*, программно ассоциированные с аппаратными средствами (например, закладки в BIOS);
- *загрузочные закладки*, которые ассоциированы с программами начальной загрузки операционной среды информационной системы;
- *драйверные закладки*, которые ассоциированы с драйверами устройств информационной системы;
- *прикладные закладки*, которые ассоциированы с прикладным программным обеспечением общего назначения;
- *исполняемые модули закладки*, которые содержат только код программной закладки, который в дальнейшем внедряется в пакетные исполняемые файлы;
- *закладки-имитаторы*, имитирующие интерфейс служебных программ, работа с которыми предполагает ввод конфиденциальной информации;

- закладки, маскирующиеся под программы, позволяющие оптимизировать работу персонального компьютера, компьютерные игры и прочие развлекательные программы.

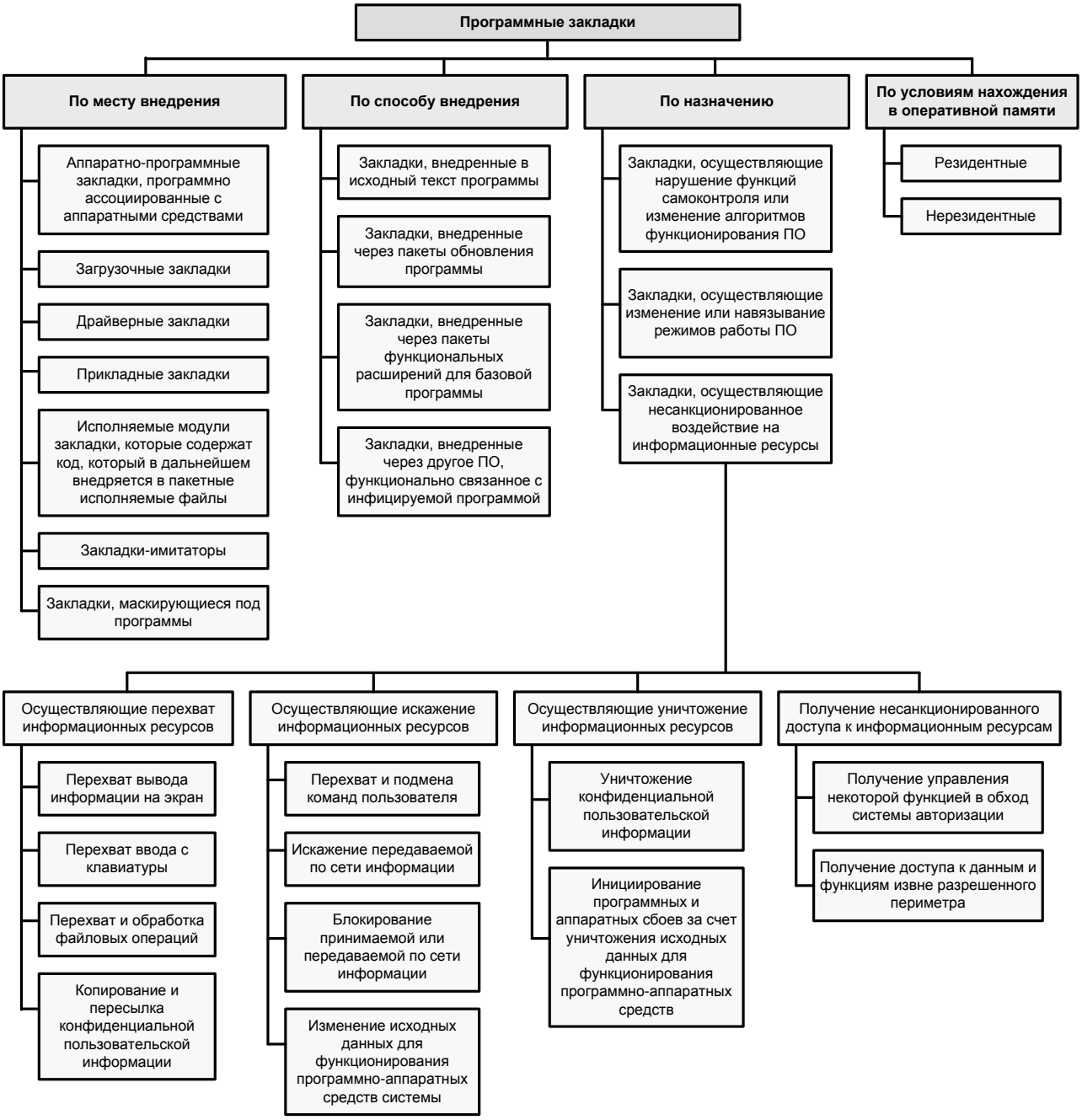


Рис. 4.8. Классификация программных закладок

2. По способу внедрения в программное обеспечение закладки можно классифицировать на:

- закладки, внедренные в исходный текст программы;
- закладки, внедренные через пакеты обновления программы;
- закладки, внедренные через пакеты функциональных расширений для базовой программы;
- закладки, внедренные через другое ПО, функционально связанное с инфицируемой программой;

3. По назначению программные закладки делятся на [321, 329]:

- закладки, осуществляющие несанкционированное воздействие на информационные ресурсы, которые находятся в оперативной памяти, внешней памяти системы либо в памяти другой системы, подключенной по локальной или глобальной сети:
    - закладки, осуществляющие перехват информационных ресурсов:
        - перехват вывода информации на экран;
        - перехват ввода с клавиатуры;
        - перехват и обработка файловых операций;
        - копирование и пересылка конфиденциальной пользовательской информации;
    - закладки, осуществляющие искажение информационных ресурсов:
        - перехват и подмена команд пользователя;
        - искажение передаваемой по сети информации;
        - блокирование принимаемой или передаваемой по сети информации;
        - изменение исходных данных для функционирования программно-аппаратных средств системы;
    - закладки, осуществляющие уничтожение информационных ресурсов:
        - уничтожение конфиденциальной пользовательской информации;
        - инициирование программных и аппаратных сбоев за счет уничтожения исходных данных для функционирования программно-аппаратных средств;
    - получение несанкционированного доступа к информационным ресурсам:
        - получение управления некоторой функцией в обход системы авторизации;
        - получение доступа к данным и функциям извне разрешенного периметра;
- закладки, осуществляющие нарушение функций самоконтроля или изменение алгоритмов функционирования системных, прикладных и служебных программ;
- закладки, осуществляющие изменение или навязывание режимов работы ПО.

Для того чтобы программная закладка начала функционировать, необходимо одновременное соблюдение двух условий, заставляющих систему исполнять команды, входящие в код программной закладки [321]:

- программная закладка должна попасть в оперативную память системы;
- должен быть выполнен ряд активизирующих условий, зависящих от типа программной закладки.

4. По условиям нахождения в оперативной памяти информационной системы программные закладки классифицируются следующим образом [321]:

- резидентные закладки, постоянно находящиеся в оперативной памяти до перезагрузки или завершения функционирования информационной системы;
- нерезидентные закладки, выгружающиеся из оперативной памяти информационной системы по истечении определенного времени либо при выполнении определенных условий.

4.7.2. Примеры средств информационно-технических воздействий на основе программных закладок

Подавляющая часть программных закладок устанавливается самими производителями ПО 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, становятся 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) официальных должностных лиц.

Как показано в работе [345], по итогам сертификации в России иностранного ПО, в нём 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 ПО являются именно такими.

Рассмотрим отдельные случаи использования закладок в ПО, широко используемого в органах военного и государственного управления.

Браузеры Internet Explorer, Chrome и Firefox, широко используемые для просмотра Интеренет-страниц, содержат программные закладки, которые реализуют скрытые функции по информированию производителя о поисковых запросах пользователя, посещаемых им адресов, интенсивности использования браузера, аппаратном и ПО компьютера, а также некоторый персональный код, по которому производитель способен идентифицировать каждую конкретную копию браузера. Причем функции скрытой передачи этих данных не отключаются средствами настройки браузеров и могут быть заблокированы только за счет использования сторонних средств защиты [330].

В смартфонах под управлением Windows Mobile используется программная закладка, позволяющая прослушивать смартфон специалистам АНБ. Скрытое прослушивание достигается путем получения удаленного административного доступа к операционной системе смартфона через TCP-порты с 1024 по 1030. Чаще всего это происходит при обращении машин к серверам Microsoft Update. При этом компания Cryptome, нашедшая данную закладку, публикует список подозрительных IP-адресов, через которые идет подобное «прослуши-

вание» и которые принадлежат либо самому агентству АНБ, либо дружественным ему компаниям и спецслужбам других стран [334].

Компания Microsoft ведет довольно агрессивную политику по несанкционированному скрытому сбору данных пользователей операционных систем Windows. При этом компания сотрудничает со специальными службами США в области предоставления последним несанкционированно собранной информации. С учетом того, что в настоящее время операционная система Windows установлена на около 90% персональных компьютеров и рабочих станций, это предоставляет фактически неограниченные возможности по ведению персонального и промышленного шпионажа.

К последним инцидентам информационной безопасности, связанным с компанией Microsoft, относится резонанс, связанный с выяснением наличия широких скрытых функций по несанкционированному сбору данных, в операционных системах Windows 10, Windows 7 и Windows 8. При этом если для Windows 10 эти скрытые функции были изначально встроены в систему, то для операционных систем Windows 7 и Windows 8 были выпущены обновления (KB3068708, KB3022345, KB30752), которые содержат программные закладки с аналогичной скрытой функциональностью [335].

Операционная система Windows 10 включает в себя широкие функции синхронизации пользовательских данных, автоматического обновления, фоновой установки приложений и взаимодействия с облачными сервисами компании Microsoft. Однако вместе с этими штатными функциями Windows 10 реализует недекларируемые возможности в части мониторинга действий пользователя и несанкционированного сбора пользовательской информации. Windows 10 собирает и отсылает на сервера Microsoft данные телеметрии (информацию об установленных и запущенных программах, объеме занятой памяти, журналы ПО, фрагменты оперативной памяти и т. д.), отслеживает поисковые запросы пользователя и анализирует почтовую переписку, анализирует названия файлов на компьютерах пользователей. После первой активации Windows 10 на короткий промежуток времени включается веб-камера, после чего на сервера компании Microsoft передается 35 Мб мультимедийных данных. Кроме того, встроенное приложение «голосовой помощник Cortana» отправляет все голосовые запросы пользователей на многочисленные сервера Microsoft. При этом приложение продолжает работать в фоновом режиме, даже если его отключить, а принудительная блокировка Интернет-соединений данного приложения вызывает ошибку в его работе [335].

До этого Microsoft была уличена в создании недокументированных возможностей для АНБ и ФБР по доступу к шифрованным данным, зашифрованным встроенным ПО BitLocker [336].

Производители других закрытых операционных систем, например, таких как iOS для iPhone, также широко используют программные закладки, реализующие недекларируемые возможности по несанкционированному мониторингу действий пользователя и сбора его данных.

Помимо производителей, в ряде случаев разработчиком программных закладок могут выступать и заинтересованные государственные службы.

Так, после обнародования данных [337] о закладках, разработанных и использующихся АНБ, выяснилось, что значительная часть оборудования, а именно коммутаторы и аппаратные брандмауэры производителей Cisco, Juniper, Huawei, сервера производства Dell и Hewlett-Packard, а также SIM-карты, используемые в сетях GSM, имеют программные закладки, предоставляющие недекларируемые возможности и несанкционированный доступ для американских спецслужб. Интересно отметить, что отдельные экземпляры этого оборудования (или их близкие аналоги) были неоднократно сертифицированы ФСТЭК России по 3 классу защищенности, что позволяло использовать их при передаче данных, содержащих гостайну. Все обнародованные программные закладки были реализованы путем внедрения кода на самый нижний уровень управления — 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 [341].

Необходимо отметить, что в настоящее время подавляющее число закладок предназначено для шпионажа в пользу производителей ПО, а также сотрудничающим с ними службам государственной безопасности. Однако в ближайшее время направление развития программных закладок может измениться. Подобные закладки смогут применяться как для активного воздействия на пользователя, так и на управляемые программами технологические процессы. Например, за счет закладок можно реализовать средства психологического воздействия на пользователей информационной системы.

4.8. Аппаратные закладки

4.8.1. Определение и классификация аппаратных закладок

Аппаратная закладка — устройство в электронной схеме, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу аппаратных средств информационной системы. Результатом 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 [339].

Также аппаратной закладкой может называться отдельная микросхема, несанкционированно подключаемая к атакуемой системе для достижения тех же целей [339].

Аппаратные закладки можно классифицировать по различным основаниям, следующим образом (рис. 4.9) [340].

1. По типу:
   - функциональная — закладка производится путем изменения состава аппаратных средств, добавлением или удалением необходимых элементов (например, транзисторов или логических вентилей в микросхеме);
   - параметрическая — закладка производится путем использования уже существующих компонентов аппаратного средства.

2. По расположению закладки:
   - в виде элементов микросхемы;
   - в отдельной микросхеме;
   - на электронной плате;
   - в аппаратных средствах информационной системы;
   - пространственно-распределенная по нескольким аппаратным средствам.
3. По объему — характеризует количество измененных, добавленных или удаленных элементов аппаратных средств, необходимых для внедрения закладки.
4. По месту нахождения закладки относительно ассоциированной информационной системы:
   - в аппаратных средствах информационной системы;
   - в другом месте.

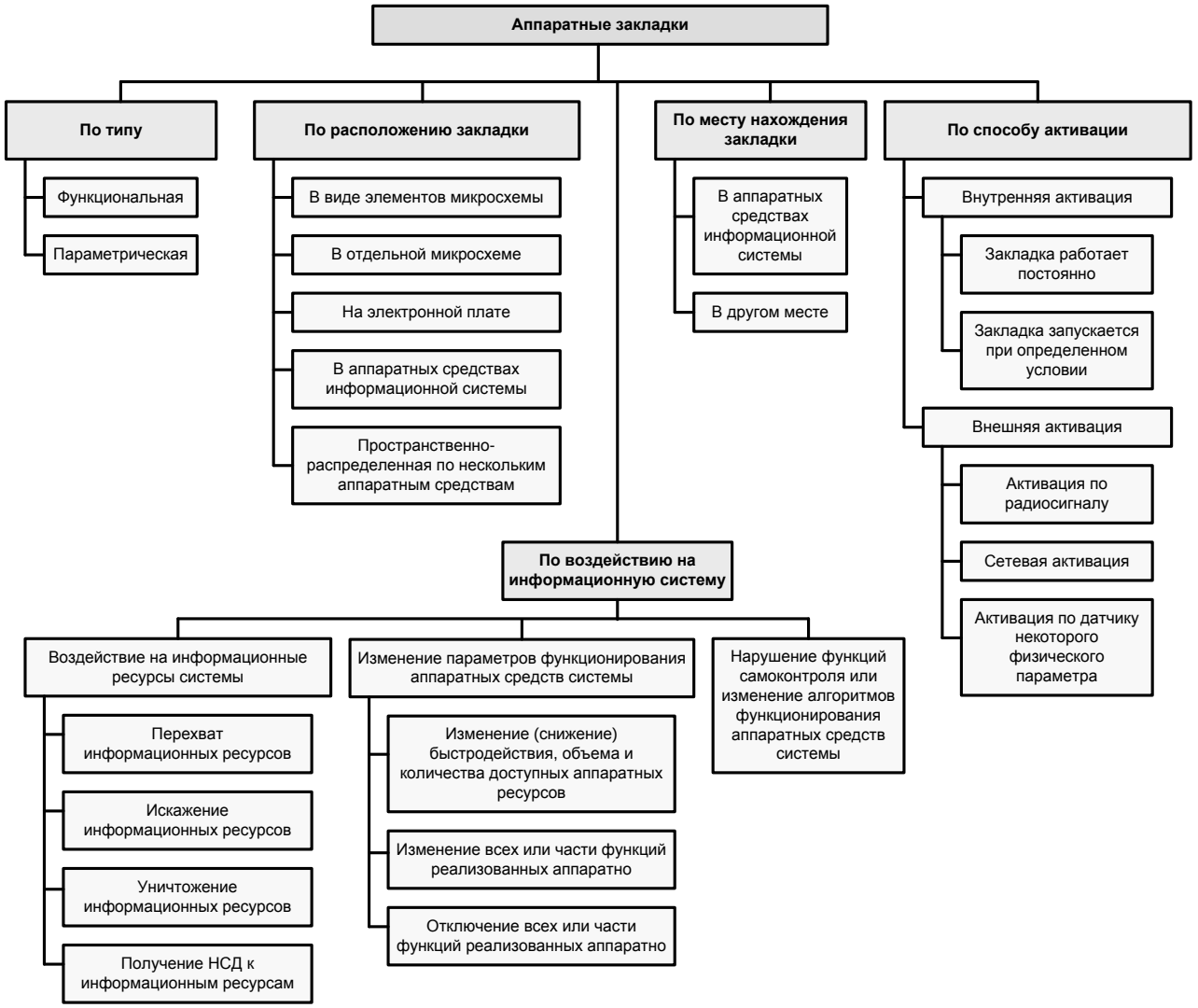


Рис. 4.9. Классификация аппаратных закладок

5. По способу активации:
   - внутренняя активация:
     - закладка работает постоянно в составе аппаратного средства;
     - закладка запускается при определенном условии, заложенном при ее разработке;
   - внешняя активация — для запуска закладки используется внешний сигнал, который принимается антенной или датчиком:
     - активация по радиосигналу;
     - сетевая активация;
     - активация по датчику некоторого физического параметра.
6. По воздействию на информационную систему:
   - воздействие на информационные ресурсы системы:
     - перехват информационных ресурсов;
     - искажение информационных ресурсов;
     - уничтожение информационных ресурсов;
     - получение несанкционированного доступа к информационным ресурсам;
   - нарушение функций самоконтроля или изменение алгоритмов функционирования аппаратных средств системы;
   - изменение параметров функционирования аппаратных средств системы:
     - изменение (снижение) быстродействия, объема и количества доступных аппаратных ресурсов;
     - изменение всех или только некоторых функций, реализованных аппаратно;
     - отключение всех или только некоторых функций, реализованных аппаратно.

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 [343]:

- 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.

Краткая характеристика технологий современных аппаратных закладок представлена в таблице 4.1 [343].

Таблица 4.1— Технологии современных аппаратных закладок [343]

Методы внедрения	**Методы обнаружения**	**Методы маскировки**
Встраивание закладок в технологию микроядра управления в современных СБИС, построенного на уникальном списке команд (управление основной работой и блокировка и замена неисправных узлов для продления срока службы СБИС)	Технологии послойного сканирования кристаллов	Механизм технологической защиты топологии кристалла от послойного сканирования (впервые внедрен в i486)
	Вычитывание и дизассемблирование аппаратно доступных микрокодов	Размещение микроядер с закладками и ресурсов памяти в области, недоступной пользователю. Шифрование (мутирование) участков кода, антитрассировка
Виртуализация вычислений	Анализ контента проходящих по сети данных	
Встраивание целевых микроядер и узлов, реализующих стратегию влияния	Мониторинг аномальной активности платформы. Радио-мониторинг. Электромагнитный контроль	

4.8.2. Примеры средств информационно-технических воздействий на основе аппаратных закладок

Рассмотрим отельные примеры реализации и использования аппаратных закладок при проведении информационных операций.

Образцом использования аппаратных закладок является обнародованная Э. Сноуденом информация о закладках АНБ [337, 341, 342], использующихся для несанкционированного сбора данных в интересах разведывательных служб США. Практически все закладки были 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 [341].

АНБ использовало аппаратные закладки для USB- и LAN-кабелей (перехватывают данные), VGA-кабелей (позволяют перехватывать видеосигнал, идущий с ПК на монитор), закладки для компьютеров и прочих вычислительных систем, системы имитации базовых станций сотовой связи и модифицированные телефоны Samsung и других производителей с интегрированной системой прослушки. Интересной особенностью аппаратных закладок АНБ являются функциональное взаимодополнение и возможность совместного использования различных закладок [337, 341, 342].

Другим ярким примером использования аппаратной закладки в военном конфликте является факт отключения системы иракской ПВО в военном конфликте 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 [321].

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 ВС России вычислительной техники, которая фактически произведена иностранным изготовителем, снабжена разнообразными аппаратными закладками (например, одновременно в BIOS-е и сетевой карте компьютера), однако которая, пройдя перемаркировку и установку отечественного ПО, 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 [344].

4.8. Нейтрализаторы тестовых программ и программ анализа кода

Одним из способов противодействия угрозам программных закладок является проверка программ, используемых в информационных системах управления критической инфраструктуры в процессе сертификационных испытаний и тематических исследований по требованиям безопасности [345, 346].

Сертификационные испытания и тематические исследования проводятся путем [345, 349]:

- функционального тестирования ПО на соответствие нормативным и методическим документам или документации;
- структурного (статического и динамического) анализа ПО на отсутствие недекларированных возможностей.

Особенностями указанных подходов является следующее.

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. [345, 346]

При структурном анализе проводится главным образом проверка полноты/избыточности кода. Проводится 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 [345].

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.

При отсутствии исходных текстов программ применяются подходы реверс-инжиниринга и функциональные методы (по принципу «черного ящика»).

Реверс-инжиниринг может проводиться путем [345]:

- ретрансляции/дизассемблирования, прогона в отладочном режиме — для машинных и процедурных языков;
- высококачественной декомпиляцией — для языков с промежуточным кодом.

Примеры отдельных способов тестирования представлены в таблице 4.2 [345].

Таблица 4.2— Способы тестирования программного обеспечения [345]

Способ тестирования	**Основные выявляемые дефекты и уязвимости**
Функциональное тестирование	Дефекты реализации функций и ошибки документации
Фаззинг-тестирование	Дефекты реализации интерфейсов данных
Граничное тестирование	Ошибки граничных условий
Нагрузочное тестирование	Ошибки производительности
Стресс-тестпрование	Отказ в обслуживании
Профилирование	Недостатки оптимизации кода
Статический семантический анализ (прикладная верификация)	Некорректности кодирования
Статический сигнатурный анализ	Заданные потенциально опасные фрагменты
Статический анализ отсутствия недекларируемых возможностей	«Мертвый код»
Динамический анализ отсутствия недекларируемых возможностей	«Мертвый код»
Мониторинг операционных процессов	Нарушения целостности процессов и ресурсов
Тестирование конфигураций	Ошибки администрирования
Сканирование уязвимостей	Известные опубликованные уязвимости
Тест на проникновение	Известные уязвимости, ошибки конфигурирования
Регрессионное тестирование	Повторные ошибки прошлых версий

При этом все методы тестирования, представленные в таблице 4.2, имеют ограничения по использованию [345]:

- функциональные методы ограничены размерностью входных данных, неэффективны при выявлении программных закладок и пригодны только для небольших продуктов;
- структурные статические методы, кроме наличия исходных текстов, имеют ограничения на выявление дефектов, связанных с динамикой программы (циклами и т. д.);
- дизассемблирование — реально можно провести только для небольших незащищенных программ;
- ручные экспертные методы — предъявляют высокие требования к опыту и знаниям тестировщиков.

Сложность и размер современных программ таковы, 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 используются 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. 4.10) [347–349]:

- обфускация (запутывание) кода;
- упаковка и шифрование кода;
- определение факта применения тестовых программ и противодействие отладке;
- полиморфизм (самомодифицирующийся код).

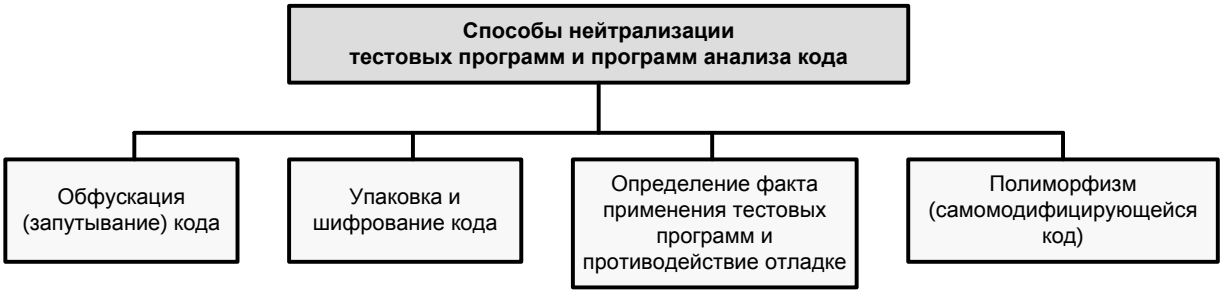


Рис. 4.10. Классификация способов нейтрализации программ

Рассмотрим данные способы более подробно.

Обфускация кода — приведение исходного текста или исполняемого кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ и понимание алгоритмов работы, а также модификацию при декомпиляции. Обфускация может осуществляться на различных уровнях: уровне алгоритма, уровне исходного текста, уровне машинного кода (ассемблерного текста). Кроме того, выделяют обфускацию на уровне виртуальных машин. Для создания запутанного машинного кода могут использоваться специализированные компиляторы, использующие неочевидные или недокументированные возможности среды исполнения программы. Существуют также специальные программы, производящие обфускацию, называемые обфускаторами [349].

Недостатками обфускации кода являются:

- код после обфускации может стать более зависимым от используемой платформы или компилятора;
- после обфускации дальнейшая отладка и тестирование программного кода становятся невозможны;
- обфускация обеспечивает скрытие программных закладок через неясность программного кода, однако ни один из существующих обфускаторов не гарантирует устойчивости к определенному уровню сложности декомпиляции и не обеспечивает безопасности на уровне современных криптографических схем.

Упаковка и шифрование участков кода. При этом способе в ПО встраиваются код шифратора и генератор ключей, после чего программа в процессе работы «на лету» дешифрирует инструкции машинного кода и передает

их на исполнение. Использование такого способа противодействия тестовым программам позволяет существенно сузить их возможности по тестированию. Данный подход делает невозможным непосредственное дизассемблирование кода программы. Помимо этого, сохранение дампов памяти для последующего дизассемблирования становится крайне неэффективным, т. к. каждый дамп содержит только небольшой расшифрованный фрагмент программы [349].

Определение факта применения тестовых программ и противодействие отладке. Существует ряд приемов, позволяющих обнаружить выполнение тестирования и отладки. В случае обнаружения этого факта со стороны программы предпринимаются действия, направленные на противодействие исследованию за счет изменения логики своего функционирования:

- меняется работа алгоритмов;
- блокируется исполнение кода программы;
- преднамеренно искажаются данные отладчика.

Такие способы противодействия отладке преодолеваются применением потактовых симуляторов. В этом случае обнаружение отладки возможно только из-за ошибок в симуляторе, приводящих к отличному от аппаратной платформы поведению [349].

Полиморфизм — генерация различных версий машинного кода для одного и того же алгоритма. Технология полиморфной генерации машинного кода позволяет проводить запутывающие преобразования защищаемого ПО. Для этого производятся встраивание дополнительных или незначащих инструкций в защищаемый код, перестановка последовательности выполнения инструкций. Как правило, на этапе компиляции в ПО добавляется полиморфный генератор, который в процессе функционирования программы проводит модификацию ее машинного кода [347]:

- перестановка, обмен местами инструкций, порядок следования которых неважен;
- добавление «мусорных команд»;
- введение незначащих переменных;
- изменение процедуры самомодифицирования и др.

4.9. 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 [350].

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 [350].

В связи с этим в настоящее время актуальным становится применение «стратегии обмана» или отвлечения атаки информационным оружием на ложный информационный ресурс. Как показали исследования [351], 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 (рис. 4.11):

- ложные объекты и ресурсы в семантической части информационного пространства (например, дезинформация или заведомо ложная информация, размещаемая в СМИ или в сети Интернет);
- ложные объекты и ресурсы в телекоммуникационной части информационного пространства (например, ложные сети, узлы, БД и т. д.).

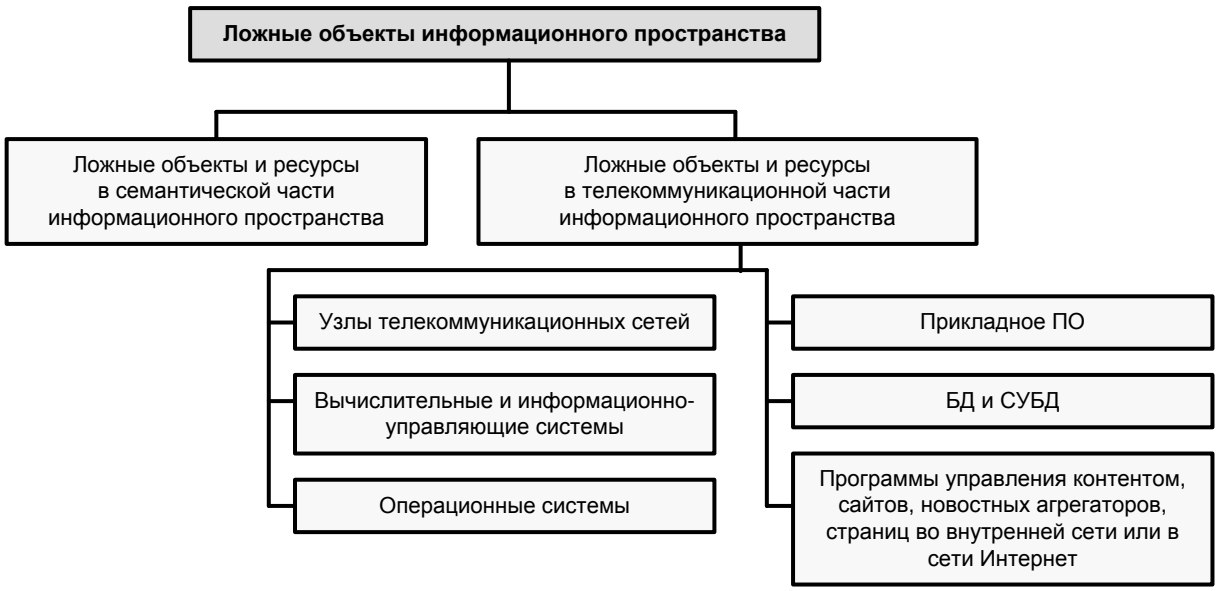


Рис. 4.11. Классификация ложных объектов информационного пространства

Ложные объекты и ресурсы, размещаемые в семантической части информационного пространства, ориентированы на ведение информацион-

ного 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 ПО;
- базы данных и системы управления ими;
- программы управления контентом сайтов, новостных агрегаторов, страниц во внутренней сети или в сети Интернет.

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 [350].

4.10. Средства моделирования боевых действий

4.10.1. Общие сведения о средствах моделирования боевых действий

Анализ вооруженных конфликтов свидетельствует о том, что успех сопутствует стороне, проявляющей большую активность и инициативу, эффективно управляющей подчиненными силами и средствами. 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 [352].

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 обеспечит подавляющее асимметричное информационное превосходство над противником при условии отсут-

ствия у него подобных средств. При противоборстве двух сторон, обладающих подобными средствами, может создаться ситуация, что 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, позволяют 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. 60-е годы характеризуются активизацией работ в этой области. Развиваются преимущественно модели боевых действий тактического уровня, материально-технического обеспечения, использования стратегических ядерных сил и стратегического развертывания ВС. Появляется первое поколение моделей стратегических операций разнородных группировок ВС на ТВД. Расширяется сфера их применения: НИОКР, учения, командно-штабные игры. В 70-е гг. моделирование становится обязательным инструментом военных исследований. Широкое развитие получают имитационные модели, которые находят применение в военном планировании. В 80-е гг. модели становятся повседневным рабочим инструментом в военном планировании, в непосредственном обеспечении деятельности руководства МО и видов ВС. Унифицируется информационное обеспечение моделей (базы данных). Проектируются иерархические системы моделей боевых действий различного уровня. Всё более широкое распространение получает использование моделей в АСУ военного назначения. В ходе учений АСЕ-89 в Германии впервые реально была задействована система, объединившая модели различных уровней DWS (Distributed Wargaming System). 90-е годы характеризуются еще более масштабными проектами 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 со 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 [354].

С начала 2000-х гг. Пентагон при формировании военно-технической политики включил средства имитации и моделирования боевых действий в

число приоритетных технологий. С начала 2000-х гг. 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 обозначила огромный прорыв США в области разработки моделей и имитационных систем [353, 354].

В настоящее время в МО США действует классификация, определяющая назначение модели, объекты и процессы, а также метод моделирования (рис. 4.12) [354].

По назначению американские специалисты выделяют три группы моделей [354]:

- используемые в целях анализа и оценки (обеспечение оперативной работы);
- применяемые в сфере создания ВВТ;
- предназначенные для обучения личного состава, обеспечения боевой подготовки войск и штабов.

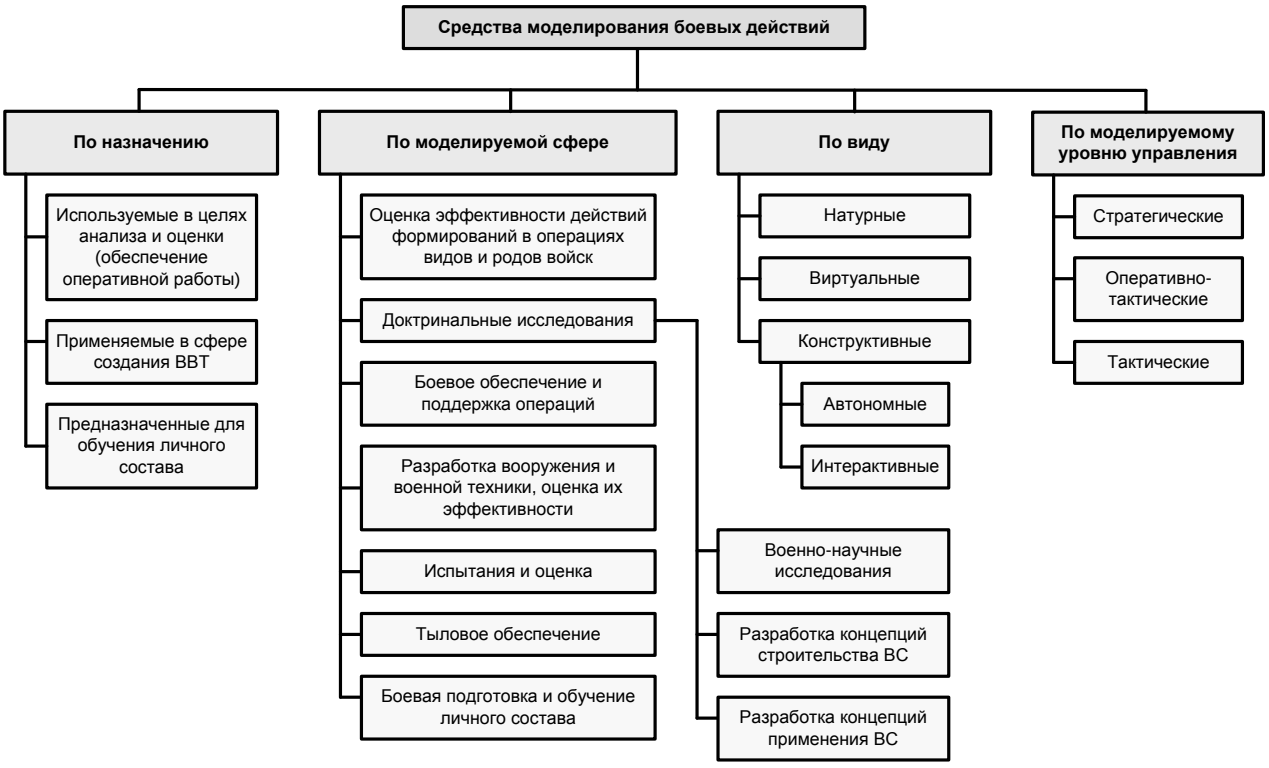


Рис. 4.12. Классификация средств моделирования боевых действий

В последнее время в ряде официальных документов военного ведомства предлагается более подробное подразделение моделей с выделением семи функциональных сфер моделирования [354]:

1. оценка эффективности действий формирований в самостоятельных, совместных и объединенных операциях видов и родов сил;

2. доктринальные исследования (военно-научные исследования и разработка концепций в области строительства ВС и их боевого применения);
3. боевое обеспечение или поддержка операций (разведка, РЭБ и др.);
4. создание ВВТ (снижение стоимости новых образцов и сокращение времени их создания, включая сферу НИОКР и закупок);
5. испытания и оценка (потребностей ВС, повышение качества принимаемых решений в сфере планирования и разработки бюджетных программ, оценка эффективности новых образцов ВВТ);
6. тыловое обеспечение;
7. 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 основные их вида, подчеркивая различие в степени и характере участия человека в процессе моделирования [354]:

- 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 использование других видов моделирования и имитации, особенно это касается виртуальных систем [354].

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 [354].

Конструктивные системы могут быть [354]:

- полностью автономными (процесс моделирования не требует участия человека),
- интерактивными человеко-машинными системами.

Большинство используемых моделей являются именно конструктивными. Здесь предметная область, характерные для нее объекты и процессы представляются с помощью математического (алгоритмического) описания и соответствующего ПО. Термин применяется главным образом, чтобы подчеркнуть отличие этого класса моделей от натурных и так называемых виртуальных моделей.

К конструктивным системам относятся разного рода имитационные модели [354].

Архитектура современных систем моделирования боевых действий стандартизирована. Она включает библиотеки стандартных программных модулей — генерирования случайных чисел, форматирования специфических докладов, выполнения сложных математических вычислений, управления ходом моделирования и др. [354].

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 [354].

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% [354].

Важным направлением деятельности МО США в сфере военного моделирования являются 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 [354].

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., требуют разработки таких моделей, в которых был бы отражен значительно расширившийся спектр возможного применения ВС. Требуются новые или уточненные модели для использования в следующих предметных областях: системы управления и связи; вычислительные системы и разведка; применение систем ПРО; радиоэлектронная борьба; применение оружия нелетального воздействия; роботизированные комплексы и системы;

специальные операции; миротворческие операции; борьба с терроризмом и наркобизнесом и другие [354].

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 [354].

Перспективы развития моделирования связываются с развитием таких ключевых направлений развития науки и технологий, как: высокопроизводительные вычисления; компьютерные сети; визуализация; системы виртуальной реальности; распределенные системы моделирования. Благодаря программе МО США по высокопроизводительным вычислениям ресурсы суперкомпьютеров становятся всё более доступными для имитации через облачные вычислительные ресурсы [354].

В целом необходимо отметить, что развитие систем моделирования и имитации в США рассматривается как один из основных факторов обеспечения эффективности строительства и применения ВС. Громадный потенциал, накопленный в данной области, уже сейчас оценивается как значительно опережающий возможности других стран мира в этой сфере [353].

В перспективе ожидается дальнейшее глобальное комплексирование моделей и внедрение систем виртуальной реальности (искусственного многомерного боевого пространства) на базе информационно-вычислительных 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 ВС 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 [353].

Более подробная информация о подходах к моделированию боевых действий представлена в работе [358]. Примеры средств моделирования боевых действий применяемых в США в настоящее время, — в работах [353–357]. Кроме того, в работе [352] рассмотрен вариант подобного комплекса, разработанного специалистами республики Беларусь.

4.10.2. Примеры средств моделирования боевых действий

4.10.2.1. Система JWARS

Объединенная система моделирования боевых действий JWARS (Joint Warfare System) — система моделирования ведения военных операций объединенными группировками войск для ВС США. Она позволяет моделиро-

вать наземные, воздушные, морские операции и боевые действия, действия сил специальных и информационных операций, защиту/применение химического оружия, действия систем ПРО/ПВО на ТВД, управления и космической разведки, связи, тылового обеспечения [353].

JWARS — это современная конструктивная система моделирования, разработанная с использованием CASE-средств на языке программирования Smalltalk. Она использует событийное моделирование и имитирует деятельность и взаимодействие военных подразделений. В рамках этой системы достаточно глубоко проработаны вопросы создания трехмерного виртуального боевого пространства, учета погодных условий и особенностей рельефа местности, тылового обеспечения боевых действий, создания четкой системы информационных потоков, а также вопросы поддержки принятия решений в системе управления и контроля [353].

Основным назначением JWARS является моделирование боевых действий объединенных оперативных формирований (ООФ), что должно повысить качество объединенного оперативного планирования и применения ВС, оценки боевых возможностей объединенных формирований и разработки концептуальных документов строительства ВС в целом. Система позволяет осуществлять комплексный контроль процесса оперативного планирования и исполнения, а также многократную отработку выполнения одних и тех же задач, что существенно повышает возможности анализа результатов проводимых действий и выбора наиболее эффективного сценария применения сил и средств [353].

Возможности JWARS [353]:

- позволяет планировать военные операции продолжительностью более 100 дней;
- временной масштаб моделирования — 1:1000 (в 1000 раз быстрее, чем реальное время);
- время инициализации модели — до 3 мин.

Последняя версия JWARS отличается: наличием модульной системы моделирования сети межтеатровых воинских перевозок; усовершенствованным блоком моделирования системы управления ООФ; возможностью моделирования ударов по мобильным целям; наличием геоинформационной и геофизической баз данных по Юго-Восточной Азии, Дальнему Востоку, Южной Азии и Южной Америке; возросшим быстродействием вследствие модернизации программного кода и внедрения новой технической базы; возможности конструирования сценария и др. [353].

Моделирование применения оружия массового поражения в настоящее время охватывает имитацию защиты от химического оружия и оценку его воздействия на боевые подразделения и окружающую среду. В ближайшей перспективе планируется создание блоков моделирования оценки применения биологического и ядерного оружия [353].

Модель действий ВВС в JWARS поддерживает решение около 20 видов типовых задач. В системе формализованы и моделируются процессы: непосредственной авиационной поддержки, применения крылатых ракет, нанесения массированных ракетно-авиационных ударов; обеспечения ПВО районов

боевых действий; уничтожения наземных/воздушных/морских целей; подавления системы ПВО противника; массированного применения БПЛА; целеуказание и наведение при временных ограничениях; постановка мин с воздушных носителей, дозаправка в воздухе и т. д. [353].

Модель действий ВМС в JWARS отражает процессы: поражения надводных целей, применения подводных лодок против надводных сил; морской блокады; противолодочной обороны (воздушными, подводными и надводными средствами); минной войны на море; поддержки наземных сил корабельной артиллерией; проведения морских десантных операций и др. [353].

Модель действий ПРО/ПВО на ТВД в JWARS базируется на оценке действий системы Patriot, Aegis, лазерного оружия воздушного базирования. Имитируются ракетная угроза и функционирование интегрированной системы ПРО на ТВД [353].

Моделирование систем управления, связи, компьютерного обеспечения, разведки и наблюдения (C4ISR) в JWARS основывается на: ситуационной цифровой карте обстановки; имитации информационных потоков на поле боя; сборе и агрегации информации об обстановке с распознаванием целей; постановке задач средствам обнаружения, в том числе космическим, и др. [353].

Процесс принятия решений в JWARS основан на базе знаний по тактическим нормативам, а также на предпочтениях лиц, принимающих решения [353].

Система JWARS также позволяет моделировать работу средств РЭБ, оценивать процессы восстановления системы управления после воздействия противника. При моделировании в JWARS информационных операций имитируется прямое воздействие на системы связи, обнаружения и обработки информации противника. В настоящее время в JWARS невозможна оценка последствий динамического ввода информационных вирусов либо искажения информации в компьютерах или информационных потоках противника, а также отсутствует возможность вскрытия мер по введению в заблуждение (планируется реализовать в последующих версиях) [353].

Моделирование функционирования космических сил и средств учитывает планируемую модернизацию (перспективный облик) сил и средств, процессы контроля космического пространства, имитацию противокосмических операций и информационной войны [353].

Тыловое обеспечение моделируется с учетом автономности, планирования перевозок сил и средств воздушным, железнодорожным, автомобильным, морским и трубопроводным транспортом, обеспечения со стороны союзников и др. [353].

Примерами задач, решавшихся с помощью JWARS в условиях сетецентрических военных действий, являются оценка эффективности [353]:

- защиты критически важных объектов (территория США, базы, группировки ВС на ТВД, силы и объекты союзников и др.);
- нейтрализации оружия массового поражения и средств его доставки;
- защиты информационных систем;
- мер по противодействию противнику посредством непрерывного наблюдения, слежения, массированного воздействия высокоточными

воздушными и наземными средствами по критически важным стационарным и мобильным целям;
- новых информационных технологий и инновационных концепций для разработки архитектуры «объединенной» системы управления и системы единой карты оперативной обстановки и др.

В JWARS учитываются особенности, характерные для условий сетецентрических военных действий [353]:
- возможность динамически в интерактивном режиме реагировать на происходящие события исходя из восприятия ситуации каждой стороной на базе анализа оперативной обстановки;
- создание основы для принятия решения с использованием аналитической оценки сложившейся ситуации;
- осуществление высокой степени координации/синхронизации действий командующего ООФ с действиями подчиненных командиров во всех звеньях руководства;
- интеграция разведывательной информации для приятия решений;
- моделирование поведения «центров силы» (по терминологии Дж. Вардена) как военных, так и экономических — в отношении состояния ВПК противника;
- оценка реализации конечной цели военной операции, например в виде изменения политики руководства государства;
- описание агрегированных критериев достижения победы (географических — отсутствие подразделений противника на определенной территории; желаемого соотношения сил — избежание потерь своих сил и союзников; нанесение поражения противнику в течение определенного времени);
- определение степени достижения целей военной операции.

При этом более ранние версии системы JWARS позволяли учитывать такие факторы, как уровень подготовки личного состава и его морально-психологическое состояние. В результате имелись возможности по созданию подразделений разного уровня боеспособности, с различными личными качествами командиров, такими как склонность к авантюризму, обеспокоенность некачественным решением поставленной боевой задачи и др. Эти характеристики дают определенную гибкость при создании стратегии поведения тех или иных подразделений. В последних версиях JWARS была установлена жесткая иерархия командной линии постановки задач, которая позволила в целом имитировать реальную оценку выполнения задач подчиненными подразделениями и вырабатывать оптимальные варианты их боевого применения. Другими словами, вышестоящие инстанции ставят боевую задачу и вводят ограничения для ее решения [353].

Технологически JWARS является интеллектуальной информационной системой, основанной на продукционной экспертной системе с выводом на основе решающих правил «если.., то.., иначе...». Обновление базы знаний (значений фактов, правил) о противнике осуществляется в результате информационного процесса разведки. База знаний содержит также информацию о своих си-

лах, результатах оценки обстановки, в том числе противником. Она предоставляет пользователям автоматически генерируемые решения, в которые можно вносить свои коррективы в интерактивном режиме. Решающие правила базы знаний являются ключевыми для динамического функционирования модели. В результате срабатывания правила каждому факту могут быть назначены одно или несколько действий. Действия выполняются, когда значение вычисленного факта становится равным определенной пороговой величине и производит изменения в состоянии базы данных. Срабатывание правил также в автоматическом режиме генерирует запросы к системе разведки, которая выдает ответы на эти запросы. Работа правил определяет динамику поведения модели во времени. Генерируемые системой разведки ответы оцениваются критерием сатисфакции (степени удовлетворения запроса). В случае низкого значения коэффициента удовлетворения запрос переформулируется с учетом взаимозависимости между запросами и состоянием оперативной обстановки [353].

При оценке оперативной обстановки в JWARS используется цифровая географическая карта с нанесенной сеткой координат. Для каждой ячейки координатной сетки, соответствующей участку суши, рассчитывается значение показателя, характеризующего степень контроля ситуации своих сил и противника, на базе вычисления «силы влияния» по определенной методике. В результате каждая ячейка окрашивается в синий или красный цвет [353].

Модель процессов обнаружения и классификации объектов (целей) носит стохастический характер, зависящий от действий сил противника, видимости, степени радиоэлектронного противодействия, характера местности. На основе рассчитанных вероятностей определяется количество обнаруживаемых сил и средств противника из реально присутствующих, затем моделируется вероятностный процесс распознавания/классификации целей, в результате чего они соотносятся, например, либо с конкретным типом образца ВВТ, либо лишь с определенным классом образцов. Затем формируется итоговый доклад работы средства обнаружения [353].

Процесс ассоциации и корреляции результатов работы различных разведывательных средств в условиях единого информационного пространства заключается в следующем. Результаты обнаружения каждого средства разведки наносятся на ситуационную карту. Экстраполируются позиции каждого из ранее обнаруженных объектов во времени к моменту поступления новых докладов о результатах работы средств разведки. На основе расчета расположения «центра масс» ранее обнаруженных объектов производится отбор вероятных кандидатов для ассоциации с объектами, информация о которых содержится во вновь поступивших докладах о результатах работы средств разведки. Вычисляется вероятностная величина ассоциации объектов. На базе относительной величины вероятности ассоциации определяется, является ли объект вновь обнаруженным из ранее известных или новым объектом, обнаруженным впервые [353].

Программно система JWARS состоит из трех модулей: функционального, имитационного и системного, которые объединены в единый комплекс. Функциональный модуль содержит прикладное программное обеспечение, позво-

ляющее моделировать боевые функциональные возможности. Специальное программное обеспечение имитационного модуля создает виртуальное изображение боевого пространства. Системный модуль обеспечивает функционирование аппаратных средств системы JWARS и создает человеко-машинные интерфейсы обмена данными, с помощью которых осуществляются ввод исходных данных и получение результатов моделирования [353].

Более подробные данные о внутренней логике моделирования боевых действий системой JWARS представлены в работе [353].

4.10.2.2. Система JTLS

Имитационная система моделирования боевых действий JTLS (Joint Theater Level Simulation) — это программно-аппаратный комплекс моделирования действий войск (сил) на ТВД, позволяющий решать различные задачи не только строительства и применения объединенных группировок ВС в различных условиях военно-стратегической обстановки, но и отрабатывать вопросы борьбы с терроризмом, а также проводить тренировки в урегулировании различных кризисных и чрезвычайных ситуаций. Система JTLS может быть установлена как на отдельном (выделенном) автономном компьютере, так и функционировать в глобальной информационно-управленческой сети GIG, объединяющей не только формирования ВС США, но и группировки ВС других стран НАТО и их ближайших союзников [355].

Система JTLS активно применяется в следующих областях военного строительства [355]:

- исследование, развитие и оценка планов применения группировок ВС в различных условиях обстановки (в том числе в кризисных условиях) и совершенствования тактики применения объединенных (межвидовых) и многонациональных формирований;
- сравнительная оценка альтернативных вариантов боевого применения войск (сил);
- анализ структуры и состава боевых и обеспечивающих формирований, имеющих на вооружении различные образцы ВВТ;
- проведение командно-штабных учений, военных игр и других мероприятий в системе оперативной подготовки объединенных и коалиционных (многонациональных) штабов и пр.

JTLS — интерактивная конструктивная многопользовательская система, предназначенная в основном для моделирования и имитации операций на ТВД объединенными и коалиционными группировками войске воссозданием воздушной, наземной и морской обстановки (то есть действий преимущественно оперативного масштаба). В системе предусмотрена имитация решения боевых задач, которые могут быть поставлены ООФ и их компонентам (наземному, воздушному и морскому), а также формированиям сил специальных операций, органам разведки, силам и средствам тыла. Все задачи разработаны в соответствии с «Единым перечнем универсальных задач» КНШ ВС США. И хотя в основу JTLS положена комплексная модель подготовки и ведения крупномасштабной войны на ТВД с применением обычного оружия, в системе преду-

смотрено влияние на ход и исход операции ограниченного применения ядерного и химического оружия, а также иных мероприятий, которые могут проводиться в угрожаемый период или вне рассматриваемого ТВД. При этом моделирование может осуществляться для любого ТВД и от пользователей не требуется знания основ программирования [355].

Для нормальной работы в систему JTLS необходимо внести информацию и создать базы данных:

- по интересующим пользователей ТВД (цифровые карты с характеристиками, влияющими на ведение боевых и других действий, в том числе погодные и климатические условия, рельеф, объекты инфраструктуры и т. д.);
- по боевому и численному составу, возможностям формирований ВС (в том числе и иррегулярным формированиям), которые могут привлекаться для моделирования и имитации;
- по тактико-техническим характеристикам и возможностям образцов ВВТ всех сторон;
- по характеристикам и возможностям других (невоенных) организаций и структур, которые могут существенно повлиять на ход и исход моделирования;
- по таблицам поражения объектов (целей);
- по переброскам войск и грузов;
- по поэтапному и повременному развертыванию войск (сил) на удаленных ТВД.

В качестве картографической основы в системе JTLS применяются цифровые карты и базы данных поверхности Земли и Мирового океана, разработанные Национальным управлением геопространственной разведки МО США [355].

Кроме того, система JTLS сопрягается с реальными системами управления ВС США и их союзников по НАТО. Так, в ходе учений и командно-штабных игр осуществлялась проверка ее сопрягаемости с Глобальной системой оперативного управления GCCS (Global Command Control System), Системой информационного обеспечения объединенного командования JMCIS (Joint Military Command Information System) и Объединенной системой оперативного отслеживания обстановки JOTS (Joint Operational Tracking System) ВС. В результате на мониторах пользователей JTLS отражалась картина реальной оперативной обстановки, сложившаяся к тому времени в разных регионах мира [355].

С помощью системы JTLS могут быть смоделированы действия межвидовых формирований, включающих компоненты воздушных, морских, наземных сил и сил специальных операций (ССО) оперативного уровня (от дивизии сухопутных войск (сил) и ей равных формирований других видов ВС). Все процессы, связанные с организацией и ведением боевых и других действий, воспроизводятся на основе алгоритмов, разработанных с учетом действующих руководящих документов ВС США и НАТО. При этом предусмотрена возмож-

ность гибкой подстройки заложенных правил в зависимости от требований пользователей JTLS [355].

Система имеет возможность одновременного отображения целей и объектов, имеющих различные уровни детализации и агрегации. При этом объекты «своих» войск представляются, как правило, на более высоком уровне агрегации с предоставлением необходимой информации об их составе, структуре и возможностях по требованию пользователя. В модели могут имитироваться действия до 10 сторон (участников) одновременно. При этом каждая группировка теоретически может быть разделена на неограниченное число элементов — единичных объектов, способных к отображению на картографической основе и обладающих функциями целого, состав и функции которых могут меняться в ходе игры. Как правило, применяется уровень детализации до мотопехотного, танкового батальона (артиллерийского дивизиона) для «своих» подразделений и до цели (объекта поражения) — для войск «противника» [355].

Взаимоотношения сторон в ходе сценария могут иметь различный характер (союзнические, нейтральные, подозрительные или враждебные), который определяется в начале игры с помощью активации соответствующей базы данных. В дальнейшем взаимоотношения могут меняться — как по решению пользователя-руководителя одной из сторон, так и автоматически (в случае нанесения ударов одной из сторон по объектам «противника»). Это влияет на то, как формирования противоположных сторон могут реагировать на взаимный контакт. Например, средства ПВО могут открывать «огонь» только по авиации «противника», оставляя без воздействия летательные аппараты и конвои «союзников», «нейтралов» и подозрительной стороны [356].

Модель системы JTLS предполагает наличие определенных правил ведения боевых действий. Это позволяет пользователям планировать предстоящие действия, принимая во внимание различные варианты развития ситуации, и прогнозировать действия противоположных сторон. Правила моделирования учитывают как общепринятые законы войны, так и характер взаимоотношения сторон. Например, ни один объект противоположной стороны не может быть атакован, если он однозначно не определен как «противник». Кроме того, предусмотрена возможность учитывать особенности обстановки, складывающейся в районе боевых действий в отношении гражданских организаций и некомбатантов [356].

Ближний бой между формированиями сторон моделируется на основе смешанных, разнородных дискретных уравнений Ланчестера. В отдельную группу вынесен математический аппарат для расчета потерь от огня прямой наводкой и с закрытых огневых позиций. Предусмотрено влияние на результаты моделирования условий окружающей среды (климата, погоды, местности и пр.), времени года и суток. Действия формирований более высокого уровня иерархии (агрегации) имитируются с учетом конкретных возможностей по огневому поражению входящих в их состав частей и подразделений с детальной оценкой полученных результатов [356].

Действия сил и средств ПВО моделируются стохастически при решении всех задач сценария для каждого уровня детализации. При этом основными

расчетными величинами являются вероятность обнаружения и вероятность поражения воздушной цели противника средствами противовоздушной обороны. Огневое поражение с использованием ракет классов «воздух-поверхность» и «поверхность-поверхность», а также артиллерии (включая корабельную огневую поддержку) учитывается на всех этапах сценария, если это необходимо, с помощью двух разных моделей. При расчетах поражения с применением высокоточных боеприпасов используется стохастическая модель, основанная на вероятности попадания и вероятности поражения объектов (целей) противника. В основу детерминированной модели огневого поражения обычными средствами (стрельбы по площадям) положена плотность поражения цели [355].

Моделирование действий ВВС осуществляется с помощью специальной программы — генератора ATOG. Генератор автоматически разбивает цели по группам важности и типам самолетов. Кроме того, у пользователей имеется возможность самим формировать задачи авиации. Модель воздушного боя, реализованная в системе JTLS, позволяет решать следующие задачи: имитации действий авиации в ходе воздушного боя; системы дальнего радиолокационного обнаружения и управления AWACS; ведения РЭБ; выполнения заправки в воздухе; конвоирования; нанесения ударов по наземным целям, непосредственной авиационной поддержки и боевого дежурства в воздухе; ПВО; разведки (в пилотируемом и беспилотном вариантах); осуществления воздушных перебросок и десантирования войск и грузов; минирования с воздуха; противолодочной борьбы; опознавания войск; поиска и спасения и др. [357].

В ходе моделирования действий ВВС могут отрабатываться действия как самих летательных аппаратов, так и оружия, имеющегося на их борту. Типовые задачи авиации создаются заранее для каждого типа самолетов и закладываются в базу данных сценариев, что позволяет системе автоматически предлагать пользователям варианты для их решения. Ущерб, наносимый «противнику», зависит от эффективности применяемого по нему оружия и условий его применения, которые также заранее занесены в базу данных. Правила ведения воздушного боя разработаны как для авиационной эскадрильи, так и для выполнения задач на индивидуальном уровне. Пользователь может самостоятельно выбирать необходимое оружие для выполнения специфических заданий. В ходе имитации полета автоматически ведется учет расхода топлива и боеприпасов, пополнение которых возможно только на базовых аэродромах. Неиспользованные боеприпасы и топливо по возвращении на аэродромы базирования сохраняются. В случае отсутствия специфического оружия для решения той или иной задачи она может быть выполнена другим, альтернативным видом оружия с учетом новых коэффициентов. При необходимости на аэродромах имитируется процесс ремонта и восстановления летательных аппаратов, что отражается на общем сценарии игры [357].

Военно-морские силы в модели системы JTLS могут выполнять задачи как самостоятельно, так и в составе объединенной (межвидовой) группировки. К числу наиболее важных из них можно отнести: бой кораблей с применением артиллерийских орудий и ракет класса «корабль — корабль»; огневые удары по берегу с использованием артиллерийского и ракетного оружия; перевозки

амфибийных сил и их высадку; патрулирование района и противолодочную борьбу; операции ВВС флота; ПВО, включая ПРО важных объектов; минную войну; блокада ВМС «противника» [357].

Надводные и подводные корабли ВМС в составе моделей обладают значительными возможностями по совершению маневра и поражению целей. Авиация флота может быть использована практически в любых сценариях развития обстановки. Корабли флота способны выполнять различные задачи и в условиях мирного времени. Все эти особенности учитываются в системе JTLS [357].

При моделировании действий ВМС применяются соответствующие правила ведения боевых действий. Так, например, корабли, имеющие незадействованные системы ракетного оружия, могут автоматически уничтожать морские цели «противника», если они находятся в зоне их досягаемости. В то же время специальные возможности, включая палубную авиацию, считаются недействующими, если корабль подвергся удару «противника». В случае значительного повреждения корпуса корабли могут выводиться из боевых действий, в том числе и путем их автоматического затопления. Ремонт должен проводиться в военно-морских базах (ВМБ) с соответствующими затратами времени, что немедленно заносится в базу данных системы JTLS. Пополнение запасов материально-технических средств может осуществляться в море путем доставки их необходимой номенклатуры транспортами и гражданскими судами «своих» сил или сил «союзников» [357].

Подводные лодки в JTLS моделируются как уникальное боевое средство военно-морской группировки. Они вводятся в игру скрытно, имея особый статус. Их не могут обнаружить традиционные средства разведки, за исключением сонаров кораблей или противолодочной авиации. Однажды обнаруженная лодка теряет контакт со средством разведки, а для повторного ее обнаружения необходимо провести дополнительные разведывательные мероприятия. На вооружении подводной лодки обычно имеются сонар, ракеты класса «корабль — корабль» и/или торпеды, что обеспечивает наиболее эффективное ее использование только против морских целей. В случае повреждения лодки она автоматически переводится в надводное положение и теряет статус «невидимости». Как и надводные корабли, подводная лодка способна выполнять задачи самостоятельно или входить в состав морских группировок [357].

Модель разведки в JTLS может решать следующие задачи: ведение разведки штатными силами и средствами; получение разведданных от старшего начальника или из общей сети; создание единой базы данных по разведке; доведение разведывательной обстановки до пользователей системы, в части их касающейся; создание общей картины оперативной обстановки за войска сторон; распределение разведывательной информации между пользователями и др. [357]

Пользователи JTLS, выступающие в роли командиров всех степеней и офицеров штаба, могут получать информацию о противнике в боевом приказе и иных распоряжениях в части, касающейся выполнения полученной задачи. Одним из достоинств системы является то, что существует возможность визуаль-

ного отображения реальных размеров группировок сторон. Другая информация начинает поступать с подключением к работе систем разведки. И хотя для добывания сведений различными методами требуется разное время, что учитывается в базе данных, информация, один раз попавшая к добывающим органам одной из сторон, становится доступна всем ее формированиям. В то же время, когда в боевом пространстве обнаруживается какой-либо объект, он не сразу может быть опознан и идентифицирован по имеющейся базе данных. В связи с этим такой объект классифицируется как «неопознанный» с присвоением шестизначного номера и уникальной буквы до получения дополнительной информации о нём [357].

Пользователи могут обмениваться разведывательной информацией с представителями другой стороны, если в этом возникает необходимость и это не противоречит сценарию игры, причем такой обмен может осуществляться как однократно, так и периодически [357].

Командиры формирований, действия которых моделируются в системе, наделены способностью пользоваться данными о положении и статусе войск (сил) других сторон в зоне своей ответственности. Эта зона распространяется на всё боевое пространство в трех измерениях в зависимости от досягаемости основных ударных сил и средств. При этом пользователям необязательно предпринимать какие бы то ни было усилия для получения уже имеющихся разведданных. Достаточно лишь включить соответствующее меню, где отразится таблица целей, находящихся в зоне его ответственности, с разделением объектов поражения по важности. Иногда объект может быть важным по своему назначению, но не входить в зону повышенных интересов данного уровня пользователей, — тогда информация о нём может выдаваться по запросу или появляться периодически [357].

В системе имеются модели тылового обеспечения группировок войск (сил), существенно влияющих на общие результаты боевых действий. В этих моделях учитываются следующие возможности тылового обеспечения: имитация доставки материально-технических средств и их перемещение между формированиями с помощью автотранспорта, морских судов или по железной дороге; автоматическое пополнение материально-технических средств (МТС) формирования; разработка предложений по тыловому обеспечению в предстоящий план действий; создание запасов материально-технических средств; работа нефте- и трубопроводов, доставка топлива морским транспортом; захват запасов МТС «противника» и защита «своих» баз, складов и хранилищ; замена всего имущества на складах или его отдельных категорий, в том числе в интересах выборочных формирований или всей группировки; доставка имущества по воздуху и морю с использованием грузовых модулей; эвакуация погибших, раненых и больных из района ведения боевых действий и др. [357]

Другие рода войск и служб наземных сил также имеют свои правила ведения действий, которые в ходе моделирования просчитываются соответствующими моделями, а их результаты учитываются в общей модели системы JTLS [357].

Таким образом, можно констатировать, что система имитации JTLS — это мощная аналитическая компьютерная модель, используемая в ВС ведущих зарубежных стран для решения различных задач военного строительства и применения войск (сил). Наибольшее развитие она получила в американских ВС и органах военного управления. Используя подобную систему, можно существенно сократить финансовые и временные затраты на разработку планов применения группировок ВС в различных условиях обстановки, на анализ структуры и состава боевых и обеспечивающих формирований, имеющих на вооружении различные образцы ВВТ, а также на проведение КШУ, военных игр и других мероприятий в системе оперативной подготовки объединенных и коалиционных (многонациональных) штабов [357].

4.11. 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 средства технической разведки с полным основанием можно отнести к одному из видов обеспечивающего информационно-технического оружия. Эти средства 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 технической 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 по разведываемым странам и их вооруженным силам [359].

Задачи технической разведки — добывание и последующая обработка сведений [359]:

- о содержании стратегических и оперативных планов вооруженных сил, их боеспособности и мобилизационной готовности, создании и использовании мобилизационных ресурсов;
- о направлениях развития ВВТ, научно-исследовательских и опытно-конструкторских работах по созданию и модернизации образцов ВВТ;
- о количестве, устройстве и технологии производства ядерного и специального оружия;
- о тактико-технических характеристиках и возможностях боевого применения ВВТ;
- о дислокации, численности и технической оснащенности ВС;
- 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 ВВТ 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 [362].

При анализе технических средств разведки используют различные классифицирующие признаки. Классификация видов технических разведок приведена на рис. 4.13.

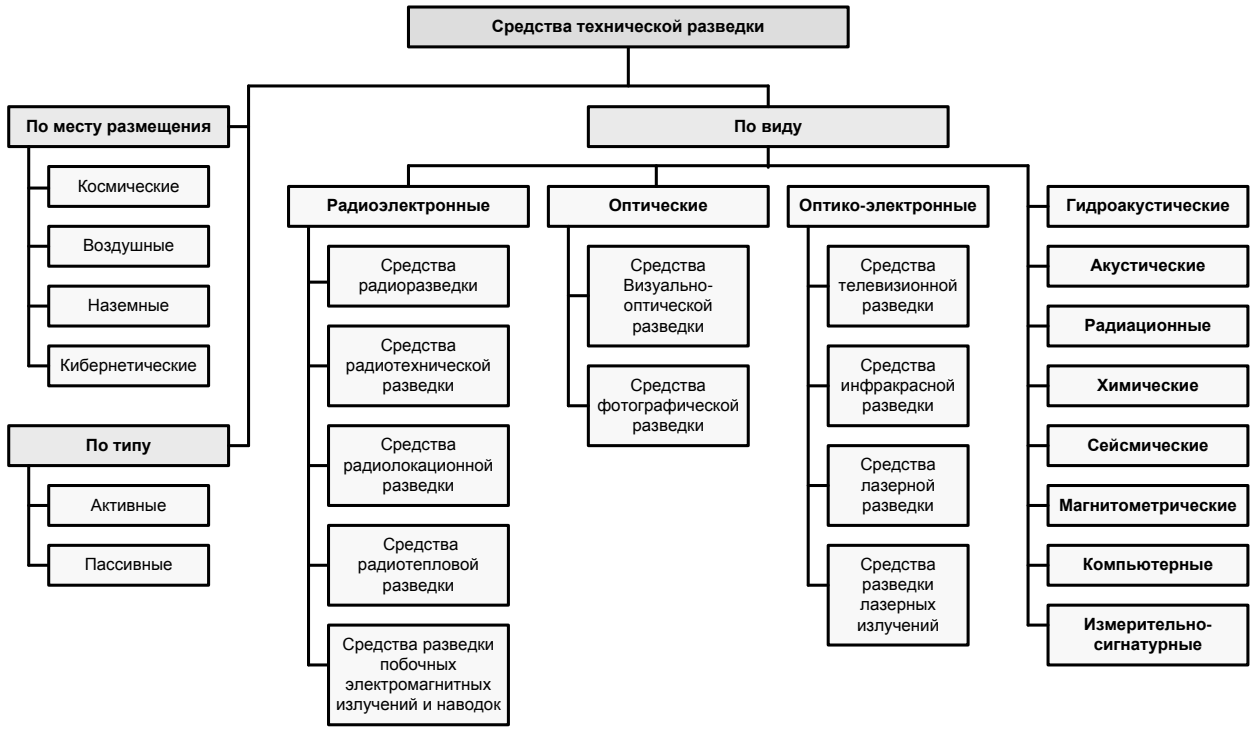


Рис. 4.13. Классификация средств технической разведки [363]

По месту размещения технические средства разведки могут быть классифицированы на:

- космические;
- воздушные;
- наземные;
- кибернетические (размещаемые в киберпространстве).

Для разведки используются различные каналы утечки информации, которые по используемой физической среде (полю) классифицируются следующим образом [360, 362]:

- радиоканалы (электромагнитные излучения радиодиапазона);
- акустические каналы (звуковые колебания в звукопроводящей среде);
- электрические каналы (напряжения и токи в токопроводящих коммуникациях);
- оптические каналы (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой частях спектра);
- материально-вещественные каналы (бумага, фото, магнитные носители, отходы, выбросы и т. д.);
- другие каналы (радиационные, магнитометрические и т. д.).

Выделяют следующие виды технической разведки, которые используют соответствующие средства и каналы утечки информации [359, 360]:

- радиоэлектронную;
- оптическую;
- оптико-электронную;
- акустическую;
- гидроакустическую;
- химическую;
- радиационную;
- сейсмическую;
- магнитометрическую;
- компьютерную;
- измерительно-сигнатурную.

Далее на основании материала, представленного в работе [359], более подробно рассмотрены основные виды разведок и соответствующие им технические средства.

4.11.1. Радиоэлектронная разведка

Радиоэлектронная разведка (РЭР) — это процесс получения информации в результате приема и анализа электромагнитных излучений (ЭМИ) радиодиапазона, создаваемых работающими РЭС [359].

ЭМИ, создаваемые объектами разведки, могут быть первичными (собственными) или вторичными (отраженными) [359].

Радиоэлектронная разведка позволяет решать следующие задачи [359]:

- обнаруживать объекты, определять их местоположение и параметры движения;
- определять параметры объектов и характер их изменения во времени;
- определять назначение объектов и их типы;
- перехватывать передаваемую по каналам связи информацию.

Средства РЭР работают в пассивном или активном режиме (без излучения электромагнитных волн или с излучением) в широком диапазоне спектра радиочастот [359].

Радиоэлектронная разведка обладает следующими особенностями:

- действует без непосредственного контакта с объектами разведки;
- охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн разных частот;
- функционирует непрерывно в разное время года и суток и при любой погоде;
- обеспечивает получение достоверной информации, поскольку она исходит непосредственно от противника (за исключением случаев радиодезинформации);
- добывает большое количество информации различного характера и содержания;
- получает информацию в кратчайшие сроки и чаще всего в реальном масштабе времени;
- малоуязвима и во многих случаях недосягаема для противника;
- действует скрытно, в связи с чем противник, как правило, не в состоянии установить факт разведки.

Радиоэлектронная разведка, в зависимости от ее целевого назначения, подразделяется на стратегическую и тактическую.

Стратегическая РЭР ведется в интересах правительственных органов и высшего военного командования с целью добывания всесторонней информации о разведываемой стране через его радиоэлектронные средства. Такая информация необходима для подготовки ВС и ресурсов страны к войне, принятия решения о начале военных действий и умелого ведения стратегических операций [359].

Тактическая РЭР считается одним из основных видов обеспечения войск информацией путем непрерывного слежения за электромагнитным излучением многочисленных военных устройств и систем противника. Она в состоянии добывать важные сведения для ведения боевых действий силами соединений, частей и подразделений [359].

Различают наземную, морскую, воздушную и космическую радиоэлектронную разведку. По своему содержанию информация, добываемая этим видом разведки, делится на оперативную и техническую.

Оперативная информация включает сведения, которые необходимы для решения оперативных задач военного командования. К ним относятся [359]:

- открытая или зашифрованная смысловая информация, передаваемая противоборствующей стороной по различным каналам радиосвязи;
- тактико-технические данные и особенности разведываемых активных радиоэлектронных систем (частота настройки, вид модуляции и манипуляции, диаграммы направленности антенн, мощность излучения и т. п.), составляющие их «электронный почерк»;
- типы радиоэлектронных систем: радиосвязи, радиолокации, радионавигации, наведения ракет и дальнего обнаружения, различные телеметрические системы передачи данных;
- количество обнаруживаемых радиоэлектронных систем противника;

- местоположение и территориальная плотность размещения источников излучения электромагнитной энергии противника.

Техническая информация содержит сведения о новых системах оружия и управления радиоэлектронными устройствами и об их электрических характеристиках, используемых разведываемой стороной впервые. Целью добывания технической информации является своевременная разработка аппаратуры и методов радиоэлектронной разведки новых систем оружия и средств управления противника [359].

Для получения такой информации средствами РЭР ведется систематическая разведка новых, ранее неизвестных источников радиопередач, отличающихся диапазоном частот, видами модуляции и манипуляции, параметрами импульсного сигнала, диаграммой направленности антенны и другими характеристиками. При этом к наиболее важным источникам РЭР относятся:

- активные средства радиосвязи, используемые во всех видах ВС и в интересах управления государством;
- РЛС разных типов и назначений, применяемые главным образом в ПВО;
- автоматизированные системы управления, слежения и наведения ракетного и противоракетного оружия, а также космических объектов;
- радионавигационные системы, используемые в морской, воздушной и космической навигации;
- различные телеметрические системы передачи информации.

Радиоэлектронная разведка включает в себя следующие составные части [359]:

- радиоразведка;
- радиотехническая разведка;
- радиолокационная разведка;
- радиотепловая разведка;
- разведка побочных электромагнитных излучений и наводок.

Радиоразведка (РР) — самый старый вид радиоэлектронной разведки. Она ориентированна против различных видов радиосвязи. Основное содержание радиоразведки — обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций; пеленгование их сигналов; анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения источников излучения; снижение нагрузки или подрыв криптографических систем [359].

Сведения радиоразведки о неприятельских станциях, системах их построения и о содержании передаваемых сообщений позволяют выявлять планы и замыслы противника, состав и расположение его группировок, установить местонахождение их штабов и командных пунктов управления, место размещения баз и стартовых площадок ракетного оружия и др.

Радиотехническая разведка (РТР) — вид разведывательной деятельности, целью которого являются сбор и обработка информации, получаемой с помощью РЭС о радиоэлектронных системах по их собственным излучениям, и последующая их обработка с целью получения информации о положении

источника излучения, его скорости, наличии данных в излучаемых сигналах, смысловом содержании сигналов. Объектами РТР являются: радиотехнические устройства различного назначения (РЛС, импульсные системы радиоуправления, радиотелекодовые системы, а также ЭМИ, создаваемые работающими электродвигателями, электрогенераторами, вспомогательными устройствами и т. п.) [359].

Средства РТР устанавливаются на самолетах, космических аппаратах, кораблях и других объектах.

Средства РТР позволяют:

- установить несущую частоту передающих радиосредств;
- определить координаты источников излучения;
- измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры);
- установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная);
- определить структуру боковых лепестков излучения радиоволн;
- измерить поляризацию радиоволн;
- установить скорость сканирования антенн и метод обзора пространства РЛС;
- проанализировать и записать информацию.

Радиолокационная разведка (РЛР) — вид технической разведки, в ходе которой информация добывается с помощью радиолокационных станций. РЛС могут быть стационарные наземные, переносные и установленные на самолетах, спутниках, кораблях и других мобильных объектах. В качестве средств ведения РЛР применяются [359]:

- РЛС бокового, широкополосного и прожекторного обзора, которые устанавливаются на космических и воздушных носителях и используются для получения видовой информации о местности и объектах на ней, над которыми пролетает носитель с аппаратурой;
- наземные и корабельные РЛС, объектами которых являются морские, воздушные и космические цели;
- передвижные и переносные РЛС наблюдения за полем боя, обеспечивающие обнаружение движущихся целей (живой силы и техники) в зоне обзора, приблизительное определение количества целей и скорости их перемещения.

Радиотепловая разведка — вид разведывательной деятельности, целью которой является сбор информации о местоположении наземных, морских, воздушных и космических объектов по их тепловому излучению в радиодиапазоне. Характеристики радиотеплового излучения, такие как интенсивность и спектральный состав, зависят от физических свойств вещества и температуры объекта. Разведка ведется с помощью радиотеплолокационных станций, устанавливаемых на воздушных и космических платформах. Радиотепловая разведка возможна только при наличии контрастности теплового излучения объектов и фона (земной поверхности, неба и т. д.) [359].

Разведка побочных электромагнитных излучений и наводок — получение информации о передаваемой, обрабатываемой информации, а также информации об особенностях построения и функционирования технических средств путем анализа их побочных электромагнитных излучений и наводок от них.

4.11.2. Оптическая разведка

Оптическая разведка — добывание информации с помощью оптических средств, обеспечивающих прием электромагнитных колебаний ультрафиолетового, видимого и инфракрасного диапазонов, излученных или отраженных объектами и предметами окружающей местности. Оптическая разведка позволяет решать следующие задачи [359]:

- поиск военных и военно-промышленных объектов и определение их координат;
- выявление начала строительства военных и военно-промышленных объектов, периодическое наблюдение за ним в целях определения назначения;
- выяснение профиля оборонных предприятий, вида выпускаемой продукции и производственной мощности;
- контроль за выполнением договоров и соглашений по ограничению стратегических вооружений;
- периодическое наблюдение за коммуникациями для обнаружения крупных перевозок военной техники и грузов;
- съемка территории для картографирования местности;
- выявление проводимых учений, маневров войск и сил флота, а также испытаний ВВТ.

Оптическая разведка подразделяется на [359]:

- визуально-оптическую разведку;
- фотографическую разведку.

4.11.3. Оптико-электронная разведка

Оптико-электронная разведка (ОЭР) — процесс добывания информации с помощью средств, включающих входную оптическую систему с фотоприемником и электронные схемы обработки электрического сигнала, которые обеспечивают прием и анализ электромагнитных волн видимого и ИК-диапазонов, излученных или отраженных объектами и местностью [359].

ОЭР предназначена для решения следующих задач [359]:

- выявления военных и военно-промышленных объектов;
- определения их формы, размеров, состояния и боеготовности;
- раскрытия характера выпускаемой ВПК продукции, ее объема и др.;
- съемки территорий в целях картографирования местности;
- разведки метеообстановки в заданных районах.

ОЭР подразделяют на [359]:

- телевизионную разведку;
- инфракрасную разведку;

- лазерную разведку;
- разведку лазерных излучений.

Средства ОЭР устанавливаются на космических и воздушных носителях, а также могут применяться в наземных условиях, например при ведении технической разведки [359].

Средства ОЭР делятся на [359]:

- пассивные;
- активные.

Пассивные основаны на приеме собственного или переотраженного излучения объектов разведки. Активные предполагают использование для подсвета местности собственного излучателя. Зондирующее излучение рассеивается объектами, местными предметами и местностью, часть этого излучения поступает на вход оптической системы аппаратуры разведки с последующим его преобразованием, обработкой и индикацией на соответствующих устройствах [359].

Средства пассивной ОЭР подразделяются на [359]:

- телевизионные;
- инфракрасные;
- средства разведки лазерных излучений.

Аппаратура телевизионной разведки охватывает устройства на ЭЛТ и на ПЗС. К средствам инфракрасной разведки относят тепловизоры, телепеленгаторы, радиометры и приборы ночного видения. Средства разведки лазерных излучений предназначены для обнаружения, определения местоположения и распознавания средств ВВТ, в состав которых входят лазерные излучатели [359].

Средства активной ОЭР подразделяется на [359]:

- лазерные со сканированием зондирующего светового луча;
- инфракрасные с использованием ИК-излучателя для подсвета местности.

4.11.4. Другие виды технической разведки

Гидроакустическая разведка — получение информации путем приема и анализа акустических сигналов инфразвукового, звукового и ультразвукового диапазонов, распространяющихся в водной среде от надводных и подводных объектов [359].

По принципу использования энергии акустического излучения средства гидроакустической разведки делятся на активные (гидролокаторы) и пассивные [359].

Активные средства работают по принципу излучения в водной среде зондирующих акустических сигналов с последующим приемом и анализом отраженных от объектов и морского дна эхосигналов [359].

При ведении пассивной гидроакустической разведки используют шумопеленгаторы, которые принимают и анализируют шумовые акустические излучения в водной среде, возникающие при работе двигателей, гребных валов, машин и механизмов различных агрегатов надводных кораблей, подводных лодок

и других плавсредств, а также средства разведки, предназначенные для приема и анализа акустических сигналов, создаваемых гидролокаторами, эхолотами, системами гидроакустической связи и др. [359].

Акустическая разведка — получение информации путем приема и анализа акустических сигналов инфразвукового, звукового, ультразвукового диапазонов, распространяющихся в воздушной среде от объектов разведки. Акустическая разведка обеспечивает получение информации, содержащейся непосредственно в произносимой либо воспроизводимой речи (акустическая речевая разведка), а также в параметрах акустических сигналов, сопутствующих работе ВВТ, механических устройств оргтехники и других технических систем (акустическая сигнальная разведка) [359].

Радиационная разведка — получение информации в результате анализа радиоактивных излучений, связанных с выбросами и отходами атомного производства, хранением и транспортировкой расщепляющихся материалов, ядерных зарядов и боеприпасов, производством и эксплуатацией реакторов, двигателей и радиоактивным заражением местности [359].

Химическая разведка — добывание информации путем контактного или дистанционного анализа изменений химических свойств состава окружающей среды под воздействием выбросов и отходов производства, работы двигателей, в результате взрывов и выстрелов, преднамеренного рассеивания химических веществ, испытаний и применений химического оружия [359].

Сейсмическая разведка — добывание информации путем обнаружения и анализа деформационных и сдвиговых полей в земной поверхности, возникающих под воздействием различных взрывов [359].

Магнитометрическая разведка — добывание информации путем обнаружения и анализа локальных изменений магнитного поля Земли под воздействием объектов с большой магнитной массой [359].

Измерительно-сигнатурная разведка ведется в интересах обеспечения успеха военных операций ВС, создания новых поколений ВВТ, определения направлений модернизации ВС, контролем за распространением оружия, окружающей средой, а также выполнением военных договоров [359].

Сущность измерительно-сигнатурной разведки заключается в комплексном характере сбора разведывательной информации: во-первых, измерение геометрических размеров и соотношений статических, динамических и других физических характеристик разведываемых объектов (стационарных и подвижных) и, во-вторых, регистрация сигнатур характерных физических полей, создаваемых этими объектами (электромагнитных, магнитных, радиационных, акустических, сейсмических и других), а также выявление химических и биологических агентов и даже состава конструкционных материалов объектов и их элементов. При этом используются все существующие датчики: оптические, радиолокационные, лазерные, радиочастотные, акустические, сейсмические, радиационные, химические, оптико-электронной и радиолокационной съемки с перекрытием практически всего спектра электромагнитных колебаний [359].

Следует иметь в виду, что физические измерения и снятие сигнатур не являются самоцелью измерительно-сигнатурной разведки. Главное в ней —

выявление назначения, тактики применения, возможностей и основных характеристик, а также уязвимых мест разведываемого объекта [359].

Дополнительные сведения о средствах технической разведки, а также примеры и описание принципов функционирования конкретных технических устройств представлены в работах [359, 360].

4.12. Средства компьютерной разведки

4.12.1. Общие сведения о средствах 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 [359]. Однако в настоящее время стало общепризнанным, что это слишком узкий, упрощенный подход к компьютерной разведке и в настоящее время данное понятие активно модернизируется и развивается.

Объектами компьютерной разведки являются компьютерные системы и сети, которые включают: 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. [361].

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 [361]:

- данные, сведения и информация, обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях;
- характеристики программных, аппаратных и программно-аппаратных комплексов;
- характеристики пользователей компьютерных систем и сетей.

Общая классификация средств компьютерной разведки представлена на рис. 4.14.

По виду реализации средства компьютерной разведки можно классифицировать на:

- *физические* — реализованные в виде физических или аппаратных средств, которые подключаются к инфокоммуникационной инфраструктуре, ведут анализ физических полей, побочных электромагнитных излучений и наводок (ПЭМИН) в интересах добывания данных, сведений и информации;
- *программные* — реализованные в виде программных средств, которые в виде вирусов, закладок или специализированного программного обеспечения добывают данные, сведения и информацию за счет анализа логики построения и функционирования компьютерных систем, а также информационных потоков, циркулирующих в них.

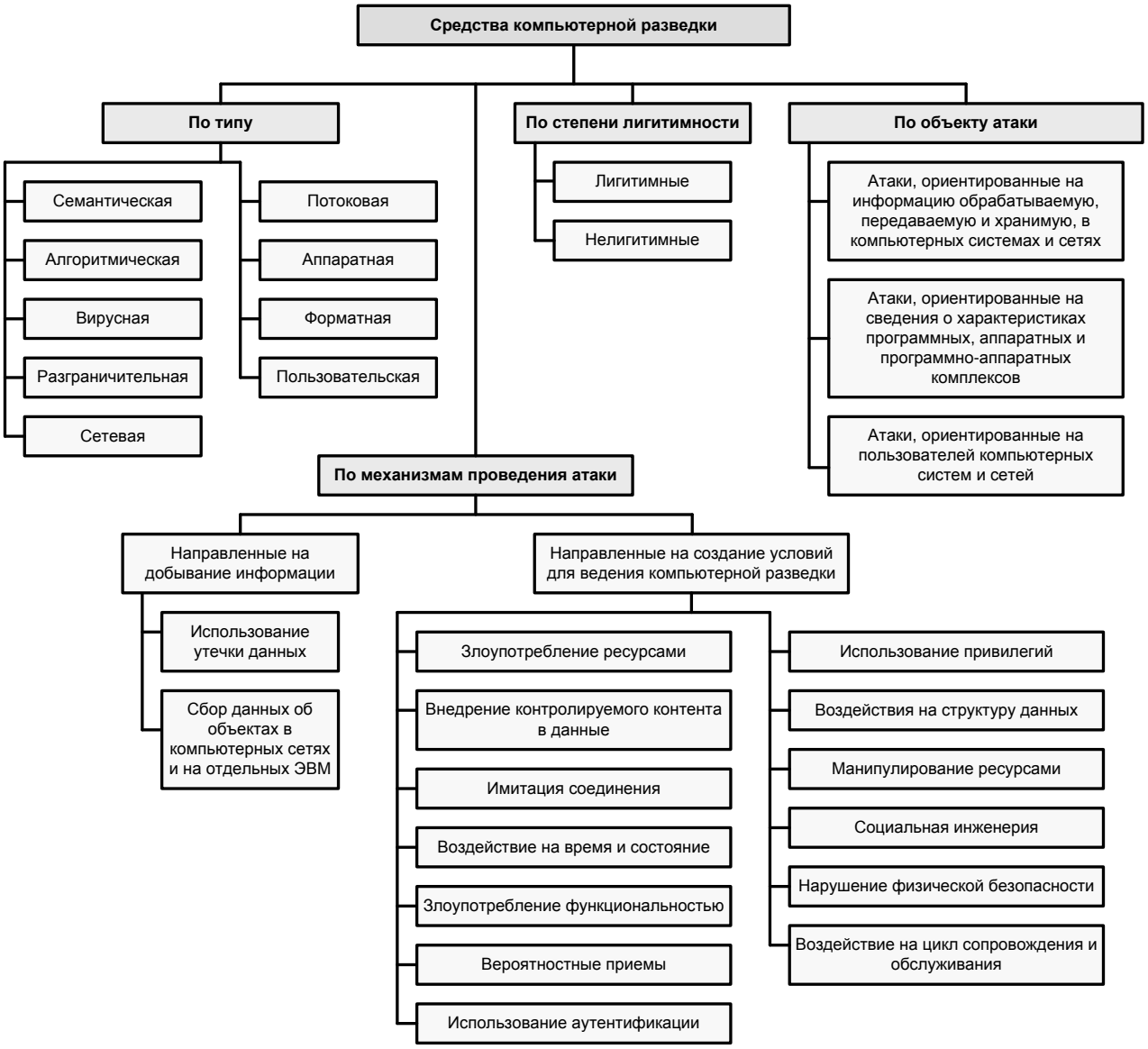


Рис. 4.14. Классификация средств компьютерной разведки

По принципам построения средств и их функциональному предназначению можно выделить следующие типы компьютерной разведки [361]:

- *семантическая* — обеспечивающая добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов в целях создания специальных информационных массивов;
- *алгоритмическая* — с использованием программно-аппаратных закладок и недекларированных возможностей, обеспечивающая добывание данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей;

- *вирусная* — обеспечивающая добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и в системы для перехвата управления компьютерными системами;
- *разграничительная* — обеспечивающая добывание информации из отдельных (локальных) компьютерных систем, возможно, и не входящих в состав сети, на основе преодоления средств разграничения доступа (несанкционированный доступ к информации в АСУ), а также реализация несанкционированного доступа при физическом доступе к компьютеру или компьютерным носителям информации;
- *сетевая* — обеспечивающая добывание данных из компьютерных сетей путем мониторинга сети, инвентаризации и анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскировка своих действий;
- *потоковая* — обеспечивающая добывание информации и данных путем перехвата, обработки и анализа сетевого трафика, выявления структур компьютерных сетей, а также их технических параметров;
- *аппаратная* — обеспечивающая добывание информации и данных путем обработки сведений, получения аппаратуры, оборудования, технических модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими видами компьютерной разведки;
- *форматная* — обеспечивающая добывание информации и сведений путем «вертикальной» обработки, фильтрации, декодирования и других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем — в информацию для последующего ее наилучшего представления пользователям;
- *пользовательская* — обеспечивающая добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной ложной информационной инфраструктуре.

На данном этапе развития компьютерных систем и сетей эти девять типов компьютерной разведки охватывают все существующие многоуровневые «горизонтальные» и «вертикальные» каналы утечки информации из компьютерных систем и сетей. При этом внутри указанных типов возможно выделение нескольких подтипов разведки, например по виду добываемой информации на: *фактографическую* («*видовую*») и *параметрическую*.

Основным способом реализации разведки является *атака средств компьютерной разведки* [364, 365].

Атака средств компьютерной разведки — 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.

Атаки средств компьютерной разведки также можно классифицировать по различным основаниям.

1. По степени легитимности атаки средств компьютерной разведки можно разделить на [364]:

- легитимные (разведка на основе открытых источников, анализ сетевого трафика);
- нелегитимные (перехват трафика, несанкционированный доступ к компьютерным системам и т. д.).

2. По объекту атаки [361]:

- атаки, ориентированные на данные, сведения и информацию, обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях;
- атаки, ориентированные на сведения о характеристиках программных, аппаратных и программно-аппаратных комплексов;
- атаки, ориентированные на сведения о пользователях компьютерных систем и сетей.

3. По механизмам проведения атаки [365]:

- атаки, направленные на добывание информации в компьютерных сетях и ЭВМ:
    - использование утечки данных;
    - сбор данных об объектах в компьютерных сетях и на отдельных ЭВМ;
- атаки, направленные на создание условий для ведения компьютерной разведки:
    - злоупотребление ресурсами;
    - внедрение контролируемого контента в данные;
    - имитация соединения:
    - воздействие на время и состояние;
    - злоупотребление функциональностью;
    - анализ вероятностей событий;
    - использование аутентификации;
    - использование привилегий;
    - воздействия на структуру данных;
    - манипулирование ресурсами;
    - социальная инженерия;
    - нарушение физической безопасности;
    - воздействие на цикл сопровождения и обслуживания.

Другие аспекты атак, такие как способы нападения и используемые уязвимости, также можно рассматривать в качестве оснований для классификации атак компьютерной разведки.

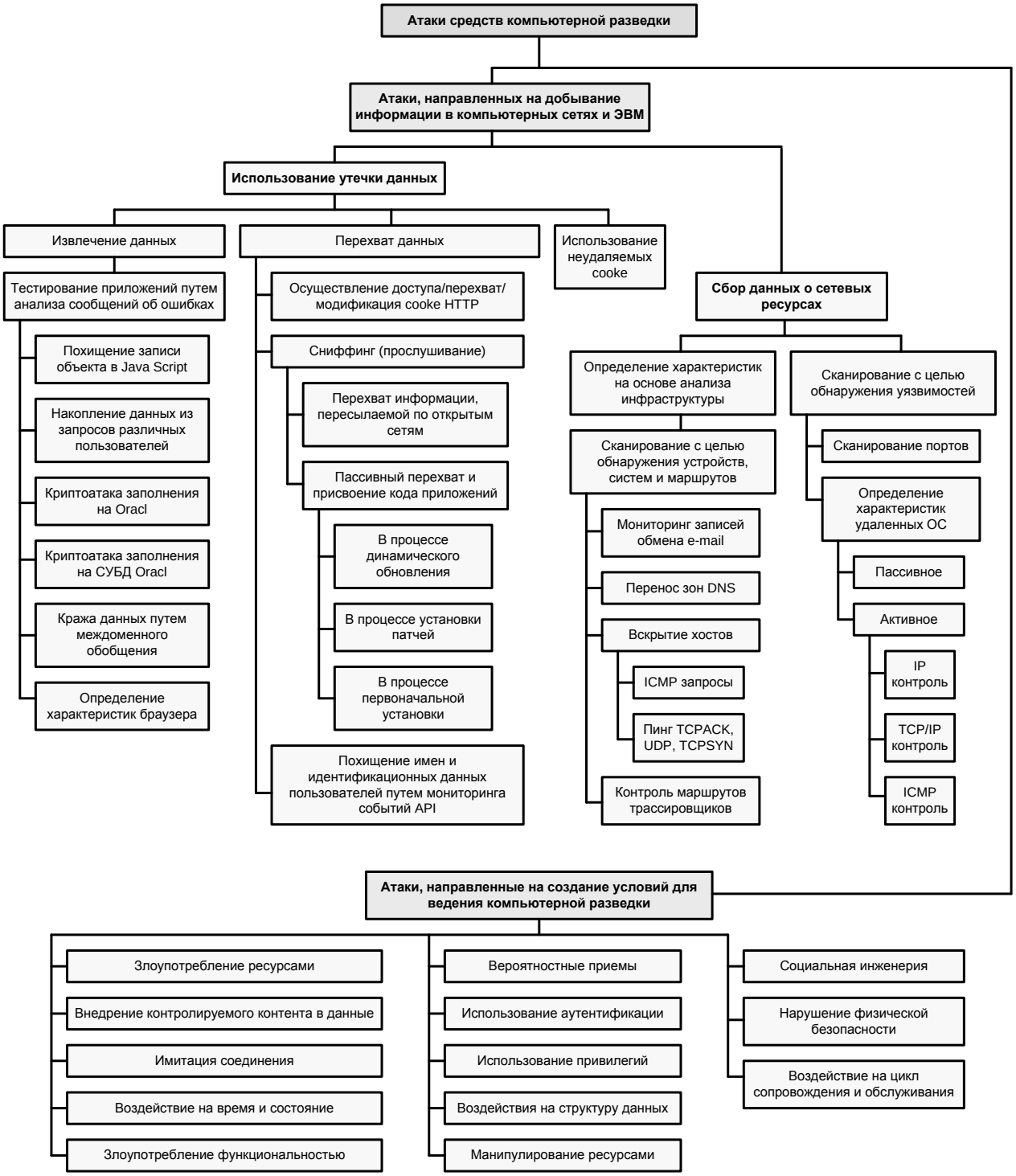


Рис. 4.15. Классификация атак средств компьютерной разведки [365]

К настоящему времени сложился подход к описанию компьютерных атак, основанный на использовании их классификации с учетом множества признаков. Наиболее полный учет признаков реализован в классификации CAPEC [366], разработанной корпорацией MITRE. Однако классификация CAPEC не выделяет в отдельную категорию атаки средств компьютерной разведки. Учитывая этот недостаток классификации CAPEC, отечественными специалистами в работе [365] была предложена классификация атак средств компьютерной разведки с включением в классификацию образцов конкретных атак. Эта классификация представлена на рис. 4.15.

4.12.2. Примеры 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 санкционированы на государственном уровне и ведутся для получения стратегического информационного превосходства в военной, политической и промышленной сфере.

К странам, имеющим наибольшие достижения в области создания глобальных комплексов компьютерной разведки, необходимо отнести США (программы: Carnivore, Eshelon, NarusInsight, Turbulence, CO-TRAVELER, PRISM, Dropmire, X-Keyscore), Великобританию (программа Tempora), Китай (программа «Золотой щит») и Россию (программа СОРМ). Другие технически развитые страны также создают свои комплексы компьютерной разведки — Франция (программа Frenchelon), Швейцария (программа Onyx), Швеция (программа Titan), Индия (программы NATGRID, Central Monitoring System, DRDO NETRA).

Eshelon — глобальная система радиоэлектронной разведки, работающей в рамках соглашения о радиотехнической и разведывательной безопасности Великобритании и США. Система Eshelon разрабатывалась в 80-х гг. и с тех пор неоднократно модернизировалась. Eshelon обеспечивает возможность перехвата и анализа телефонных переговоров, факсов, электронных писем и других информационных потоков по всему миру путем подключения к различным каналам радио- и электросвязи, таким как спутниковая связь, телефонная сеть общего пользования, радиосвязь. В последних сообщениях по техническим средствам системы Eshelon отмечается, что основной упор в данной системе сделан на перехвате и анализе спутниковых коммуникаций, но помимо них перехватываются сообщения, проходящие через подводные межконтинентальные кабели электросвязи, а также ВЧ- и СВЧ-каналы связи. Использование суперкомпьютеров для автоматизированного анализа сообщений позволяет системе Eshelon перехватывать, запоминать и анализировать до 3 млрд сообщений в день [367].

Stellar Wind — программа слежения за электронными коммуникациями, осуществлявшегося АНБ США в период президентства Дж. Буша. Stellar Wind представляет собой пакет из четырех программ, которые, используя технологии интеллектуального анализа данных, вели поиск по обширной базе коммуникаций граждан США, включая сообщения электронной почты, телефонные разговоры, финансовые операции и интернет-активность в целом [369].

Программы Eshelon и Stellar Wind являлись прототипами глобальной системы PRISM.

PRISM (Program for Robotics, Intelligents Sensing and Mechatronics) — государственная программа США, осуществляемая с целью глобального негласного сбора информации, передаваемой по сетям электросвязи. PRISM представляет собой комплекс мер, предоставляющих возможность глобального мониторинга интернет-трафика пользователей и некоторых интернет-ресурсов.

Потенциальной целью наблюдения могут быть любые пользователи определенных сервисов, не являющиеся гражданами США, либо граждане США, чьи контакты включают иностранцев. Средства PRISM дают возможность АНБ США просматривать электронную почту, прослушивать голосовые и видеочаты, просматривать фотографии, видео, отслеживать пересылаемые файлы, вести мониторинг социальных сетей. По программе PRISM с АНБ сотрудничали многие крупные компании — Microsoft, Google, Yahoo!, Facebook, YouTube, Skype, AOL, Apple и Paltalk. Ежедневно системы сбора информации АНБ (в том числе PRISM) перехватывали и записывали около 1,7 млрд телефонных разговоров и электронных сообщений и около 5 млрд записей о местонахождении и передвижениях владельцев мобильных телефонов по всему миру [368].

CO-TRAVELER — программа АНБ США для отслеживания передвижения владельцев сотовых телефонов и выявления сети их контактов. Программа CO-TRAVELER позволяет по собранным данным о зарегистрированных в сети операторов мобильным телефонам определять траектории движения абонентов и выстраивать социальные сети взаимодействия между людьми. Основой программы является интеллектуальный анализ данных, позволяющий выявить закономерности или подозрительные паттерны поведения групп пользователей за счет анализа их звонков и передвижений в глобальной пространственно-временной области. При этом в рамках программы CO-TRAVELER ежедневно АНБ собирает около 5 млрд записей о местонахождении и передвижениях владельцев мобильных телефонов по всему миру [370].

Dropmire — программа АНБ США для наблюдения за иностранными посольствами и дипломатическим персоналом, в том числе стран-союзников по НАТО. Программа Dropmire имела 38 объектов компьютерной разведки среди посольств и дипломатических миссий, включая миссии ЕС, Франции, Италии, Греции и др. Основными техническими средствами реализации программы являлись аппаратные и программные закладки, внедряемые в телекоммуникационные системы дипломатических представительств, через которые осуществилась добыча информации [372].

X-Keyscore — программа компьютерной разведки, используемая совместно АНБ США, Управлением радиотехнической обороны Австралии и Службой безопасности правительственных коммуникаций Новой Зеландии. Предназначена для слежения за иностранными гражданами во всём мире. Техническим обеспечением программы являются более чем 700 серверов, расположенных в США и на территории стран — союзников США, а также в посольствах и консульствах США в нескольких десятках стран. Система X-Keyscore выявляет гражданство иностранцев, анализируя язык, используемый в их сообщениях электронной почты, перехваченных в странах Латинской Америки, особенно в Колумбии, Эквадоре, Венесуэле и Мексике. Система X-Keyscore имеет возможность сохранять на протяжении нескольких дней метаданные и содержание перехваченных сообщений [373].

Tempora — программа компьютерной разведки, открытая в 2011 г. и используемая Центром правительственной связи Великобритании GCHQ

(Government Communications Headquarters) совместно с АНБ США. Программа Tempora состоит из двух компонентов — Mastering the Internet и Global Telecoms Exploitation, — каждый из которых ведет сбор данных из перехватов телефонных разговоров и интернет-трафика в максимально возможных объемах. Полученные данные сохраняются в течение трех дней, метаданные хранятся в течение 30 дней. Программа Tempora предусматривает ведение записи телефонных звонков, фиксации содержания сообщений электронной почты, записей в Facebook и личных профилей интернет-пользователей в других социальных сетях. На момент запуска программа Tempora в 2011 г. обладала сетью из 200 каналов передачи данных, каждая с пропускной способностью 10 Гбит/с. В настоящее время центр GCHQ ведет техническую модернизацию каналов передачи данных Tempora, планируя довести их пропускную способность до 100 Гбит/с [374].

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 — 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.

4.13. 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 в. глобального информационного пространства и сети Интернет, по оценкам американского военного руководства, OSINT резко повысила свою значимость [375, 376].

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. Естественно, что информация, полученная таким образом, нуждается в верификации [377].

В сферу интересов такой разведки входят добывание и анализ официальных документов, проектов уставов и наставлений, отслеживание новых науч-

ных разработок и проектов, баз данных, коммерческих и государственных интернет-сайтов, сетевых дневников и многого другого [375, 376].

Для решения задач анализа открытых источников используются аппаратно-программные средства, основу которых составляют алгоритмы поиска и семантического анализа. Вариант классификации таких средств представлен на рис. 4.16.

Рис. 4.16. Вариант классификации
средств разведки по отрытым источникам

4.13.1. Средства разведки на основе традиционного семантического анализа и поисковых программ

В качестве средств разведки на основе анализа открытых источников в Интернете традиционно используются специальные программы анализа данных. Под ними понимаются программы-роботы, которые опрашивают сайты и извлекают из них нужную информацию, используя широкий спектр средств лингвистического, семантического и статистического анализа. Действуя автономно, такие программы анализа данных выявляют любую целевую информацию, как только она появится в Интернете [377].

Примерами таких программ могут служить программы Taiga, Tropes, Noemic, а также современные комплексы интеллектуального анализа так называемых «Больших данных» (Big Date).

К первым упоминаниям о подобной программе анализа стоит отнести упоминание о французской программе Taiga (Traitement automatique d’information geopolitique d’actualite — автоматическая обработка актуальной геополити-

ческой информации). Программный комплекс Taiga первоначально разрабатывался для нужд французской разведки, где он успешно применялся в течение 11 лет. После этого Taiga был передан для коммерческого использования. Задачи, которые перед ним ставят теперь уже гражданские специалисты, остались теми же: исследовать Интернет с целью извлечения ценной информации из баз данных о патентах, сообщений информационных агентств и публикаций в научных журналах. Методика ведения разведки с помощью ПО Taiga следующая: обрабатывая материалы открытого доступа, имеющиеся в Интернете, программа статистического анализа составляет так называемые карты работ в различных отраслях науки. В свою очередь, это позволяет аналитикам устанавливать наиболее перспективные научные разработки, а также оценить перспективность и результативность различных исследовательских коллективов [377].

Стоит упомянуть еще одну французскую разработку. Для проведения семантического анализа крупных информационных массивов компания Acetic совместно с учеными Парижского университета разработала пакет прикладных программ Tropes. Отбор требуемой информации происходит в соответствии с ключевыми словами и понятиями, связанными по смыслу. Помимо анализа, Tropes предоставляет возможность задавать информационные «сценарии», на основе которых автоматически осуществляется не только поиск, но и целевое группирование требуемых данных [377].

Программа Noemic, сменившая Taiga на боевом посту во французской разведке, не только сканирует, но и автоматически осуществляет семантическое объединение источников, обрабатывая полученную информацию со скоростью 1 млрд знаков в секунду, независимо от того, существует ли она в виде готовой базы данных или, например, передается электронным агентством новостей на любом языке в виде целостного текста. Кроме того, программа Noemic оснащена модулем семантического анализа и сбора данных и способна подвергать обработке заслуживающие внимания концепции, метафоры и совокупности идей, а также цепочки неслучайных совпадений и событий [377].

Американская фирма Intelligent Search Solutions выпустила на рынок пакет ПО Info Tracer, предназначенный для сбора разведывательной информации в открытых источниках сети Интернет. Для «фильтрации» информации указанное ПО использует ключевые слова и фразы, после чего автоматически составляются сообщения по заданной пользователем форме [377].

Ввиду того, что имеющимися техническими средствами полностью формализовать процедуру поиска информации пока не представляется возможным, реализовать сложную стратегию поиска необходимой информации часто бывает весьма затруднительно. Поэтому при ведении разведки по открытым источникам в сети Интернет приходится идти по пути информационной избыточности, что накладывает весомые ограничения на релевантность найденных документов. Из-за высокого информационного шума в общем объеме найденных документов значительно увеличивается время, необходимое для аналитической обработки полученных сведений [377].

Особенностью программ анализа данных на основе семантических поисковых алгоритмов является то, что они могут находить только ту информацию,

которая в явном виде находится 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 интересным 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).

4.13.2. Средства разведки на основе технологий «Больших данных»

Термин «Большие данные» был впервые введен в 2009 г. в специальном выпуске ведущего американского научного журнала Nature, целиком посвященного этой теме. Введение этого понятия обусловлено следующими факторами.

1. Глобальная сеть Интернет перешла в фазу явно выраженного экспоненциального развития, или по-другому — «информационного взрыва». Примерно с 2008 г. объем информации, вновь генерируемой в сети Интернет, стал удваиваться в течение примерно полутора-двух лет. По данным компании Cisco, объем сгенерированных данных в 2012 г. составил 2,8 зеттабайта и увеличится до 40 зеттабайт к 2020 г. Примерно треть передаваемых данных составляют автоматически сгенерированные данные, т. е. управляющие сигналы и информация, характеризующие работу машин, оборудования, устройств, присоединенных к Интернету, или, как его еще называют, «Интернету вещей» [378].
2. В 2010-х гг. появились и стали доступны принципиально новые IT-решения, позволяющие в режиме реального времени обрабатывать практически безразмерные массивы данных самого различного формата. Причем эти решения сразу же стали реализовываться не только как программные платформы, устанавливаемые на серверы, но и как облачные решения, при использовании которых от организации не требовалось наличия дорогостоящей компьютерной инфраструктуры [378].
3. К концу 2000-х гг. западные поведенческие и когнитивные науки, с одной стороны, получили широкое признание, а с другой — из фазы фундаментальных исследований перешли в стадию разработок эффективных технологий анализа поведения и социальных связей в обществе [378].

Таким образом, формирование глобального электронного, постоянно пополняющегося архива поведенческой активности самых различных субъектов, от отдельных государств и огромных компаний до небольших групп и отдельных индивидуумов, собственно и послужило базисом появления Больших дан-

ных. С тех пор направление Больших данных стало ведущим в сфере информационных технологий.

Анализ накопленного за последние годы опыта применения технологий Больших данных позволяет выделить несколько ключевых черт, отличающих Большие данные от всех других информационных технологий. К ним относится следующее [378].

- Огромные массивы разнородной информации о процессах, явлениях, событиях, объектах, субъектах и т. п., пополняемые непрерывно в режиме реального времени. Согласно имеющейся статистике, 60% этой информации носит неструктурированный, в основном текстовой характер, и 40% составляет структурированная, или табличная информация. В последние годы в общем объеме Больших данных постоянно нарастает доля информации структурированного характера, поступающей от вещей, имеющих связь с Интернетом, — от сегмента глобальной сети, называемой Интернетом вещей.
- Специально спроектированные программные платформы, где Большие данные любого объема могут храниться в удобном для вычислений виде. Особо надо подчеркнуть, что эти архивы отличаются от привычных баз данных, которые предназначены для хранения структурированной или табличной информации. Отличительной чертой этих хранилищ является то, что структурированная и неструктурированная информация могут обрабатываться совместно, как единое целое.
- Наличие различного рода математического, прежде всего статистического инструментария для обработки Больших данных и получение результатов в виде, понятном для человека. Причем при анализе Больших данных используются не только традиционные методы математической статистики, но и интеллектуальные алгоритмы обработки данных.

В соответствии с данными исследования [378], не более 0,6% информации, находящейся в Интернете, подпадает под категорию Больших данных, т. е. накапливается, хранится и перерабатывается. В этом же исследовании указывается, что потенциально в качестве Больших данных может использоваться порядка 23% всей хранимой в настоящее время информации. То есть фактически сейчас из всей этой информации в качестве Больших данных, т. е. тех, которые обрабатываются и анализируются, используется чуть больше 3%. Между тем последние достижения в области создания платформ накопления, хранения и обработки объемов данных всех форматов позволяют увеличить потенциальный объем Больших данных с 23% до примерно 40% от всей информации, передаваемой в сети Интернет.

Технологии Больших данных основаны прежде всего на методах статистического и интеллектуального анализа данных, применяемых на огромных, постоянно пополняемых массивах данных.

Технологии Больших данных позволяют [378]:

- *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 корреляционные связи между самыми различными параметрами, характеристиками, событиями и т. п. Эти связи не отвечают на вопрос «почему?», но они указывают на вероятность, с которой при изменении одного фактора изменится 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, то на один из них 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 [378].

Как показано в работе [378], на сегодняшний день существует достаточно большое количество имеющихся в открытой печати, а также в специализированных публикациях данных и фактов, подтверждающих высокий интерес к использованию технологий Больших данных в США.

Во-первых, в США введен в эксплуатацию центр АНБ в штате Юта, в котором размещено хранилище данных в один йоттабайт, что соответствует объему 100-летнего мирового интернет-трафика.

Во-вторых, в США еще в 1994 г. была создана специальная широкополосная сеть для совместного межведомственного использования ресурсов (аппаратных и программных) суперкомпьютеров. Таким образом, в США, в отличие от других стран, суперкомпьютерная сеть не разделена ведомственными и корпоративными барьерами, а функционирует как единое целое. Более того, в начале 2000-х годов американцы договорились, что к этой сети подключатся и британские суперкомпьютеры. Косвенные расчеты позволяют утверждать, что мощность этой объединенной сети составит от половины до двух третей суммарной мощности всех 500 суперкомпьютеров, входящих в настоящее время в мировой рейтинг. С 2014 г. общее руководство этой сетью осуществляет Киберкомандование США. При этом наиболее мощные суперкомпьютеры, входящие в сеть, принадлежат АНБ, Министерству энергетики США, британской разведке и американским университетам, тесно работающим с военно-разведывательным комплексом.

В-третьих, в последние 4 года США истратили несколько сотен миллионов долларов на разработку программ интеллектуального анализа не просто Больших, а сверхбольших массивов данных. При этом, анализируя гранты таких агентств, как DARPA и IARPA, можно увидеть, что средства затрачивались на разработку программ по анализу и прогнозированию на основе Больших данных, базирующихся на принципиально новых разделах математики, типа теории категорий и функторов, на системах распознавания образов, нейронных вычислениях и так называемом глубоком машинном обучении. Все эти методы на порядки превосходят, с точки зрения выявления нетривиальных зависимостей и связей, мощности и точности прогнозирования, методы стандартной математической статистики, которые описываются как основной инструмент в литературе по Большим данным.

В-четвертых, в США предпринимаются организационные и законодательные меры по обеспечению потребностей разведсообщества Большими данными. Прежде всего следует иметь в виду, что само по себе АНБ является обладателем крупнейших массивов Больших данных, которые оно получает в результате своей разведывательной деятельности. Кроме того, организация FSD, тесно сотрудничающая с АНБ, концентрирует у себя данные, которые собирают практически все федеральные ведомства, министерства, агентства и т. п. При этом надо иметь в виду, что в данную организацию дополнительно передаются все данные из страховых компаний, банков, пенсионных фондов, авиакомпаний и т. п., находящихся под американской юрисдикцией. Практически все крупнейшие провайдеры Больших данных (а ими являются компании Google, Facebook, Twitter, Amazon, eBay и т. п.) имеют американскую юрисдикцию. При этом, если в отношении персональных данных предусмотрены некоторые ограничения, то обезличенные Большие данные должны предоставляться, что называется, в рабочем порядке по требованию. Важно, что такие данные должны предоставлять не только американские компании — провай-

деры Больших данных либо брокеры данных, но и все компании, которые котируются на американском биржевом рынке.

При этом Большие данные — это не персональные данные, на передачу которых накладываются определенные ограничения. Более того, для технологий Больших данных сама по себе идентификация конкретного человека не важна и не интересна, потому что связи и закономерности, выявляемые при помощи Больших данных, имеют статистический характер, а не касаются судьбы конкретного индивидуума.

Большие данные, в первую очередь, были использованы в маркетинге, инвестиционном бизнесе, в продажах и т. п. В дальнейшем технологии Больших данных стали использоваться в таких сферах, как разведка и контрразведка, военное дело, геостратегия, а также в информационном противоборстве [378].

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, 378].

4.13.3. Средства прогнозирования на основе технологий «Больших данных»

Еще одним направлением эффективного применения технологий Больших данных является прогноз развития социальных, политических, военных и экономических процессов. При этом к началу 2000-х годов специалисты, ведущие исследования в этой сфере, сформулировали по меньшей мере три фундаментальных положения [378]:

- 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 трем ключевым направлениям [378]:

- 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. Система Recorded Future базируется на трех основных элементах [378].

1. *Поисковая система третьего поколения*. Первое поколение поисковых систем (такие как Rambler, Yahoo и др.) просто искало те или иные слова в документах. Второе поколение поисковых систем (таких как Google) вело не только поиск по словам, но и учитывало в значительной степени связи между документами или сайтами. Третье поколение поисковых систем ищет не только объекты, соответствующие поисковым запросам, и не только связи между документами, но и взаимосвязи между объектами, их характеристиками и отношениями, содержащимися в различных документах [378].

2. *Разделение информационного поля на составляющие — события, мнения, реакции*. В Recorded Future выделено три класса сообщений. Первый — это сообщения о событиях. События — это длящиеся определенный, достаточно небольшой период времени устойчивые конфигурации, которые характеризуются единством времени, места, участников и т. п. К событиям Recorded Future относится то, что может быть интерпретировано как факты, то, что реально произошло или происходит в данный момент. Второй — это мнения. К мнениям относятся любые сообщения относительно прошлых, настоящих или будущих событий, высказанные в авторитетных источниках либо авторитетными людьми. В системе есть специальные алгоритмы, которые позволяют для каждой области выделить большую выборку таких источников и персон. Наконец, третий — это реакции. Здесь принимаются во внимание любые спонтан-

ные реакции людей на те или иные ожидаемые события, зафиксированные в различного рода текстовых сообщениях. Не обязательно, чтобы эти сообщения были из авторитетных источников. Главное — чтобы они имели отношение к событиям и мнениям, так или иначе рассматриваемым и высказываемым в авторитетных источниках. Такое разделение на три сегмента информационного поля, как выяснилось, позволяет достаточно хорошо как улавливать господствующие тенденции и опережающим образом реагировать на их изменения, так и выявлять слабые сигналы [378].

3. *Рассмотрение Интернета как огромной распределенной сетевой базы неструктурированных данных*. Recorded Future использует поисковик, работающий в сегментированном информационном пространстве в масштабе огромной сетевой базы данных. В сетевой базе данных разные объекты и их характеристики связаны друг с другом прямыми, обратными и опосредованными связями. Соответственно, такой подход позволяет выявлять не только явные и очевидные связи, но и вести так называемый латентный анализ, т. е. получать неочевидные, а иногда даже и абсолютно не предполагаемые связи и отношения. К тому же обрабатывать огромное количество информации в алгоритмическом режиме. То есть оперировать информационными массивами, непосильными для непосредственной обработки человеком [378].

В настоящее время Recorded Future используется в трех сферах: государственной разведке и безопасности, в бизнесе и в финансах для разработки инвестиционных стратегий [378].

Другим ярким примером прогностических систем нового поколения является система Quid. Эта система создана известным американским программистом и разработчиком Ш. Горли на деньги П. Тиля, чья разведывательная программа Palantir является давно и эффективно используемым средством американского разведывательного сообщества [378].

Система Quid занимается прежде всего научно-техническим прогнозированием, а также поиском тех ниш, которые могут дать максимальный эффект с точки зрения развития технологий в любых сферах, включая сферу вооружения. Одновременно система может быть использована для выявления «технологических дыр» в потенциале любой страны мира. В качестве материала для прогнозирования программа использует патентные Большие данные, т. е. миллионы файлов, входящих в патентные базы по всем странам мира, а также информацию из научно-технических, технологических журналов и средств массовой информации. Система Quid обнаруживает незаполненные технологические ниши, и именно эти пустые места оказываются точками роста, где появляются наиболее эффективные и одновременно наиболее прибыльные технические и технологические решения. С 2012 г. пользователями этой системы стали ведущие американские корпорации, разведывательные и военные структуры [378].

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 всё тех же Больших данных позволяют говорить о соз-

дании принципиально нового вида информационного оружия, а именно — прогностических средств. Этот вид оружия может быть использован как обеспечивающий механизм для разработки и применения традиционных вооружений.

4.13.4. Средства манипуляции и формирования поведения 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 целевая социальная группа действовала бы необходимым, заранее предопределенным образом. В работе [379] 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 [378].

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 [378].

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 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 неспособны 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» [378].

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 высокопроизводительных технических средств обработки, технологиях Больших данных и достижениях объективной психологии [378].

4.14. Перспективные технологии информационного противоборства в технической сфере (на основе анализа проектов DARPA)

Разработка новых способов и средств информационного противоборства в технической сфере требует существенного научно-технического задела во многих областях фундаментальной и прикладной науки. Тенденции перспективных исследований, проводимых в интересах совершенствования систем способов и средств информационного противоборства, можно оценить путем анализа проектов, выполняемых Агентством передовых оборонных исследовательских проектов Министерства обороны США — DARPA. Ниже представлена краткая характеристика проектов DARPA за 2015 г., которые напрямую или опосредованно ориентированны на формирование научно-технического задела в области информационного противоборства в технической сфере.

4.14.1. Технологии активных информационно-технических воздействий

Программа превентивной киберзащиты — Active Cyber Defense (ACD). 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].

Обход блокировок в сети — Safer Warfighter Computing (SAFER). Программа SAFER предусматривает создание пакета утилит, который позволит об-

ходить 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].

Информационно-технические средства проведения кибератак — Logan. Программа Logan обеспечит для ВС возможность расширить способности проведения компьютерных атак. Разработанные технические средства позволят разрушать и ослаблять информационные системы противника [234].

Управление кибервойной в режиме реального времени — 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].

4.14.2. Технологии информационной безопасности

Транспарентные вычисления — Transparent Computing. В рамках программы разрабатываются технологии, позволяющие осуществлять более эффективную политику безопасности в распределенных системах. Масштаб и сложность современных информационных систем скрывают связи между событиями, связанными с безопасностью, в результате чего работа по обнаружению атак и аномалий приходится на специализированную 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].

Поиск и понимание анклавов в программном обеспечении — Mining and Understanding Software Enclaves (MUSE). 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 вычислительные возможности в таких областях, как обработка графов, лечение компьютерных вирусов, анализ ссылок, анализ больших данных [234].

Автоматический программный анализ в интересах обеспечения кибербезопасности — Automated Program Analysis for Cybersecurity (APAC).

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].

Программа по созданию надежной защиты военной техники от кибератак — High Assurance Cyber Military Systems (HACMS). 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].

«Чистый» сетевой компьютер — Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH). Программа CRASH направлена на реализацию компьютерных систем, которые 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 привилегий. 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].

Активная проверка прав доступа — 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].

Интегрированные системы киберанализа — Integrated Cyber Analysis System (ICAS). 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].

Подтверждение аутентичности электронных компонентов — Supply Chain Hardware Intercepts for Electronics Defense (SHIELD). В последние 2 года на оборудовании, использующемся в ВС, было выявлено более 1 млн электронных деталей и компонентов сомнительного качества и подлинности. 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 процесс производства [234].

Защита киберфизических систем — Protecting Cyber Physical Systems (PCPS). В последнее время получили развитие киберфизические 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, противодействие атакам типа «имитация соединения» (спуфинг) и «отказ в обслуживании» [234].

Активно-реактивные кибернетические системы — Active-Reactive Cyber Systems (ARCS). 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].

Адаптивный информационный доступ и контроль — Adaptable Information Access and Control (AIAC). 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 технологиях, которые ограничивают обмен информацией между коммерческими предприятиями и правительственными учреждениями. Программа AIAC ориентирована на создание технологий многоуровневой безопасности, избирательного управления доступом и подсистем 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 в военной сферах [234].

Соревнование автоматических систем в обнаружении и исправлении уязвимостей нулевого уровня — Cyber Grand Challenge (CGC). В рамках соревнований участники должны создать системы для тестирования ПО, выявления уязвимостей, генерации патчей и установки их на компьютеры в сети. Все эти задачи должны выполняться полностью в автоматическом режиме. Цель 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].

Сетевая защита — 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. Кроме того, 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].

Безопасные распределенные динамические вычисления — Secure Distributed Dynamic Computing (SDDC). 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 ВС и поддержки принятия тактических решений на поле боя [234].

4.14.3. Технологии радиотехники

Защита беспроводных сетей — Wireless Network Defense. В настоящее время беспроводные сети используются всё 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].

4.14.4. Технологии электроники

Самоуничтожающиеся микросхемы — Vanishing Programmable Resources (VAPR). 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 характеристикам; кроме того, она должна уметь самоуничтожаться при заранее заданных условиях по команде извне или при попадании в заданное окружение [234].

Кортикальный процессор — 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. Существующие вычислительные подходы в подавляющем большинстве ресурсоемки и способны извлечь лишь ограниченную часть полезной информации из больших объемов данных. Современный машинный интеллект плохо распознаёт 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].

Разнообразные методы интеграции разнородных электронных систем — Diverse & Accessible Heterogeneous Integration (DAHI). Характеристики электронных микросистем играют жизненно важную роль в широком перечне боевых и обеспечивающих систем, стоящих на вооружении Минобороны. Именно они обеспечивают технологические преимущества над противником в сферах, связанных с выскоскоростной обработкой информации. 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 программы DAHI проводятся исследования по поиску новых методов и технологий, позволяющих комплексировать электронные микросистемы различного назначения и материалов изготовления в единой микросхеме [234].

4.14.5. Вычислительные системы

Нетрадиционная обработка сигналов для интеллектуального использования данных — Unconventional Processing of Signals for Intelligent Data Exploitation (UPSIDE). 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 система, реализующая «мягкие» вычисления, с более низким энергопотреблением, чем сравнимые с ней по вычислительной мощности традиционные компьютеры [234].

Технологии вероятностного программирования для самообучающихся машин — Probabilistic Programming for Advancing Machine Learning (PPAML). 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, 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 сетей [234].

Высокоэффективные встраиваемые вычислительные системы — Power Efficiency Revolution For Embedded Computing Technologies (PERFECT). 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 Гфлопс/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].

Создание защищенной облачной инфраструктуры, обеспечивающей сетевую поддержку военных операций — Mission-oriented Resilient Clouds (MRC). 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].

Быстрая разработка программного обеспечения за счет использования двоичных логических элементов — Rapid Software Development using Binary Components (RAPID). 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 ПО на устаревших и более не поддерживаемых разработчиком операционных системах. Данный проект направлен на решение этой проблемы [234].

Технология интеграции системных архитектур — System of Systems Architecture, Technology Development, and Demonstration. Программа SSATDD нацелена на поиск оптимальных путей интеграции системных архитектур различных программных сред в единую универсальную среду для ее эффективного использования в многокомпонентных информационно-коммуникационных системах [234].

4.14.6. Технологии обработки информации и анализа данных

Big Mechanism. 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].

Симбиоз человека и машины — Human and Computer Symbiosis (HCS). Программа направлена на разработку компьютерной технологии для поиска и использования источников информации. Технология HCS позволит компьютерам определять, в какой момент они будут испытывать потребность в необходимой информации, составлять и отправлять тексты с вопросами к экспертам, объединяться с ними и извлекать знания из их ответов. Приобретая знания и встраивая их в современные экспертные системы, компьютеры будут специализироваться и сами станут 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 случаях потребуется математическая формализация, рисунок или другая формулировка [234].

Виртуальный вычислительный интеллект — Cyber Computational Intelligence (CCI). Программа CCI 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 производительность сетей в условиях кибератак, а также восстанавливать их работоспособность после нападения [234].

Глубокий анализ и фильтрация текстовых материалов — Deep Exploration and Filtering of Text (DEFT). 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].

Глобальная количественная аналитика — 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].

Поиск в Интернете — Memex. В рамках программы Memex 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 пред-

метно-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].

Обработка больших данных — XDATA. В рамках программы XDATA разрабатываются вычислительные методы и программные инструменты анализа больших объемов данных, как «полуструктурированных», 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 программного обеспечения для обработки больших объемов данных в сроки, заданные требованиями оборонных проектов [234].

Система автоматизированного контент-анализа изображений и мультимедиа — Visual Media Reasoning (VMR). 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].

Доказательства агрессии — Battlefield Evidence. На сегодняшний день основной объем работы по экспертизе инцидентов информационной безопасности 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 медиа-материалы 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 проведения последующих оперативных мероприятий [234].

4.14.7. Технологии разведки, наблюдения и целеуказания

Адаптивные низкобюджетные сенсоры — Adaptable Low Cost Sensors (ADAPT). Программа ADAPT 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].

Автоматизированная система помощи аналитикам за счет комплексирования датчиков различных разведывательных платформ — Insight. Сегодня аналитики разведывательных служб страдают от избытка информации. 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 интеллекта ограничивает возможности операторов, а также затрудняет разбор и понимание сложных данных. Программа Insight предусматривает создание автоматизированной системы помощи аналитикам путем комплексирования датчиков различных платформ, в частности за счет разработки системы эксплуатации и управления ресурсами (E&RM) разведывательной службы нового поколения [234].

Глобальная система сбора информации, наблюдения и разведки — Worldwide Intelligence Surveillance and Reconnaissance (WISR). 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-реконструкции событий. Методы WISR также могут быть использованы для отслеживания культурных и социальных изменений при подготовке к вводу на территорию экспедиционных войск [234].

5. Информационное противоборство в психологической сфере

В настоящее время теория информационного противоборства в психологической сфере достаточно широко и глубоко исследована. Ведущие отечественные ученые, такие как С.Г. Кара-Мурза [20], Г.В. Грачёв [26, 33], В.М. Щекотихин [32], С.Н. Бухарин, В.В. Цыганов [34, 35], С.А. Модестов [37], И.Н. Панарин [52, 53], В.А. Лисичкин, Л.А. Шелепин [54], А.В. Манойло [71, 72, 318], Г.Г. Почепцов [73, 74, 272], С.П. Расторгуев [75, 76, 79, 277], Д.А. Новиков, А.Г. Чхартишвили [77, 78], Д.А. Губанов [77], А.Г. Караяни [80, 400], Д.А. Волкогонов [81], Н.Л. Волковский [83], В.А. Минаев, А.С. Овчинский, С.В. Скрыль, С.Н. Тростянский [85], В.Ф. Прокофьев [303], В.П. Шейнов [315], В.А. Баришполец [390], Л.В. Воронцова, Д.Б. Фролов [402], В.Г. Крысько [405], а также другие специалисты подробно исследовали различные аспекты информационного противоборства в психологической сфере. Ниже обзорно рассмотрены основные аспекты разработки и использования в современных военных конфликтах психологического и информационно-психологического оружия. При этом более подробно отдельные аспекты этой тематики представлены в вышеуказанных работах.

5.1. Основы информационно-психологического противоборства

5.1.1. Информационно-психологическое противоборство, понятие информационной и психологической войны

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 [388].

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 [388].

В настоящее время руководством США проведение мероприятий по информационно-психологическому воздействию на военно-политическое руко-

водство и общественное мнение различных стран, на мировое сообщество в целом возводится в статус основного содержания подготовки к военным действиям [388].

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 [400]:

- 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 [400]:

- 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 [400].

При этом в качестве сторон могут выступать как государства, так и неформальные объединения, например, террористические, религиозные или преступные группировки.

Такая война включает следующие направления деятельности [400]:

- 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 [400]:

- средства информационно-технического оружия;
- средства подавления информационных систем противника, вхождения в них в целях воздействия на циркулирующую информацию;
- средства пропагандистского вмешательства.

Более подробно анализ понятия «информационная война» представлен в подразделе 3.3 «Основные термины и определения информационного противоборства».

Психологическая война — борьба между государствами и их вооруженными силами за достижение превосходства в психологической и духовной сферах, а также 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.

В рамках психологической войны следует выделить следующие направления [400]:

- мобилизация и оптимизация моральных и психологических сил нации и вооруженных сил в интересах решения военных задач;
- защита населения своей страны и ее вооруженных сил от разлагающего информационно-психологического влияния противника (психологическое противодействие; психологическое прикрытие; контрпропаганда; психологическая защита);
- психологическое воздействие на войска и население противника в целях их дезориентации, деморализации и дезорганизации (психологическая борьба);
- влияние на взгляды, настроения, поведение дружественных и нейтральных аудиторий (стран, социальных групп, вооруженных формирований) в направлении, благоприятном для достижения победы над противником.

Задачи психологической войны [400]:

- противодействие и защита своих войск от психологических операций противника;
- психологическая борьба (воздействие на войска противника и население враждебных, дружественных и нейтральных государств, т. е. то, что зарубежными специалистами квалифицируется как психологические операции).

Рассматривая атакующие аспекты информационно-психологического противоборства, можно сформировать 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 [388].

Задачи информационно-психологического противоборства в мирное время и угрожаемый период, решение которых обеспечивает достижение ее цели [388]:

- 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 на-

зываемых «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 [388].

Области ведения информационно-психологического противоборства государств [392]:
- *географическое* — установление контроля над территорией посредством поощрения сепаратистских движений и террористической активности в различных формах на территории противника, вовлечение противника в конфликты малой интенсивности, а также организация смен власти, волнений народных масс и «цветных» революций;
- *экономическое* — навязывание противнику кабальных кредитов, введение эмбарго, организация экономических санкций и провокаций;
- *идеологическое* — формирование у людей заданного мировоззрения — обобщенной системы взглядов на окружающий мир, место и роль в нём человека, на отношение людей к объективной реальности и друг к другу, а также соответствующих этому идеалов и убеждений, принципов познания и деятельности, ценностных ориентаций;
- *информационное* — использование клеветы, искажения информации, подмена понятий, внесение ментальных вирусов и мифологем в созна-

ние населения противника, а также организация других информационно-психологических операций через СМИ или сеть Интернет.

5.1.2. Психологические операции

В настоящее время в странах НАТО весь комплекс мер информационно-психологического воздействия на войска и население противника обозначается термином «психологические операции» (ПсО) [400].

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, впитывает в себя всё, 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 [400].

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 [400].

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 [400].

Еще одним определением психологической операции является следующее.

Психологическая операция — главный элемент содержания психологической войны. Ее проведение предполагает использование на практике в условиях вооруженной борьбы сложной совокупности согласованных, скоординированных и взаимосвязанных по целям, задачам, месту и времени, объектам и процедурам видов, форм, способов и приемов психологического воздействия [405].

Разовые мероприятия психологической войны представляют собой кратковременные целенаправленные действия специальных подразделений или

отдельных специалистов, которые отличаются ограниченным характером и осуществляются в ограниченных (локальных) масштабах [405].

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 [405].

Психологические операции состоят из политических, военных, экономических, дипломатических и собственно информационно-психологических мероприятий, направленных на конкретные группы населения и войск противника с целью внедрения чуждых им 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 или дополняют повторное ее использование. Они осуществляются в рамках государственной политики, а их военная и прикладная стороны согласовываются и координируются с деятельностью соответствующих правительственных учреждений [405].

Рис. 5.1. Классификация психологических операций [405]

Психологические операции бывают различных видов, которые, в свою очередь, классифицируют по срокам, условиям осуществления, направленности — рис. 5.1.

1. По срокам осуществления и ориентированности на уровни военного управления психологические операции можно классифицировать на [405]:

- стратегические;
- оперативные;
- тактические.

Стратегические (долгосрочные) психологические операции имеют глобальный характер и осуществляются в течение длительного периода времени (продолжительностью от месяца до нескольких лет). Эти операции обычно имеют выраженный политический характер. Как правило, они представляют собой информационно-пропагандистские кампании, объектом которых может выступать вся мировая общественность, включая, разумеется, население своей страны. Достаточно часто главной целью стратегической операции является подготовка общественного мнения к прямому вооруженному вмешательству. Для ее проведения используются политическая, финансово-экономическая и дипломатическая изоляция государства-противника, широко привлекаются спецслужбы, влиятельные лица в самых различных сферах и на всех уровнях вплоть до первых руководителей страны [405].

Оперативные (среднесрочные) психологические операции осуществляются в поддержку войны в целом или крупномасштабных боевых действий. С началом войны устанавливается монополия на всю информацию, поступающую из зоны боев. При этом информация оттуда преподносится таким образом, чтобы хотя бы на первом этапе создавалось выгодное впечатление внутри страны и за рубежом о деятельности военно-политических кругов [405].

Тактические (краткосрочные) психологические операции, проводимые в поддержку боевых действий частей и соединений своих войск. Объектом таких операций обычно является противостоящая группировка войск противника. Основное психологическое воздействие в их ходе направлено, как правило, на разжигание национально-этнических, конфессиональных (религиозных), социально-политических и других противоречий, деморализацию различных групп войск противника, их дезинформацию [405].

2. По времени осуществления психологические операции классифицируются следующим образом [405]:

- проводимые в мирное время (в угрожающий период);
- проводимые в военное время;
- проводимые в ходе миротворческой деятельности.

Психологические операции, проводимые в мирное время (угрожающий период), — это аналог стратегических психологических операций. Разница лишь в том, что они носят менее глобальный характер и ориентированы преимущественно на население государства-противника, его союзников и дружественных ему стран [405].

Психологические операции, проводимые в военное время, отличаются прежде всего максимальной широтой спектра применяемых видов, методов, способов и приемов психологического воздействия, разнообразием и наибольшей концентрацией его средств, опорой на широкое использование психогенных факторов. Кроме того, эти операции, в свою очередь, делятся на подвиды: проводимые в обороне, в наступлении, в тылу противника и своем тылу, в ходе деятельности войск специального назначения [405].

Психологические операции в ходе миротворческой деятельности проводятся в интересах предотвращения военных конфликтов или для их прекра-

щения. Как правило, эти операции носят открытый характер и должны санкционироваться ООН.

3. По направленности психологические операции классифицируются следующим образом [405]:

- направленные против гражданского населения;
- направленные против войск противника;
- направленные против командования противника;
- направленные на введение противника в заблуждение;
- направленные на содействие оппозиционным силам и диссидентским движениям;
- направленные на осуществление культурной экспансии и диверсий;
- консолидирующие психологические операции.

Психологические операции, направленные против гражданского населения. Применяемое в ходе них психологическое воздействие, объектом которого является население какой-либо страны, может осуществляться «мягко», т. е. гуманными средствами с целью вызвать положительное отношение к своей стране и своим войскам, и «жестко» — с использованием всего арсенала способов и приемов влияния на общественное сознание людей с целью обмана, введения в заблуждение. Эти операции являются прелюдией и дополнением вооруженной борьбы [405].

Психологические операции, направленные против войск противника. Психологическое воздействие в ходе данных операций ориентировано преимущественно на «прокручивание» в сознании военнослужащих противника различных вариантов двух традиционных тем [405]:

- акцентирование страха быть убитым или раненым, остаться калекой на всю жизнь;
- разжигание ненависти тех, кто на переднем крае, по отношению к тем, кто в тылу, и наоборот.

Психологические операции, направленные против командования противника. Они преследуют цель дезориентации командного состава противника, внушения ему мысли о неизбежности поражения, нарушения его самообладания и на этой основе — побуждения к действиям, наносящим урон своим войскам [405].

Психологические операции по введению противника в заблуждение. Они являются весьма распространенной формой как пропагандистских, так и военных акций в ходе вооруженной борьбы [405].

Психологические операции по содействию оппозиционным силам и диссидентским движениям. Они проводятся как в мирное, так и в военное время. Психологическое воздействие, осуществляемое в ходе них, направлено на создание благоприятных условий, оказание моральной и другой поддержки оппозиционным силам и диссидентским элементам, находящимся на территории противника. Кроме того, подразделения психологической войны используют и для прямого управления действиями этих объектов, направленными на срыв военных и других усилий противника [405].

Психологические операции по осуществлению культурной экспансии и диверсий. Многие государства сознательно стремятся распространять свои «культурные» идеалы и принципы среди населения других стран, что в конечном итоге, с одной стороны, приводит к установлению моральной и нравственной зависимости вторых от первых, с другой — способствует нарушению устоявшихся культурно-этических представлений в обществе, приводит к деградации национального сознания. По этой причине многие народы всерьез озабочены масштабами вторжения в их национальную культуру западной (преимущественно американской) массовой культуры [405].

Консолидирующие психологические операции проводятся в интересах психологического воздействия на население нейтральных и дружественных стран, а также на население своего государства. Психологические операции в нейтральных странах преследуют цель побудить их лояльно относиться (активно поддерживать) к странам-союзницам, выступающим против реального или потенциального противника. Задачи психологических операций по отношению к населению дружественных стран состоят в завоевании его доверия и поддержке его морального духа, а также в устранении страха, предотвращении паники и создания общественного мнения, способствующего добровольному принятию установленных властями ограничений и мер контроля, вызванных борьбой с противником. Консолидирующие психологические операции среди населения своего государства направлены на завоевание поддержки с его стороны, обеспечение положительного восприятия им непопулярных мер правительства, а также неизбежного ограничения (в условиях военного времени) прав и свобод личности. Еще одна важная задача таких операций — предотвращение выступлений антиправительственных сил, так называемой «пятой колонны», способной создать помехи действиям своих войск и дестабилизировать обстановку в тылу [405].

Основные принципы подготовки и применения психологических операций [405]:

- подготовка психологических операций начинается заблаговременно, скрытно, тщательно, с учетом индивидуальных и социально-психологических особенностей объектов воздействия;
- психологические операции планируют и проводят с учетом выявленных слабых мест в морально-психологическом состоянии населения и личного состава войск противника, с учетом особенностей военно-политической и оперативной обстановки, имеющихся сил и средств;
- соответствующие начальники органов психологической войны лично отвечают за проведение и эффективность психологических операций, а также за использование имеющихся в их распоряжении сил и средств;
- психологические операции различных видов проводят по единому плану, согласовывают между собой, а также с боевыми действиями войск;
- все силы и средства психологических операций надо использовать массированно, комплексно и разнообразно.

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 [405].

Мероприятия психологических операций классифицируются следующим образом [405].

- *Мероприятия по снижению морального духа населения и военнослужащих противника.* В ходе них в течение длительного периода времени осуществляется эффективное психологическое воздействие, а очень часто — ничем не прикрытое информационное давление с целью деморализации гражданского населения и войск противника, утраты ими веры в собственные силы, в компетентность военно-политического руководства страны. Эти мероприятия очень широко распространены, в настоящее время они стали элементом не только психологической войны, но также повседневной политики, находящей свое выражение в экономической и дипломатических областях.
- *Мероприятия по подрыву боеспособности подразделений и частей противника.* Это психологическое воздействие, направленное на введение противника в заблуждение относительно военного потенциала и боевых возможностей противоположной стороны, пропаганда преимуществ своей военной техники и оружия, разъяснение причин поражений и больших потерь, осуществляемые совместно с другими военными и специальными акциями. Они значительно снижают боеспособность личного состава противника.
- *Мероприятия по побуждению противника к переходу на нашу сторону.* Личный состав конкретных частей и подразделений противника, ведущих боевые действия длительное время, и потому измотанных, истощенных, несущих серьезные боевые потери, переносящих серьезное психологическое воздействие, а также необстрелянные военнослужащие, только что переброшенные в район боевых действий и по этой причине оказавшиеся в экстремальных условиях, являются удобным объектом психологического воздействия, результатом которого часто бывают массовое дезертирство или самовольное оставление фронтовой полосы, симуляция, сдача в плен.

Основные задачи психологических операций [400]:

- убеждение общественного мнения в правильности, необходимости военного вмешательства;
- воздействие на военно-политическое руководство противника и его союзников с целью заставить их отказаться или воздержаться от вступления в войну;
- поддержка оппозиции, сил сопротивления, расовых, этнических, религиозных и других противоречий внутри страны-противника, подрыв доверия к руководству страны;

- руководство и содействие диссидентским элементам, взаимодействие с силами, ведущими борьбу в подполье;
- воздействие на население дружественных стран;
- содействие развитию доброжелательности населения нейтральных стран;
- подрыв морального духа, создание обстановки неуверенности и беспокойства среди личного состава армии противника, снижение его боеспособности;
- проведение аналитической работы по вскрытию уязвимых мест противника, подготовка и доведение до командиров тактического звена, а также групп и лиц, выполняющих задачи в районе боевых действий, соответствующей информации;
- оказание содействия в захвате населенных пунктов противника путем предъявления ультиматума и передачи призывов к капитуляции;
- оказание помощи командованию в осуществлении контроля за враждебно настроенным населением в зоне боевых действий;
- противодействие психологическим операциям противника и подрывным элементам;
- прогнозирование степени психологического воздействия на людей боевых действий.

Как видно, решение перечисленных задач должно обеспечить достижение морально-психологического превосходства своих войск над войсками противника [400].

Сам термин «психологические операции» указывает на то, что для достижения целей подрывной деятельности широко привлекаются выводы психологической науки и что они направляется в первую очередь на изменение психологических состояний противника [400].

Таким образом, психология как наука в рамках психологических операций решает следующие задачи [400]:

- 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 [400]:

- 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».

Эффекты, которые широко применяются в психологических операциях [400]:

- эффект первичности;
- эффект авторитета;
- эффект «голос пророка»;
- эффект повторения;
- эффекты возложения ответственности;
- другие эффекты.

Более подробная информация об использовании этих эффектов представлена в работе [400].

Одной из сравнительно новых теорий развития информационных операций, активно обсуждаемых специалистами, является концепция «стратегические коммуникации», реализующаяся в США. Под этой концепцией понимается комплекс мероприятий по целенаправленному воздействию на военно-политическое руководство, различные общественно-политические силы, международные организации — т. е. на так называемую целевую аудиторию других стран, — предпринимаемых различными правительственными и неправительственными учреждениями и организациями США, а также их союзниками [95].

Цель «стратегических коммуникаций» — убеждение или принуждение целевой аудитории к принятию решений или совершению действий, направленных на формирование, сохранение или развитие благоприятных условий для продвижения американских национальных интересов [95].

В США к основным структурам, реализующим эту сравнительно новую концепцию, относятся Госдепартамент, Министерство обороны, Объединенные (боевые) командования вооруженных сил, Агентство по международному развитию, неправительственные организации [95].

Следует отметить, что в американском Госдепартаменте понятие «стратегические коммуникации» подменяют термином «публичная дипломатия». Однако «публичная дипломатия» на самом деле является составным компонентом стратегических коммуникаций. Она заключается в преднамеренном создании в представлениях целевой аудитории идеального имиджа США, американских идеалов и образа жизни посредством проведения информационных кампаний, акций экономической, технической и гуманитарной помощи [95].

Военным ведомством США в качестве основных определены следующие **основные принципы концепции «стратегических коммуникаций»** [95]:

- *квалифицированное руководство* — подразумевает четкое представление руководителями целей и задач концепции;
- *правдоподобие* — предусматривает действия, восприятие и объяснение которых должны вызывать доверие у целевой аудитории;
- *доступность* — учет особенностей культуры, образа жизни, истории и общественного строя целевой аудитории, лингвистического, исторического, религиозного, природного и других объективных факторов;
- *диалог* — по мнению специалистов в области психологических операций, в ходе многостороннего обмена мнениями способствует взаимопониманию и установлению доверительных отношений;
- *масштабность* — предусматривает отсутствие временных или пространственных ограничений на информационно-психологическое воздействие;
- *согласованность* — подразумевает согласованные, интегрированные на всех уровнях в единую систему действия по единому замыслу и плану на всех уровнях иерархии как по «вертикали» — от тактического до стратегического, так и по «горизонтали» — в пределах одного уровня;
- *целенаправленность* — направленность информационно-психологического воздействия на получение конкретного заданного результата;
- *оперативность* — по мнению специалистов, принцип оперативности при реализации концепции в перспективе может дать стратегический эффект;
- *непрерывность* — предполагает непрерывный процесс, для успешного осуществления которого необходимо наличие постоянной обратной связи между планированием и действиями, с одной стороны, и анализом с оценкой результатов этих действий — с другой. В идеальном случае он должен проходить быстрее, чем у противника.

Реализация концепции «стратегических коммуникаций» включает в себя следующие этапы [95]:

- уточнение политических целей;
- определение целевой аудитории и желаемого поведенческого эффекта объекта воздействия;
- всесторонний анализ аудитории и определение идеологических установок;
- формулирование основных целей для подготовленных сообщений и планируемых акций;
- согласование информационного воздействия, организованных акций и политических действий;
- синхронизация действий носителей информации по времени;
- планирование первоочередных мероприятий и контрмер;
- оценка результатов и корректировка планов.

В качестве средств информационно-психологического воздействия, согласно концепции «стратегических коммуникаций», могут выступать радио, наземное, кабельное и спутниковое телевидение, печать, Интернет, потоковое видео, мобильные телефоны, общественные организации, распространяемые слухи, а также войсковые учения, демонстрация силы, визиты, конференции, различные рабочие семинары, научные и военные обмены, ассоциации выпускников, организация и проведение восстановительных работ, торговля и гуманитарная помощь, благодаря которым военно-политическое руководство США пытается вызвать симпатии к своей стране и к ее вооруженным силам или страх перед их мощью [95].

Таким образом, СМИ и телекоммуникации, открытые информационные ресурсы, глобальная сеть Интернет уже сейчас активно используются Министерством обороны и Госдепартаментом США не только для мониторинга угроз национальной безопасности страны, изучения общественного мнения, позиции государств в отношении США, но и в целях манипулирования общественным мнением, дезинформации и введения в заблуждение военно-политического руководства других стран, принуждения его к принятию выгодных Вашингтону и его союзникам решений [95].

5.1.3. Информационно-психологические воздействия

Основным способом ведения информационно-психологического противоборства является использование информационно-психологических воздействий.

Информационно-психологическое воздействие — информационное, психотронное 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 [390].

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 [390].

В зависимости от преследуемых целей информационно-психологическое воздействие, как правило, осуществляется на конкретные сферы индивидуального, группового, массового и общественного сознания [390]:

- мотивационную (убеждения, ценностные ориентации, влечения, желания), когда надо оказать влияние на людей для побуждения их определенным действиям;
- познавательную (ощущения, восприятия, представления, воображение, память и мышление), когда необходимо изменить в нужную сторону представления, характер восприятия вновь поступающей информации и в итоге — «картину мира» человека;
- эмоциональную (эмоции, чувства, настроения, волевые процессы), когда под прицелом находятся внутренние переживания и волевая активность людей;
- коммуникативную (общение и взаимоотношения, взаимодействие, межличностное восприятие) с целью создания социально-психологического комфорта или дискомфорта, побуждения людей сотрудничать либо конфликтовать с окружающими.

Информационно-психологическое воздействие может осуществляться с помощью различных методов (приемов, форм, методик) и средств, бóльшая часть из которых, непрерывно развиваясь и совершенствуясь, превратились 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 [390].

Области организации информационно-психологического воздействия на психику человека, групповое, массовое и общественное сознание включает в себя [390]:

- объекты информационно-психологического воздействия;
- субъекты, воздействующие на эти объекты;
- коммуникацию между субъектами и объектами информационно-психологического воздействия;
- средства и методы информационно-психологического воздействия.

Объекты информационно-психологического воздействия [390]:

- личность как гражданин, активный социальный субъект, в том числе конкретные представители органов государственной власти и управления, вооруженных сил, органов правопорядка и безопасности, работники государственных и негосударственных организаций, учреждений и предприятий, деятельность которых имеет или может иметь важные социальные последствия;
- система формирования и функционирования духовной сферы, общественного сознания и общественного мнения, в том числе: системы образования и подготовки кадров; системы распространения социально значимой информации; системы распространения социокультурных ценностей и т. п.;
- социальные группы и объединения людей как компоненты социальной структуры общества, обладающие групповым сознанием, в том числе политические, профессиональные, национально-этнические, демографические, религиозные, конкретных регионов и другие;
- органы власти, государственного и военного управления;
- органы представительной и исполнительной власти субъектов Федерации и местного самоуправления;
- общественные и политические организации, общественно-политические движения, объединения граждан на различной основе и т. п.;
- силовые министерства и ведомства;
- население страны в целом как социально-историческая общность людей, обладающая своим общественным сознанием;
- государство и общество, выступающие как объекты информационно-психологических операций других государств, особенно в период международных конфликтов, кризисов и вооруженных столкновений.

Субъекты информационно-психологического воздействия на отдельного человека (его психику, сознание, организм), группу людей, население регионов и страны в целом [390]:

- государственные и правительственные учреждения (в том числе иностранные), правовые и силовые (военные) организации;
- общественные организации — политические, религиозные, культурные, национально-этнические и т. п. (в том числе зарубежные);
- учреждения здравоохранения;
- финансово-экономические, коммерческие и торговые организации (в том числе зарубежные);
- криминальные структуры (в том числе международные);
- микрогруппы (по месту работы, учебы, службы, жительства, друзья, семья, случайные знакомые, толпа и т. п.);
- отдельные субъекты (граждане).

Субъект информационно-психологического воздействия по своему местоположению может быть [390]:

- внутренним, т. е. принадлежать стране, на объекты которой осуществляется воздействие;
- внешним (зарубежным).

Внешними субъектами информационно-психологического воздействия могут выступать отдельные государства, их политические, экономические, военные, разведывательные и информационные структуры [390].

Самым главным средством достижения политических целей государствами в недалеком будущем может стать воздействие на психологию противника — индивидуальное, массовое, групповое и общественное сознание с целью разрушения государственных и общественных институтов, провоцирования массовых беспорядков, деградации общества, развала государства [390].

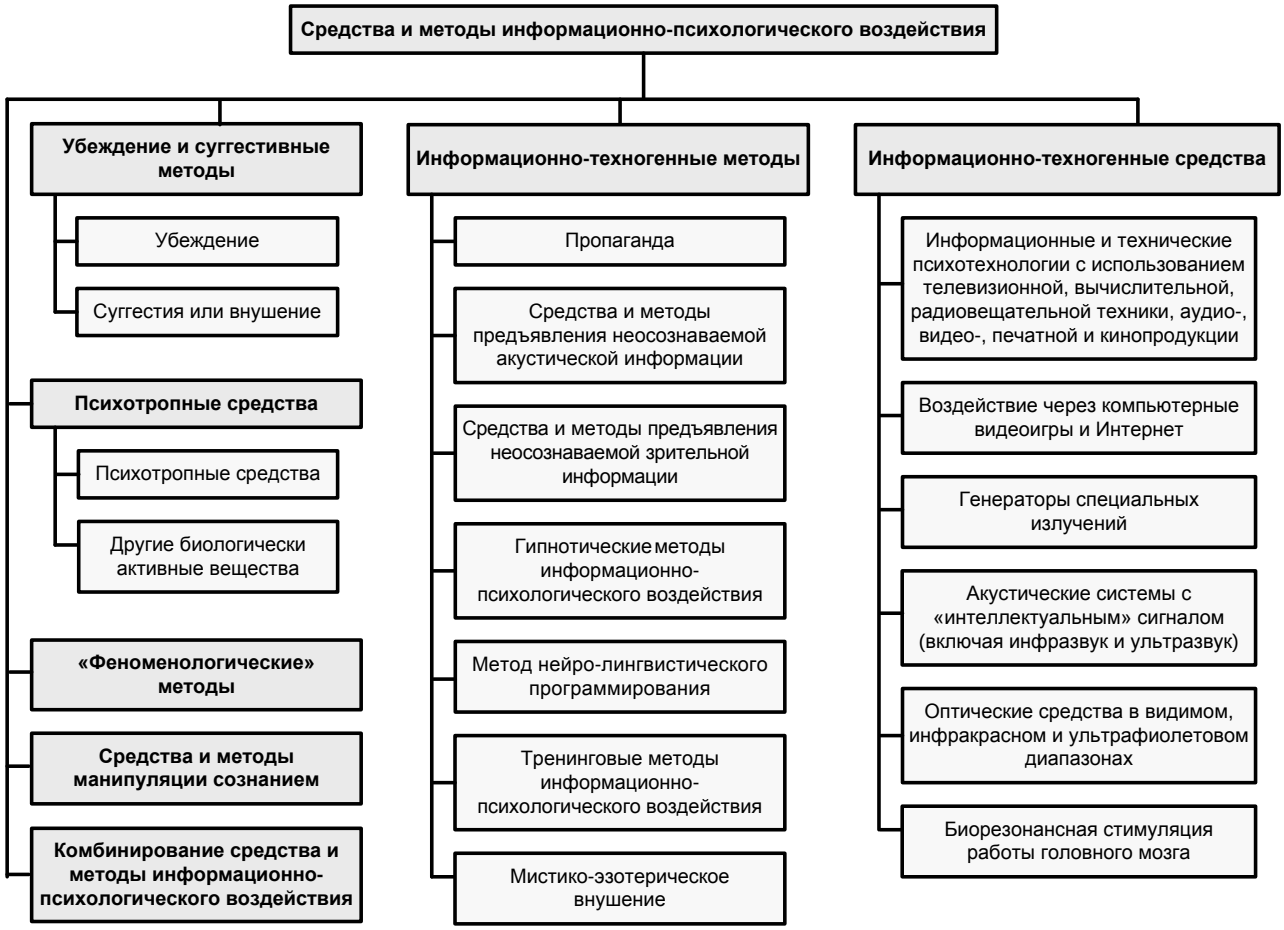


Рис. 5.2. Классификация средств и методов информационно-психологического воздействия [390, 391]

Средства и методы информационно-психологического воздействия могут быть классифицированы с точки зрения физической сущности, принципов и механизмов воздействия (рис. 5.2) [390, 391].

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 нём человека, на отношение людей к объективной реальности и друг к 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*, основанные 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, сло-

весные внушения, регуляция мышечного тонуса, управление ритмом дыхания.

- *Мистико-эзотерическое внушение*.

3. Информационно-техногенные средства и методы информационно-психологического воздействия, к которым относятся:

- 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, оказывающие преимущественно 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 путем применения методов 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 всех вышеуказанных в классификации средств и методов информационно-психологического воздействия рассмотрено в работе [390].

Выделяют три этапа при информационно-психологическом воздействии [405]:

- *операциональный*, когда субъектом осуществляется информационно-психологическое воздействие на объект;
- *процессуальный*, когда имеет место принятие (одобрение) или неприятие (неодобрение) данного воздействия объектом;
- *заключительный*, когда проявляются ответные реакции как следствие перестройки психики объекта воздействия.

Перестройка психики под влиянием информационно-психологического воздействия может быть различной как по широте, так и по временной устойчивости. По первому критерию различают парциальные изменения, т. е. изменения какого-нибудь одного психологического качества (например, мнения человека о конкретном явлении), и более общие изменения психики, т. е. изменения ряда психологических качеств индивида (или группы). По второму критерию изменения могут быть кратковременными и длительными [405].

Применение информационно-психологического воздействия в боевой обстановке имеет свои особенности [405]:

- 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 [405].

5.2. Психологическое оружие

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 [400].

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 [400].

К основным разновидностям психологического оружия можно отнести (таблица 5.1) [400, 401, 403]:

- информационно-психологическое оружие;
- лингвистическое оружие;
- психотронное оружие;
- психофизическое оружие;
- психотропное оружие;
- сомато-психологическое оружие.

Таблица 5.1 — Классификация типов психологического оружия [400, 401]

Тип оружия	**Характеристика**
Информационно-психологическое оружие	Информация со средствами ее производства, презентации и распространения, структурированная для обеспечения ее некритического восприятия в качестве побудителя и регулятора поведения объектами воздействия
Лингвистическое оружие	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 оружие	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 оружие	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 оружие	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
Сомато-психологическое оружие	Технические устройства, химические составы и биологические рецептуры, вызывающие изменения в соматическом состоянии и физической активности людей и на этой основе стимулирующие развитие астенических психических состояний и импульсивных моделей поведения

Вариант классификации психологического оружия представлен на рис. 5.3.

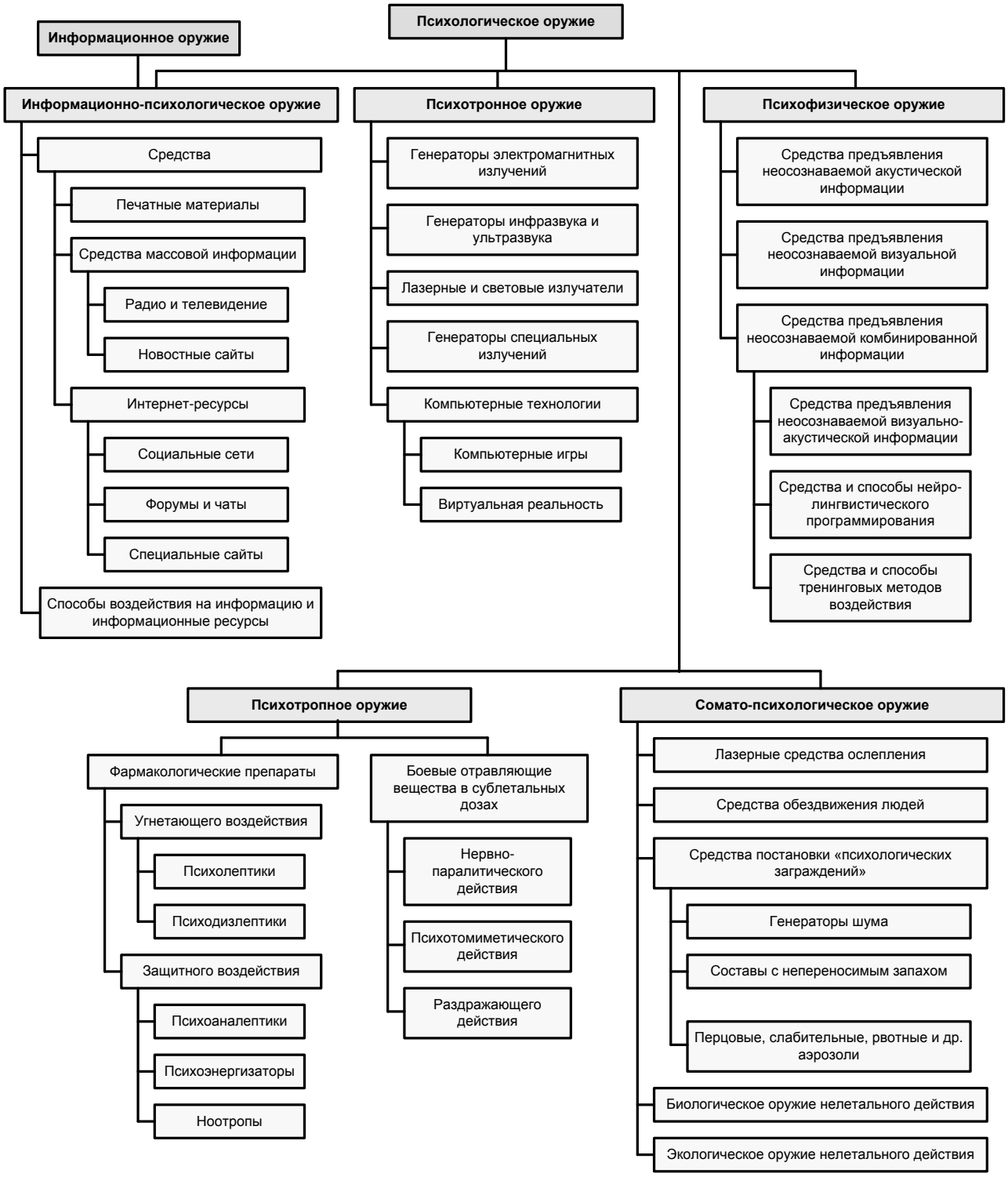


Рис. 5.3. Классификация психологического оружия

Задачи, решаемые психологическим оружием как комплексом средств преднамеренного и организованного воздействия на психику и поведение военнослужащих на поле боя [400]:

- 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 состояния, 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 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.

Рассмотрим основные типы психологического оружия более подробно. При этом отдельно выделим информационно-психологическое оружие, так как в настоящее время при осуществлении ПсО именно средства, основанные на производстве, презентации и распространении информации рассматриваются в качестве приоритетных при достижении военных целей. А для их разработки и практического применения привлекаются значительные материально-технические ресурсы, известные ученые, политики, деятели культуры и искусства, высококлассные военные специалисты.

5.2.1. 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 посредством использования их при заключении международных договоров, написании текстов деклараций, законов и т. д. [399, 401].

Например, в текстах Договоров об ограничении систем ПРО США и СССР от 1972 г., о ликвидации РСМД от 1987 г., об ограничении и сокращении стратегических вооружений от 1991 г. можно легко обнаружить следы применения такого лингвистического оружия. Так, наличие всего только одной маловразумительной фразы «РЛС с большими фазированными системами предупреждения о пуске баллистических ракет стратегического назначения должны размещаться только на национальной территории, по ее периферии и быть обращенными вовне» позволило США иметь две РЛС за рубежом своей национальной территории, в Гренландии и Великобритании, а одну — в центре

полуострова Аляска на расстоянии 800–1000 км от береговой линии Мирового океана. В то же время СССР в свое время был вынужден ликвидировать свою РЛС подобного типа, построенную под Красноярском — в 800 км от китайской границы [399].

5.2.2. Психотронное оружие

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 [399, 400]:

- генераторы электромагнитных излучений;
- генераторы инфразвука и ультразвука;
- лазерные и световые излучатели;
- генераторы специальных излучений;
- компьютерные технологии и др.

Рассмотрим особенности воздействия этих типов психотронного оружия на человека.

5.2.2.1. Генераторы электромагнитных излучений

В настоящее время СВЧ- и КВЧ-излучение широко используется в физиотерапии. Обобщение опыта физиотерапевтического лечения свидетельствует, что длительное неинтенсивное или кратковременное интенсивное (при уровнях более 10^{-4} Вт/см^2) воздействие коротковолновым ЭМИ вызывает стадию тревоги в течение нескольких суток, а затем — компенсацию и адаптацию, сопровождающиеся структурными изменениями организма. При длительном интенсивном воздействии наблюдаются стадия тревоги, стадия истощения и возникновение патологии организма. Также следует отметить, что при длительном неинтенсивном воздействии возможны генетические изменения организма, которые могут вызвать нежелательные последствия в будущих поколениях. Кроме того, необходимо добавить, что длительное (в течение многих лет) воздействие низкоэнергетических СВЧ- и КВЧ-излучений способно вызвать существенное снижение и даже полное подавление иммунитета. Это может привести к распространению различных болезней, эпидемий и вымиранию больших масс населения [390].

Кроме того, СВЧ-излучение может быть использовано для биорезонансной стимуляции работы головного мозга. Как известно, основную роль в психической деятельности человека, саморегуляции его поведения играет головной мозг. Поэтому большими потенциальными возможностями психологического воздействия обладают биорезонансные системы, способные обеспечить манипуляцию тонкими механизмами работы мозга и нервной системы [390].

Биорезонансная стимуляция работы головного мозга человека основывается на том, что в зависимости от психического состояния человека интегральное функционирование головного мозга характеризуется электрической активностью в определенных диапазонах частот (биоритмом). При том или ином

состоянии организма (умственная или физическая нагрузка, эмоциональное напряжение, сон и т. п.) регистрируются биоритмы определенной частоты и характера. Электрофизиологическое исследование головного мозга человека позволяет выделить пять основных частотных характеристик его работы (биоритмов), определяющих пять ведущих режимов работы мозга [390]:

- бета-ритм (β-ритм, частота 13–35 Гц, амплитуда 5–30 мкВ) соответствует состоянию активного поведения, стрессовому состоянию, состоянию тревоги;
- альфа-ритм (α-ритм, частота 8–12 Гц, амплитуда 30–70 мкВ) является характерным для состояния спокойного бодрствования;
- тета-ритм (θ-ритм, частота 4–7 Гц, амплитуда 10–150 мкВ) наблюдается при глубокой релаксации, медитации, гипнотическом трансе, состоянии сосредоточенного внимания;
- дельта-ритм (δ-ритм, частота 1–3 Гц, амплитуда 10–300 мкВ) имеет место во время глубокого сна, а также при коме;
- гамма-ритм (γ-ритм, частота 35–120 Гц, амплитуда до 25 мкВ) наблюдается при эмоциональном и творческом подъеме.

Воздействуя определенным образом на волны какого-либо биоритма головного мозга с помощью резонансного эффекта, можно переводить его в доминирующее состояние и тем самым влиять на сознание человека.

В настоящее время существует ряд приборов физиотерапии, использующих принцип биорезонансного воздействия, которые позволяют скорректировать нарушение биоритмов головного мозга (т. е. вызвать смену биоритма) и обеспечить состояние комфортного самочувствия. В основе этих приборов лежит воздействие на головной мозг электрическими, электромагнитными, световыми, звуковыми и т. п. волнами с низкими частотами и ничтожно малой амплитудой, близкими к собственным биоритмам головного мозга и усиливающими амплитуду их колебаний, т. е. вступающих в резонанс. Таким образом, оказалось возможным навязывание мозгу человека ритмов, характерных для разных состояний сознания. Синхронизируя тем или иным способом воздействие (например, с помощью прибора низкоинтенсивного электромагнитного излучения, совпадающего с биоритмами мозга) с деятельностью мозга на нужной частоте, можно вызвать смену биоритма, т. е. преднамеренно изменить состояние сознания человека, его настроение, эмоциональный фон, погрузить его в то состояние сознания, которое имеет место, например, во сне, под гипнозом, при стрессе и т. п. Очевидно, что информационно-психологическое воздействие с помощью указанных приборов может носить не только положительный, но и скрытый деструктивный характер [390].

5.2.2.2. Генераторы инфразвука и ультразвука

Генераторы инфразвука и ультразвука используют эффекты деструктивного воздействия на психику и организм человека инфразвука (частота колебаний ниже 16 Гц) и ультразвуковых колебаний (свыше 20 кГц) [390].

Исследования показали, что при уровне интенсивности от 95 до 150 дБ и более инфразвук может вызывать у людей неприятные субъективные ощуще-

ния и многочисленные реактивные изменения, к числу которых следует отнести изменения в центральной нервной, сердечно-сосудистой и дыхательной системах, а также в вестибулярном анализаторе. Эти изменения способны также возбуждать у людей состояние ужаса и паники, вызывать потерю самоконтроля. Частота же между 6 и 9 Гц вообще чрезвычайно опасна. Теоретически такой инфразвук достаточной мощности может разорвать внутренние органы. Объясняется это тем, что организм человека является источником собственного (эндогенного) низкочастотного акустического поля. Частотный диапазон генерируемых различными органами человека низкочастотных акустических колебаний лежит в широких пределах: от 0,5 до 100 Гц — диапазон инфразвука и низких звуковых колебаний. В качестве примера приведем собственные частоты колебаний для некоторых органов человека: биоритмы головного мозга — 1–40 Гц; глаза — 40–100 Гц; вестибулярный аппарат — 0,5–13 Гц; сердце — 4–6 Гц; желудок — 2–3 Гц; кишечник —2–4 Гц; брюшная полость — 4–8 Гц; почки — 6–8 Гц; руки — 2–5 Гц; позвоночник — 6 Гц. Существование упругих волн обнаружено также и на клеточном уровне. Так как диапазон колебаний инфразвука совпадает с собственной частотой колебаний отдельных органов человека, то в результате этого из-за резонанса могут возникнуть тяжелые последствия [390].

Ультразвуковые колебания не ощущаются человеком, но даже малая интенсивность ультразвуковых колебаний низкочастотного диапазона (20–30 кГц) значительно влияет на психику человека: вызывает головную боль, головокружение, быструю утомляемость, расстройства зрения и дыхания. Ультразвук низкочастотного диапазона может использоваться для угнетения иммунной системы и подавления воли, оказания вредного воздействия на сердечно-сосудистую, нервную и эндокринную системы, нарушения обмена веществ. Под длительным действием интенсивного ультразвука температура тела человека повышается, пульс становится реже, замедляются рефлекторные реакции на внешние раздражения [390].

5.2.2.3. Лазерные излучатели

Сравнительно новым средством психологического воздействия, которое может найти широкое применение в практике ПсО, являются генераторы голографических изображений в атмосфере, которые создаются лазерным излучением. По данным зарубежных СМИ, в ряде стран разрабатываются проекты установки на действующих космических аппаратах лазерно-световых комплексов, способных проецировать на облака различные изображения. Облака являются прекрасным естественным экраном, расположенным на высоте 60–80 км от поверхности Земли. Спроецированное на них изображение будет отчетливо видно на удалении 100–150 км. Первая попытка проекции на облака была предпринята еще в 1915 г. Тогда на одном из участков российско-германского фронта над позициями наших войск с помощью прожекторов на облака проецировалось изображение Богоматери. Очевидцы этих событий рассказывали о сильном психологическом эффекте этой акции. Другой случай подобного рода отмечен 1 февраля 1993 г. в Сомали, когда группа морских пехотинцев США,

действовавших вблизи г. Могадишо, заметила в клубах пыли и песка изображение лица Иисуса Христа размером примерно 150×150 м. Описывая свое психическое состояние, пехотинцы говорили, что они плакали, стоя на коленях, и в течение длительного времени не смогли продолжить выполнение боевой задачи. В настоящее время в США планируется создавать на небе голографические изображения исламских проповедников, которые «с небес» будут советовать своим единоверцам прекращать сопротивление, сдаваться на милость противника или возвращаться домой. Таким образом, неожиданное созерцание образов святых, чудовищ (драконов, ящеров, мутантов и др.) или иных незнакомых явлений может оказать сильное психологическое воздействие на людей, причем как мобилизующего, так и деморализующего порядка [399, 400].

5.2.2.4. Световые излучатели

Успешное практическое использование воздействия мелькающего света для деморализации психики людей проводилось английскими войсками при разгоне демонстраций в Северной Ирландии. Для этой цели использовался источник мелькающего света с частотой 10–20 Гц. Было установлено, что наиболее сильное воздействие оказывает излучение с частотой следования импульсов 15 Гц, лежащее в красной области спектра и имеющее весьма малую интенсивность (почти невидимый свет) с крутым передним фронтом импульсов. Под влиянием облучения у 5% облучаемых людей возникли эпилептические припадки, а 25% облученных чувствовали недомогание, тошноту, головокружение, затруднения при быстрых движениях и даже теряли сознание. Установлено, что при воздействии мелькающего света клетки мозга перестраивают частоты своих колебаний в соответствии с частотой вспышек света. Такое навязывание ритма может влиять на состояние психики, умственную деятельность и самочувствие человека [390].

Еще одним примером психотронного воздействия на психику на основе воздействия мелькающего света стала массовая «телевизионная эпидемия», вспыхнувшая в Японии 1 декабря 1997 г. после демонстрации очередной серии популярного мультфильма «Покемон». Более 700 детей были доставлены в больницу с симптомами эпилепсии. По мнению психиатров, массовый недуг вызвали эпизоды, сопровождавшиеся многочисленными ослепительными разноцветными вспышками. Медики доказали, что мерцание красного цвета с частотой от 10 до 30 Гц вызвало сначала раздражение глазных нервов и частичный спазм сосудов головного мозга, а потом — потерю сознания, судороги и даже спазматическое прекращение дыхания (удушье) [399].

5.2.2.5. Компьютерные технологии

Высшим достижением компьютерных технологий в области психологического воздействия на сегодня является виртуальная реальность, которая позволяет прорываться в глубинные пласты человеческой психики, подменять отдельные элементы самообраза в нужном направлении и в конечном итоге — эффективно манипулировать сознанием виртуального пользователя. Быстрое развитие компьютерных технологий виртуальной реальности создает угрозу

появления техногенного наркотика — более сильного и «гибкого» для управления сознанием человека, чем любые известные фармакологические наркотические препараты [399].

С помощью компьютерных игр можно трансформировать психику играющего человека в заданном программно-поддерживаемом направлении. При этом в мозгу играющего возникают следы-фантомы: сновидения, страхи, эпилептические припадки, кошмары. Многие дети после подобных игр попали в больницы и получили серьезные психологические травмы [399].

5.2.3. 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 [399].

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 (настроения, здоровья). В предельном варианте человек, испытавший психофизическое воздействие, превращается в «зомби», который безотказно выполняет заложенную в него программу. Психофизические средства основаны на суггестии [399].

Суггестия (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 [399].

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 внушаемого 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 следующие типы психофизического оружия, основанные на различных видах суггестии [390, 399]:

- средства предъявления неосознаваемой акустической информации;
- средства предъявления неосознаваемой визуальной информации;
- средства предъявления неосознаваемой комбинированной информации.

Рассмотрим эти средства более подробно.

5.2.3.1. Средства предъявления неосознаваемой акустической информации

Возможности по предъявлению неосознаваемой акустической информации крайне ограничены. Основным приемом здесь является предъявление акустических стимулов ниже порога слышимости на фоне более громкой маски-

рующей информации. В этом случае очень слабые нижнепороговые стимулы не воспринимаются сознанием, глубоко внедряясь в подсознание [390].

Известны способы предъявления неосознаваемой акустической информации на очень тихом уровне звучания (уровень громкости составляет 9–30% от фонового звука и более), путем спектральной маскировки речевого сигнала музыкой или шумом. К настоящему времени разработано несколько способов маскировки речи. Например, на аудиозапись очень тихой речи сверху накладывается очень громкая музыка. На осознаваемом уровне речь практически не слышна, но тем не менее она воспринимается акустической сенсорной системой головного мозга, записывается в памяти и оказывает свое воздействие на жизненные установки личности. Таким образом, человек слушает музыку или шум прибоя в комнате отдыха, следит за диалогами персонажей фильма и не подозревает, что в них содержатся не воспринимаемые сознанием, но всегда фиксируемые подсознанием команды, заставляющие его впоследствии делать то, что предписано [390].

Возможно воздействие с использованием технических средств и методов неосознаваемой аудиосуггестии, основанное на алгоритмах предварительной обработки слышимой речевой информации, воспринимаемой человеком. Сегодня разработан ряд компьютерных программ, которые разными способами трансформируют слышимую речь на неосознаваемый уровень восприятия. В такой информации неявно могут присутствовать корректирующие «речевые формулы» вербальной суггестии, трансформированные для бессознательного восприятия через слуховой сенсорный канал на подпороговом уровне [390].

Кроме того, современные компьютерные технологии также позволяют преобразовать любой музыкальный файл таким образом, чтобы при его прослушивании возникали необходимые психологические эффекты: звук, закодированный под альфа-ритм, поможет расслабиться; звук, закодированный под дельта-ритм, поможет уснуть, под тета-ритм — достигнуть состояния медитации [390].

5.2.3.2. Средства 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 [390].

Основными параметрами зрительного восприятия являются положение, форма и движение объекта, их цвет и яркость. Первые три параметра характеризуют зрительное восприятие пространства, в процессе которого происходит интеграция соответствующей информации, полученной от слуховой, вестибулярной, кожно-мышечной и других систем. Восприятие цвета может сводиться к оценке светлоты или видимой яркости, цветового тона или собственно цвета, а также насыщенности [390].

Существуют известные методы предъявления неосознаваемой информации в зрительной сфере. Это методы различной маскировки — прямой, обратной, метаконтраста и др. Все методы зрительной суггестии основаны на временных соотношениях между маскируемым и маскирующим стимулами [390].

Имеются и интенсивно разрабатываются более совершенные методы неосознаваемого предъявления зрительной информации. Такие методы основываются на «диспаратном» предъявлении, т. е. каждый кадр видеоинформации содержит только часть суггестивного образа, недостаточную для его осознания. При последовательном предъявлении ряда таких кадров происходит суммирование частей образной суггестии на неосознаваемом уровне. Понятно, что при просмотре кадров в режиме стоп-кадр суггестивную информацию увидеть невозможно — она формируется только в мозгу субъекта. Данный подход укладывается в принципы нейросемантического гипертекста, которые используются в методах нейролингвистического программирования [390].

Интересным примером средств психофизического оружия, основанного на предъявлении неосознаваемой зрительной информации, являются так называемые «биовирусы», которые распространяются в компьютерных системах и несут в себе подсознательные сообщения.

Первым таким биовирусом был «rave on» швейцарского программиста Ю. Фурхта, который маскировался под ошибочно работающую программу просмотра постскриптовских файлов. При запуске программа сообщала, что не может работать с данным режимом монитора, после чего монитор начинал мерцать. Частота мерцания монитора была подобрана так, что действовала гипнотически. Один кадр на каждые 60 передавал подсознательное сообщение «Беснуйся! Радуйся и не огорчайся!» [399].

Другой биовирус — V666 — использует классическую идею 25-го кадра. Он выводит на экран монитора строго определенную комбинацию световых пятен, вводящих оператора в гипнотическое состояние, при котором он теряет сознательный контроль над собой. Этот же вирус разрушительно влияет на физиологию оператора. По расчетам создателей вируса, подсознательное восприятие нового изображения должно вызывать изменение сердечной деятельности: ее ритма и силы сокращений. В результате появляются резкие перепады артериального давления в малом круге кровообращения, которые приводят к перегрузке сосудов головного мозга человека [399].

Информационно-психологическое воздействие как на сознание, так и на подсознание человека могут оказывать различного рода изображения. Под их воздействием у него возникают определенные интеллектуальные, эмоциональные и другие ассоциации. Эти ассоциации в последующем можно эффективно использовать для формирования вполне определенных убеждений и ценностных ориентаций [390].

Одним из самых сильных средств воздействия на психику человека является цвет, который способен порождать как положительные, так и отрицательные ассоциации. Вполне определенное эмоциональное воздействие на человека оказывают различные сочетания (комбинации) цветов. Одни сочетания цветов порождают гармоничное внутреннее состояние человека, другие вызывают

внутреннюю напряженность и внешнюю конфликтность. Установлено также, что цветовое воздействие обладает прямым физиологическим влиянием вплоть до биохимического, причем разные цветовые раздражители вызывают различные изменения в организме. Настроение, поведение, самочувствие, работоспособность тесно связаны с цветовой гаммой окружающей среды — цветом ландшафта, интерьера помещений, одежды. Однако цвета имеют смысл не сами по себе, а в различных сочетаниях (цветовая гамма). При этом сочетание цветов выбирается в зависимости от того, какое воздействие должно быть оказано. Так, психологи считают, что позитивные («радостные») эмоции вызывают белый цвет на зеленом, зеленый на желтом, желтый на зеленом, желтый на белом фоне. Напротив, негативные («грустные») эмоции вызывают синий цвет на черном, фиолетовый на черном, черный на синем фоне. Наиболее агрессивные — красный цвет на черном, коричневый на синем, фиолетовый на черном, синий на черном, синий на коричневом, зеленый на фиолетовом фоне [390].

Организованные специальным образом цветодинамические воздействия могут явиться эффективным приемом модификации сознания, поведения и физического состояния человека. Использование правильно подобранной цветовой гаммы позволяет создавать нужный эмоциональный фон для положительного информационно-психологического воздействия или, наоборот, вызывать диссонанс эмоционального восприятия. Эти приемы широко используются при психотерапии с помощью слайдов и видеофильмов [390].

5.2.3.3. Средства предъявления неосознаваемой комбинированной информации

Эффект психологического воздействия существенно усиливается при комбинированном использовании различных типов внушения. Наиболее известным и простым примером такой кооперации и воздействия является комплексное использование акустической и визуальной суггестии. Доказано на практике, что неосознаваемая акустическая суггестия, сопровождающая зрительную осознанную информацию, может модулировать отношение человека к последней. Например, при показе человеческого лица испытуемые оценивали его как образ человека хорошего или плохого в зависимости от установки, формируемой у них с помощью одновременно идущей неосознаваемой акустической суггестии (спокойной, радостной, тревожной, воинственной и т. д. музыки) [399].

Наиболее сложной формой предъявления неосознаваемой комбинированной информации является нейролингвистическое программирование (НЛП), достигаемое путем долгого и кропотливого подбора «ключа» к подсознанию человека. В качестве такого «ключа» используется специально подобранный текст (так называемый нейросемантический гипертекст), содержащий наиболее значимые слова и фразы для внушаемого лица, значительной группы лиц, подразделения, региона. Память, сознание, подсознание любого человека рассматриваются специалистами в области НЛП как участки «карты». Карта выглядит как слабо структурированная смесь данных и программ поведения, представляющая собой личную модель мира. Она легко перепрограммируется после

ввода человека в специальные психологически-интерфейсные режимы. Наиболее вероятная область применения НЛП — средства массовой информации с ориентацией на определенный, хорошо изученный контингент населения, образование и медицина [399].

5.2.4. Психотропное оружие

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 [400].

Те группы психотропных веществ и составов, которые с наибольшей вероятностью могут быть привлечены для использования в ходе войны, приведены в таблице 5.2.

Таблица 5.2 — Психотропные средства, пригодные для использования в военных целях [400]

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 [400].

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.) [390].

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 [390].

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, поставляемыми населению. Всё больше товаров ввозится из-за рубежа. Многие психотропные средства могут скрыто вводиться в организм людей через эти товары, как через кожу, так и при вдыхании аэрозолей [390].

Исходя из свойств психотропных средств, можно представить их возможности при использовании для информационно-психологического воздействия на человека [390].

Во-первых, психотропные средства модифицируют психику человека, который в большинстве случаев остается работоспособным и продолжает принимать решения, неотражающие адекватно окружающую обстановку, несоответствующие реальности. Окружающим 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 осознаётся коллективом вообще. В этом случае коллектив не связывает свои неудачи и поражения с неправильным принятием решений и считает, что всё это произошло в силу каких-то иных причин [390].

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 поведении, поступках, действиях малых групп людей и в поведении больших социальных групп [390].

В-третьих, люди, на которых было произведено воздействие психотропными средствами, сохраняют свое соматическое (телесное) здоровье. Более того, модификация психики со временем, исчисляемым в неделях или месяцах, прекращается или автоматически, или с помощью направленного психотерапевтического воздействия [390].

Таким образом, использование психотропных средств вышло далеко за рамки психиатрической клиники. Они могут широко применяться для достижения определенных политических, экономических, военных и других целей.

5.2.5. Сомато-психологическое оружие

В основе сомато-психологического 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 [400].

Основные средства сомато-психологического оружия представлены в таблице 5.3 по данным из работы [400].

Таблица 5.3 — Основные средства сомато-психологического оружия [400]

Наименование оружия	**Краткая характеристика оружия**
Лазерное оружие	Лазерные генераторы и устройства, применяемые для временного ослепления военнослужащих войск противника
Средства обездвижения людей	Быстро затвердевающие 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 трудно переносимого шума, составы с непереносимым запахом, перцовые, слабительные, рвотные и др. 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 течение длительного времени погодно-климатических условий, крайне неблагоприятных для жизнедеятельности войск противника

Оружие сомато-психологической 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 [399].

Отдельные виды сомато-психологического 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 [400].

В качестве примера можно привести средство LRAD — устройство, испускающее 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 [391].

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 [400].

5.3. 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.

К основным средствам информационно-психологического оружия, получившим широкое распространение, можно отнести (рис. 5.4) [388, 400]:

- печатные материалы — листовки, плакаты, информационные бюллетени и др., средства их производства (полиграфическая база) и распространения;
- средства массовой информации — газеты, радио, телевидение, новостные сайты и агрегаторы новостей в сети Интернет;
- интернет-ресурсы: специально созданные сайты; социальные сети, форумы, чаты;
- когнитивное оружие.

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 [388].

Рис. 5.4. Классификация средств информационно-психологического оружия

Ниже средства информационно-психологического оружия и тенденции их развития рассмотрены более подробно.

5.3.1. Средства массовой информации

Средства массовой информации 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 литера-

тура, видеофильмы, щитовая реклама и реклама на транспорте, звукозаписи и видеозаписи и т. п. — словом, всё, с помощью чего можно воздействовать на массовую аудиторию. При этом, из всех этих СМИ наивысшей эффективностью обладает телевидение [388].

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 [388].

Особую опасность представляет просмотр телевидения 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 [388].

Не меньшую опасность телевидение оказывает на психику взрослых людей. Телевидение с его огромным потоком зрительной информации и 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 [388].

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 не ясен 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 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 [388].

При современном уровне развития СМИ становится возможной даже такая операция, как перенесение методов гипнотического внушения с отдельного человека на целые общества.

При этом процесс наведения гипнотического состояния на отдельное общество требует следующих этапов [399]:

- расслабить общество, т. е. внушать через средства массовой информации, что врагов нет, при этом обсуждать отдельные исторические периоды и интересы отдельных народностей (цель: общество как целое должно исчезнуть в качестве объекта сознания общества);
- заставить общество слушать только противника, не обращая внимания на какие-то иные мысли или ощущения; допустим, акцентировать внимание средств массовой информации исключительно на какой-то одной парадигме общественного развития, например западной, исключив любой другой опыт: Китай, Японию, мусульманский мир (цель: процесс загрузки общественного сознания и действие формирующих сил ослабляются);
- заставить общество не размышлять над тем, что говорит противник; для этого исключить из средств массовой информации серьезные аналитические исследования проблем (цель: способствовать торможению непрерывного потока мыслей);
- сосредоточить внимание общества на каком-то предмете помимо входного информационного потока, например внутренние катаклизмы, войны, акты террора (цель: подсистема защиты, ответственная за обработку входной информации, оказывается не в состоянии выполнять свою функцию и как бы расстраивается);
- постоянно внушать, что само общество становится лучше и лучше, что все окружающие относятся к нему лучше и лучше (цель: подобное внушение ослабляет историческую память и чувство самоидентификации, которыми характеризуется нормальное состояние общества);
- средства массовой информации одновременно должны убеждать членов общества, что возникшее состояние — это не совсем то, что должно быть (цель: создание пассивного состояния сознания, в котором сохраняется возможность зависимости от информационного воздействия противника).

5.3.2. Средства на основе интернет-ресурсов и социальных сетей

В интересах психологических операций всё активнее и масштабнее применяется электронные СМИ, а также глобальная компьютерная сеть Интернет. Диапазон использования сети Интернет весьма широк. Он предоставляет широкие возможности для оказания влияния на формирование общественного мне-

ния, 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, 406].

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 РЭБ.

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 органов 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 этого, 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 бóльшую 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 [388].

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 [388].

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 [388].

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 [388].

В настоящее время в США разработана программа Persona Management Software позволяющая манипулировать сознанием людей в социальных сетях. С помощью данной программы 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 этой программы можно также следить за общественным мнением и находить подлинные точки зрения, чтобы затем с помощью «фиктивных» людей проводить кампании по искажению этих точек зрения и дискредитации «реальных» людей [388].

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 [388].

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 г. 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 Twitter 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].

5.3.3. 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 [388].

В практическом применении ложные научные теории, парадигмы, концепции, стратегии превращаются в оружие огромной разрушительной силы, поражающее национальную науку и образование, государственное управление, экономику, оборону [388].

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 политическими и 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 [388].

5.4. Силы психологических операций (на примере ВС США)

Вооруженные силы практически всех развитых государств имеют в своем составе специальные структуры, отвечающие за информационно-психологическое воздействие на военнослужащих и население противника. В ФРГ такая структура представлена органами оперативной информации, в Великобритании и Италии — психологических операций, в Китае — пропаганды среди войск и населения противника [393].

Наиболее мощным аппаратом ведения психологических операций располагают США. Их высокая эффективность в значительной мере связана с тем вниманием, которое уделяется этому вопросу военно-политическим руководством и командованием страны, а также гибкой организационно-штатной структурой и самым современным техническим оснащением [393].

Военно-политическое руководство США неоднократно использовало силы и средства психологических операций в вооруженных конфликтах различной степени и интенсивности, а также в миротворческих операциях. По мнению американских военных специалистов, психологические операции являются частью системы боевого обеспечения и должны быть органично «встроены» в сетецентрическую систему ведения войны. Это позволит оперативно реагировать на изменение обстановки и увязывать ПсО с боевыми действиями, в ходе которых физическое уничтожение противника сопровождается

подавлением его морального духа, в результате чего победа достигается быстрее и с меньшими затратами сил и средств. [389, 393].

При возникновении чрезвычайных (кризисных) ситуаций, в которых задействованы ВС США, на базе 4-й группы ПсО в зависимости от масштабов конфликта, задач и потребностей войск (сил) создаются оперативные формирования, а также подразделения ПсО корпусной, дивизионной и бригадной поддержки и тактические команды [389].

В случае возникновения одновременно двух или более крупномасштабных конфликтов на базе резервных групп ПсО может быть сформирована оперативная группа ПсО. При необходимости она усиливается подразделениями ПсО других видов ВС и преобразовывается в объединенную оперативную группу ПсО. После официального объявления об окончании операции эта группа обычно расформировывается [389].

Оперативное формирование ПсО применяется в операциях меньшего масштаба. Как правило, это формирование, которое возглавляет командир одного из региональных батальонов ПсО, включает штаб, часть подразделений соответствующего регионального батальона ПсО, батальона подготовки и распространения информационных материалов и батальона ПсО (тактического). Основной упор в своей деятельности оперативное формирование ПсО делает на ведение печатной, устной и радиопропаганды с использованием штатных технических средств — мобильных типографий, радио- и звуковещательных станций [389].

Секция планирования ПсО используется в качестве временного штабного органа ПсО для усиления штаба объединенных ВС на ТВД или оперативной разработки плана ПсО и оценки обстановки в регионах (странах), где они заранее не планировались [389].

Оперативное формирование военно-информационной поддержки является подразделением быстрого развертывания, располагающим широкими возможностями по информационно-психологическому воздействию. Оно перебрасывается к месту назначения самолетами типа С-141 и обеспечивается компактными СВ- и УКВ-радиопередатчиками, телепередатчиком (1 кВт), мобильной полиграфической техникой, 3–6 звуковещательными станциями [389].

Подобные команды, в частности, регулярно направляются в страны Южной Америки для информационно-пропагандистской поддержки воинских контингентов США, местных армейских и полицейских формирований [389].

Если оперативная группа (формирование) и секция планирования ПсО отвечают за подготовку и проведение психологических операций на стратегическом и оперативном уровнях, то тактические психологические операции на уровне корпуса и ниже обычно проводятся батальонами и ротами ПсО [389].

Тактические психологические операции — это комплекс мероприятий, проводящихся непосредственно на линии соприкосновения с противником для оказания поддержки боевым частям. Они организуются и проводятся подразделениями ПсО корпусной, дивизионной и бригадной поддержки, а также звуковещательными командами [389].

Подразделение ПсО корпусной поддержки предназначено для организации и планирования ПсО в интересах корпуса и руководства действиями подчиненных формирований тактических ПсО [389].

Конкретный состав подразделения корпусной поддержки зависит от предназначения и задачи поддерживающего штаба корпуса. Как правило, подразделение корпусной поддержки состоит из командования батальона ПсО, оперативного отделения и отделения разведки, а также ряда офицеров других штабных специальностей. Подразделение дивизионной поддержки координирует свои действия с оперативной группой ПсО по вопросам подготовки и выпуска материалов информационно-психологического воздействия, так как имеет ограниченные возможности в этом плане [389].

Подразделение ПсО бригадной поддержки состоит из управления и трех-пяти звуковещательных команд. В зависимости от плана ПсО бригады эти команды могут находиться под контролем штаба бригады или придаваться батальонам [389].

В основе оперативной структуры формирований ПсО Вооруженных сил США лежит модульный принцип. В зависимости от обстановки и стоящих перед ними задач создаются соответствующие подразделения ПсО.

Существует 27 типов команд с различными функциями, которые разделены на 3 группы [389]:

- штабная группа управления
- оперативная группа;
- группа снабжения и обслуживания.

По мнению американских военных аналитиков, в ближайшей перспективе ПсО должны стать действенным средством оперативной доставки необходимой информации, подстроенной с точки зрения технических возможностей восприятия под предполагаемого противника в районе боевых действий ВС США. Они смогут достичь максимальной эффективности, если будут начинаться еще до начала конфликта и вестись как в ходе, так и после завершения активной фазы боевых действий. Проводимые в угрожаемый период ПсО будут способствовать формированию благоприятной для ВС США обстановки в регионе [389].

В будущем в ходе проведения тактических ПсО уменьшится роль обычных звуковещательных средств. Тактические группы ПсО уже широко используют новейшие электронные средства получения и передачи информации. Во избежание риска для жизни военнослужащих прекращено использование переносных звуковещательных станций. Вместо них звукопрограммы передаются по беспроводным сетям не на автоматические громкоговорители, а на базовые радиотрансляторы, смонтированные на наиболее защищенной бронированной технике (например, бронеавтомобили типа «Хамви») [389].

Основной задачей тактических групп ПсО станут сбор видеоматериалов и их отправка для дальнейшей обработки в специализированные центры по обработке соответствующих материалов и выпуску фильмов и видеороликов о ВС США в целях создания их положительного образа при работе с населением. При этом планируется активно использовать новейшие цифровые средства

коммуникации в режиме реального времени. Собранные материалы будут отсылаться напрямую в объединенный штаб ПсО и использоваться в телепередачах госдепартамента, транслируемых во всемирной сети Интернет. Для распространения данных материалов в мирное время будут заключаться контракты с местными СМИ [389].

Таким образом, несмотря на то, что в настоящее время органы ПсО в ВС США являются наиболее оснащенными и боеспособными среди аналогичных структур ВС других зарубежных стран, американское военно-политическое руководство продолжает предпринимать активные меры по дальнейшему повышению эффективности всей системы операций в целях достижения информационного психологического превосходства над противником [389].

В июне 2010 г. директивой министра обороны США наименование подразделений психологических операций PSYOP (Psychological Operations) было изменено на более нейтральное — «информационное обеспечение», или MISO (Military Information Support Operation). По замыслу командования, такое переименование связано с некоторой подозрительностью, зачастую проявляемой как за рубежом, так и внутри страны, к термину «психологические операции», что часто приводит к превратному толкованию задач, решаемых этой службой. Другими словами, введение нового термина отражает опасения американских специалистов в области информационно-психологического противоборства в недопонимании командирами на местах сути и содержания их деятельности [393].

Высокая эффективность подразделений ПсО Вооруженных сил США является результатом боевого опыта, полученного в ходе войн, вооруженных конфликтов и контртеррористических операций (Корея, Вьетнам, Гренада, Балканы, Колумбия, Филиппины, Афганистан, Ирак, Ливия и др.). Практически ни одна операция с участием ВС США не проходила без применения этих формирований [393].

Объединенное командование сил специальных операций ВС США постоянно работает над совершенствованием форм и методов психологического воздействия, отвечающих конкретной обстановке и условиям применения войск.

Например, столкнувшись с низкой эффективностью проведения обычных военных операций (на тактическом уровне) для стабилизации обстановки в Афганистане, американское командование решило добиваться своих целей не «огнем и мечом», а путем «завоевания сердец и умов» афганцев. Для этого были организованы мобильные группы гражданских специалистов, которые под охраной воинских подразделений занимались восстановлением коммуникаций и инфраструктуры, оказывали помощь местному населению и содействовали стабилизации обстановки в стране. Эти подразделения получили название «команды по восстановлению провинций». На разных этапах военной операции в каждую такую команду входили от 50 до 100 военнослужащих, а также около сотни гражданских экспертов и советников. Задачами этих команд были: обеспечение безопасности в регионах, восстановление и укрепление влияния центрального афганского правительства в провинциях, мониторинг обстановки и оказание содействия властям на местах в решении информационно-пропаган-

дистских и социально-экономических задач. Успех проведения этой операции доказал, что и на тактическом уровне использование подразделений ПсО может быть достаточно эффективным [393].

На стратегическом же уровне подразделения ПсО успешно действовали с самого начала операции «Свобода Ираку». В целях достижения ее поддержки мировым сообществом Пентагон основной упор сделал на целенаправленную работу с представителями СМИ [393].

Эксклюзивные права на освещение боевых действий были предоставлены мощным информационным медиа-компаниям — агентствам CNN и BBC. Кроме того, журналисты «прикреплялись» к подразделениям, участвовавшим в боевых действиях. В зону их ведения были направлены лучшие американские репортеры. Эффективность этого решения подтвердилась в первые дни операции, когда в сети Интернет можно было в режиме реального времени наблюдать кадры наступления коалиционных войск с телекамер, установленных на американских танках. Расчет делался на то, что «акулы пера», преодолевающие тяготы и лишения боевых действий вместе с солдатами, не смогут критически отозваться о своих «сослуживцах». Всего к боевым частям и подразделениям американской армии были «прикреплены» 662 журналиста, еще 95 находились в британских подразделениях. Эта новая форма участия журналистов в информационно-психологическом обеспечении, по оценкам западных специалистов, позволила добиться существенной поддержки боевых действий со стороны общественности стран коалиции [393].

Во втором десятилетии XXI века психологические операции, проводимые ВС США, вышли на качественно новый уровень. Наряду с такими традиционными методами, как печатная пропаганда, устная агитация, теле- и радиовещание, американские специалисты ПсО стали активно использовать современные технологии социальных сетей в Интернете (Египет, Ливия, Сирия). Это позволило значительно повысить степень эффективности информационно-психологического воздействия стратегического уровня [393].

За последние несколько лет в ВС США введены в действие десятки документов, в числе которых — новая редакция наставления КНШ ВС США JP 3-13.2 «Психологические операции» от 7 января 2010 г. В этом документе отражены взгляды американского военного руководства на подготовку и ведение ПсО в ходе совместных военных операций с участием государственных и негосударственных структур как в мирное, так и в военное время. Наставление представляет собой общее руководство для командующих крупными группировками войск (сил) ПсО, а также командиров соединений и частей в области организации и ведения психологических операций [393].

Согласно этому документу, Пентагон окончательно переходит к преимущественному использованию современных медиатехнологий распространения материалов информационно-психологического воздействия, в том числе в сети Интернет. Наряду с этим предусматривается тесное взаимодействие с гражданскими структурами, занимающимися организацией поддержания связей с общественностью. В число государственных ведомств, с которыми осуществляются координация и взаимодействие, входят: ЦРУ; Бюро по международным

информационным программам Госдепартамента США; Бюро международного вещания; Совет управляющих по вещанию, министерства торговли, внутренней безопасности, транспорта, энергетики и юстиции; Управление по борьбе с наркотиками и береговая охрана [393].

Психологические операции также могут осуществляться в рамках программ связи с общественностью, предусматривающих [2]:

- доведение «точной и своевременной информации» до целевых аудиторий и личного состава вооруженных сил, а также до иностранной общественности, содержания целей и задач военных компаний и операций,
- информирование заинтересованных аудиторий о касающихся их важнейших изменениях,
- обеспечение командованию возможности посредством СМИ довести до потенциального противника сведений о намерениях и возможностях вооруженных сил.

Кроме того, в интересах психологических операций осуществляются программы по работе с гражданским населением, трактующиеся как действия командиров по установлению и поддержанию отношений между подчиненными им войсками и гражданскими властями, организациями и местным населением в дружественных, нейтральных и враждебных районах развертывания формирований ВС [2].

Рассматривая средства реализации психологических операций, необходимо отметить высокую роль информационных агентств. Сами они, как правило, не занимаются передачей информации непосредственно ее конечным потребителям, а собирают информацию, обрабатывают ее и передают СМИ. На сегодняшний день информационные агентства являются главными инструментами оперативного сбора и передачи информации, а также средством реализации психологических операций [2].

Так, под непосредственным руководством Совета национальной безопасности США функционирует Информационное агентство Соединенных Штатов USIA, директор которого одновременно является главным советником президента страны по вопросам информации. Располагая штатом около 10 000 человек и выпуская информационные программы на 62 языках мира, USIA имеет более 200 своих отделений в 120 странах мира. Более 2000 сотрудников французского агентства «Франс-Пресс» работают в 13 отделениях во Франции и в 163 отделениях в различных регионах мира. Занимающее ведущее место на немецком информационном рынке германское агентство печати «ДПА» имеет свои бюро и корпункты в 80 странах, причем половину расходов на их содержание берёт на себя федеральное правительство [2].

Таким образом, в настоящее время мировые державы благодаря наличию соответствующей правовой базы, органов и средств формирования и реализации информационной политики располагают широкими и разнообразными возможностями для достижения своих политических и военных целей, защиты государственных интересов посредством влияния на общественное сознание как внутри страны, так и за рубежом.

5.5. 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.

5.5.1. 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 [394].

Согласно наставлению сухопутных войск США по проведению ПсО, способы распространения материалов печатной пропаганды подразделяются следующим образом [394]:

- наземный (распространение военнослужащими, в том числе силами специальных операций), местными жителями, пожелавшими сотрудничать с ними, агентами;
- воздушный (авиабомбы, авиационная тара, парашютные контейнеры, воздухоплавательные ЛА, разброс непосредственно экипажами ЛА);
- морской (плавучая тара);
- 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 [394].

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 [394].

5.5.1.1. Аэростаты

Состоящие на вооружении аппарата ПсО ВС США современные пропагандистские аэростаты последней разработки способны на высоте до 25 км преодолевать расстояние в 10 000 км и нести груз (листовки) массой до 180 кг. Их преимущество перед авиационными средствами доставки состоит прежде всего в том, что использование таких систем не несет опасности потери боевых машин, а также их экипажей и возможно даже при условии мощного противодействия со стороны сил ПВО противника. Более того, даже в случае расстрела аэростата истребителями ПВО происходят раскрытие контейнера с печатной продукцией и залистование территории противника [394].

Большинство современных аэростатов, применяемых для распространения печатных материалов информационно-психологического воздействия, было разработано в странах НАТО еще в период «холодной войны». Однако до сих пор на вооружении подразделений ПсО ВС США и других государств НАТО состоят аэростаты, именуемые «воздухоплавательными системами доставки листовок» (Balloon Delivery System), — модели J-100, 170F и J-9-10-300 [394].

Специальный аэростат J-100 предназначен для доставки 3 кг листовок на расстояние не более 400 км. Принцип его действия заключается в постепенном стравливании воздуха из баллона, за счет чего происходит ослабление фиксирующих строп и раскрытие контейнера с листовками [394].

Аэростат J-9-10-300 является модернизированной версией J-100. Он способен доставить груз листовок общей массой 4,5 кг на расстояние 400–1000 км. Его модель 170F (а также ее более поздняя модификация — 180F) представляет собой современную воздухоплавательную систему доставки листовок, имеющую большую дальность полета. Она предназначена для доставки примерно 40 кг печатных материалов информационно-пропагандистского воздействия (ИПВ) на расстояние до 2500 км [394].

Согласно положениям раздела FM 33-1-1 «Технические средства ПсО и порядок их применения» полевого устава сухопутных войск США, «помимо распространения листовок аэростаты применяются для доставки объектам ПсО продуктов, игрушек, наглядной агитации, предметов повседневного пользования и т. п. Предметы наглядной агитации, распространяемые в целях оказания необходимого психологического воздействия на противника, могут включать национальные флаги, а также исполненные в различной форме листовки-пропуска, содержащие инструкции и обеспечивающие безопасность перебеж-

чиков при пересечении линии фронта. Подразделения ПсО, решающие задачи дезинформации и введения противника в заблуждение, с помощью аэростатов могут забрасывать на его территорию такие предметы, как парашюты, продукты питания, военная амуниция и обмундирование, способные создать у противника иллюзию нахождения на его территории диверсионно-штурмовых и разведывательных групп» [394].

5.5.1.2. Авиационная тара

Использование специальной тары позволяет распространять листовки с помощью авиации, не нарушая воздушного пространства страны противника. ВС США, дислоцированные в Кореи, неоднократно забрасывали такую продукцию на территорию КНДР и даже в Пхеньян с самолетов, барражировавших на разных высотах над международными водами и демилитаризованной зоной, разделяющей два корейских государства. В интересах проведения ПсО, как правило, использовались тактические военно-транспортные самолеты C-130 Hercules, которые с высоты 7600–7800 м за один самолетовылет с помощью авиационной тары доставляли груз пропагандистского характера общей массой до 9 т [394].

В настоящее время некоторые американские военно-транспортные самолеты (например, C-130 Hercules), самолеты ССО (MC-130) и бомбардировщики (B-52 Stratofortress) специально переоборудованы для распространения листовок, в частности оснащены алюминиевыми отсеками, позволяющими производить автоматический сброс листовочной авиационной тары. Так, с ее помощью в период операции «Буря в пустыне» (Ирак, 1991 г.) было распространено более 20 000 листовок, а в ходе операции «Свобода Ирака» (2003 г.) — уже 13 271 700 листовок [394].

5.5.1.3. Агитационные (листовочные) авиабомбы

В настоящее время в ВС США основным боеприпасом такого типа, предназначенным для распространения печатных материалов ИПВ, является специальная агитационная (по терминологии НАТО — листовочная) авиабомба M129 двух модификаций — E1 и E2. Она была разработана еще в период войны во Вьетнаме и успешно применялась для решения задач информационного противоборства. Специальная авиабомба M129E1/E2 может перевозиться в бомбовом люке бомбардировщика либо на внешней подвеске истребителя-бомбардировщика или штурмовика. Она позволяет сбрасывать большое количество листовок непосредственно в район нахождения противника, обеспечивая высокую степень точности их попадания и минимальное рассеивание в результате движения воздушных потоков. Ее полезная нагрузка равна 50,3 кг. Авиабомба снаряжается 30 000 листовок размером 13,7×20,3 см, которые машинным способом скручиваются в семь (7,3 кг) рулонов. В ходе войны в Ираке в 2003 г. было использовано более 2000 авиабомб M129, с помощью которых удалось распространить 122,5 млн листовок [394].

В целом в настоящее время авиабомба M129E1/E2 признаётся специалистами ПсО ВС США морально устаревшей. В качестве альтернативы рассмат-

ривались авиационные кассетные бомбы CBU (Cluster bomb units), снятые с вооружения и хранящиеся в большом количестве на военных складах. Это обусловлено тем, что конструктивно они состоят из нескольких секций (кассет), которые могут нести как заряд взрывчатого вещества, так и листовки [394].

В качестве опытного образца американские специалисты взяли кассетную авиабомбу SUU-30B/B. Длина ее корпуса 2,33 м, диаметр 40,6 см. Основой SUU-30B/B является кассетная секция SUU-30, которая ранее снаряжалась боевым зарядом, а в настоящее время обеспечивает возможность распространения печатных материалов. С использованием этой кассетной секции была разработана листовочная (агитационная) кассетная бомба, получившая обозначение LBU-30 (LBU — Leaflet Bomb Unit — «листовочный авиационный боеприпас»). Первые испытания новой листовочной (агитационной) кассетной бомбы LBU-30, которая получила в ВВС США условное обозначение Seek Eagle, состоялись в 2000 г. на базе ВВС США Эглин (шт. Флорида). В ходе них истребитель-бомбардировщик F-16 осуществил успешный сброс авиабомбы LBU-30 с высоты 6 км. После этого специалисты ПсО ВВС США приняли решение о применении кассетной секции SUU-30 для модернизации и старых авиабомб M129. Это было обусловлено тем, что новый боеприпас не ограничивает тактико-технических возможностей боевых самолетов, привлекаемых для проведения ПсО [394].

Другим опытным образцом для переоборудования, исходя из интересов распространения печатных материалов, является кассетная бомба Mk20 Rockeye II, носителями которой могут быть и самолеты палубной авиации. Ее длина 2,1 м, диаметр 33 см. По принципу действия Rockeye II аналогична рассмотренной выше кассетной авиабомбе SUU-30B/B. Созданный на ее базе листовочный (агитационный) боеприпас получил обозначение PDU-5/B (PDU-PSYOP — Dispensing Unit, или Printed Data Unit, дословно — «боеприпас для распространения печатных материалов»). В его конструкции использована кассетная секция SUU-76C/B от Мк 20 Rockeye II. Первые испытания листовочной (агитационной) кассетной авиабомбы PDU-5/B были проведены в ноябре 2001 г., а в январе 2002 г. руководство ВВС США приняло решение о серийном производстве этого боеприпаса [394].

Именно боеприпас Rockeye II поступил на вооружение частей американских ВВС, обеспечивавших информационную поддержку боевых операций «Несокрушимая свобода» (Афганистан, 2001 г.) и «Свобода Ирака» (Ирак, 2003 г.). Известно, что с началом боевых действий в Ираке в марте 2003 г. первые 60 000 листовок были распространены над Багдадом именно с помощью кассетной авиабомбы PDU-5/B. В целом же в ходе войны в 2003 г. было использовано 184 таких боеприпаса, с помощью которых на территории этой страны удалось распространить более 11,04 млн листовок [394].

Помимо указанных выше, на вооружении ВС США в настоящее время находятся следующие листовочные (агитационные) боеприпасы: кассетные бомбы PAU-6/A; 45,4 кг M104 и 227 кг M105 [394].

5.5.1.4. Авиационные пневматические рассеиватели

В настоящее время в американских ВС ведутся НИОКР в области создания и разработки дешевых и эффективных способов и методов распространения с воздуха больших объемов печатных материалов. Так, ВМС США совместно с военно-промышленной корпорацией Raytheon Corporation испытывают в качестве средства распространения печатной продукции модульные авиационные контейнеры, из которых листовки, упакованные в четыре рулона, выталкиваются сжатым воздухом. Преимущество данного способа состоит в том, что он исключает повреждение листовок в момент их рассеивания, как это случается при использовании авиабомб [395].

За основу этих разработок взяты авиационные модульные подвесные обтекаемые контейнеры двух моделей: CNU-188 Baggage Container и MXU-648 Cargo Pod. Длина подвесного обтекаемого контейнера CNU-188 4,65 м, диаметр 0,7 м, грузоподъемность 106,1 кг. Его способны нести самолеты F/A-18, F-14, S-3, AV-8B, EA-6B и A-4. Длина подвесного обтекаемого контейнера MXU-648 составляет 3,3 м, диаметр — 0,5 м, грузоподъемность — 136,1 кг. Его носителями являются самолеты F-16, F-15, A-10 и AV-8B [395].

5.5.1.5. Распространение материалов с использованием БПЛА

В интересах сил психологических операций США разработан, произведен и поступил в войска на опытную эксплуатацию (74 единицы) грузовой БПЛА планерного типа CQ-IOA WSADS. Он спроектирован с учетом жестких требований по выполнению специальных психологических операций (залистование/десантирование груза с высокой точностью) с возможностью запуска с помощью машины высокой проходимости HMMWV (Hummer) или автоприцепа-платформы, а также в воздухе с самолетов C-130 и C-17. Благодаря своим техническим возможностям CQ-IOA может также вести наблюдение в интересах разведки и использоваться для выполнения вспомогательных задач (например, перевозка грузов) [95].

5.5.1.6. Артиллерийские средства распространения материалов

Согласно положениям раздела FM-33-1-1 «Технические средства ПсО и порядок их применения» полевого устава сухопутных войск США, для распространения в расположении противника печатных материалов ИПВ предназначены «листовочные артиллерийские снаряды» LAR (Leaflet Artillery Round) XM951 и M84 калибров 155 и 105 мм соответственно. Снаряд XM951 предпочтителен для применения в интересах ведения ПсО, поскольку он специально разработан для распространения листовок. В свою очередь, M84 переоборудован для этих целей из дымового артиллерийского боеприпаса [395].

Снаряд XM951 предназначен для снаряжения рулонами с листовками высотой 10,1–12,7 см, внутренним диаметром 2,5 см и внешним 10,1 см. Количество загружаемых листовок зависит от их формата и массы бумаги, но в стандартном варианте снаряд XM951 вмещает 2000 экз. (4 рулона по 500 шт). Дальность полета снаряда 20 км [395].

Снаряд M84 вмещает один рулон с листовками, высота которого 26 см, а внешний диаметр 7,6 см. Максимальная дальность полета такого боеприпаса 11,5 км, при этом на высоте 27–46 м он распадается на части, что обеспечивает разлет листовок. Данный снаряд не отличается высокой точностью, поскольку снаряжение листовками снижает его массу и стандартные таблицы стрельбы не позволяют произвести точные баллистические расчеты. По внешнему виду листовочный артиллерийский снаряд M84 отличается от дымового боеприпаса нанесенной на него литерой *P* (Propaganda, или PSYOP). Он вмещает около 1500 стандартных листовок. Для стрельбы M84 предназначены 105 мм буксируемые гаубицы M102. Однако основным недостатком артиллерийского способа распространения печатных материалов является сгорание части листовок в момент их выброса из боеприпаса [395].

В период операции «Буря в пустыне» американские силы ПсО подготовили и снарядили 200 листовочных (агитационных) 155 мм снарядов XM951. Однако из-за высокого темпа боевой операции было использовано только 9 таких боеприпасов [395].

Помимо артиллерийских снарядов, для распространения листовок на позиции противника могут применяться специально переоборудованные для этих целей противопехотные мины и состоящие на вооружении ВС США 81 мм минометные мины от армейского миномета M1 с отсеком для груза листовок [395].

5.5.1.7. Морские средства распространения печатных материалов

Морские средства распространения листовок и других материалов отличаются простотой и минимумом материальных затрат. Печатные материалы, предметы наглядной агитации (зажигалки, спички, футболки, кепки и т. п.) в плавучей герметичной таре, которая сбрасывается на водную поверхность с низколетящих летательных аппаратов, кораблей и судов и с учетом направления течения доставляется в возможное место нахождения противника. Плавучая тара (контейнер) выполняется из дерева, бамбука, пластика, стекла, полиэтилена и т. п. [395].

Согласно наставлению ВС США по распространению материалов пропаганды морским способом, плавучая тара подразделяется на четыре основных вида [395]:

- тяжелая, сплавляемая в подводном положении под воздействием морских течений;
- средняя, сплавляемая в подводном положении, как под воздействием морских течений, так и ветра;
- легкая, сплавляемая главным образом под воздействием ветра;
- стационарная якорная плавучая тара.

Наиболее известным примером распространения печатных материалов морским способом является операция по дезинформации иракского руководства относительно направления главного удара коалиционных сил перед началом войны в зоне Персидского залива (1991 г.). Для введения противника в заблуждение аппарат ПсО Объединенного центрального командования ВС

США подготовил большое количество маскировочных листовок с изображением высадки подразделений морской пехоты на побережье Кувейта. Они должны были создать у противника иллюзию подготовки крупномасштабного морского десанта коалиционных сил. Для распространения листовок использовались обычные пустые пластиковые бутылки из-под минеральной воды, которые в избытке имелись в наличии у ВС США в связи с их пребыванием в зоне с жарким климатом. С боевых кораблей и вспомогательных судов коалиционных сил было распространено порядка 10 000 таких бутылок, с самолетов коалиционной авиации — 90 000 и еще около 12 000 — завербованными командованием американских ВС контрабандистами из ОАЭ. Большинство листовок достигло занятого иракскими войсками побережья Кувейта 14 января 1991 г. — за день до окончания предъявленного С. Хусейну ультиматума, требовавшего вывода иракских войск из этой страны. Как заявили позднее американские источники, операция по дезинформации руководства Ирака имела успех, поскольку оно не сомневалось в реальности данной угрозы на всех этапах кампании и активно готовилось к отражению морского десанта, сосредоточив на кувейтском побережье Персидского залива в общей сложности до семи дивизий [395].

Помимо листовок, морским способом в места расположения противника распространяются предметы наглядной агитации и даже небольшие радиоприемники с фиксированной частотой, настроенные на волну пропагандистских радиостанций. Для этих целей применяются герметичные пластиковые банки с яркой раскраской для привлечения внимания, а чтобы вызвать наибольший интерес со стороны объектов воздействия, первые и последующие партии плавучих контейнеров заполняются кроме печатных материалов еще и зажигалками, спичками, сигаретами, солнечными очками, ручками, карандашами, яркой одеждой, игрушками, мылом и даже деньгами [395].

5.5.2. Средства телерадиовещания

5.5.2.1. 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 [397].

Такие специализированные самолеты появились в конце 80-х гг. в США. В качестве носителя теле- и радиовещательного оборудования был выбран транспортный самолет C-130 Hercules, на базе модели которого C-130E к тому времени уже были созданы воздушные командные пункты и самолеты радиоэлектронной разведки. Все три модификации получили одинаковое обозначение — EC-130E («E» по американской системе индексации указывает на «самолет со специальным электронным оборудованием»). Самолет ПсО получил индекс EC-130E 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» — то, что самолет всегда действует в одиночку [397].

Самолет EC-130E в середине 90-х гг. 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 9 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 4 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 [397].

В качестве оборонительных средств на самолете EC-130E 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 ГСН, и генераторы инфракрасных помех AN/ALQ-157. Оборудование для дозаправки в полете позволяет находиться над зоной вещания по 10–12 ч непрерывно [397].

Экипаж состоит из двух пилотов, штурмана, офицера — руководителя ПсО и семи специалистов: инженера, специалиста по радиоэлектронному оборудованию и пяти операторов [397].

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 формирова-

лась 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 [397].

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 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 ВС и местным телерадиовещанием, Commando Solo начинает трансляцию собственных передач, причем сразу на нескольких волнах. Вещание ведется в прямом эфире, в записи либо в режиме ретрансляции телевизионного сигнала в режиме реального времени [397].

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 [397].

В 1994 г. самолеты 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 [397].

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 [396].

В Афганистане EC-130E Commando Solo интенсивно применялись для информационно-психологического воздействия 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 [397].

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 массмедиа либо расширения спектра их вещания [397].

В 1998 г. в США было принято решение пополнить парк 193-й эскадрильи, состоявшей на тот момент из четырех самолетов EC-130E Commando Solo II. На основе самолета Hercules нового поколения был разработан новый самолет — C-130J, — получивший новые высокоэкономичные двигатели и современную авионику [397].

Самолет EC-130J Commando Solo 3 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 его задачи включают в себя радиоэлектронное подавление сетей управления и ограниченное ведение радиоразведки. Кроме решения военных задач этот самолет может быть использован для стабилизации обстановки при возникновении чрезвычайных ситуаций, например природных катастроф [398].

Первый EC-130J был построен в 2000 г. на предприятии компании Lockheed Martin на базе военно-транспортного самолета C-130J, поступившего в распоряжение ВВС США в октябре 1999 г. Самолет EC-130J Commando Solo 3 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 [398].

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 Lockheed Martin до так называемой конфигурации Super 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 [398].

Последний самолет EC-130E в модификации Commando Solo II был списан в 2006 г., и в настоящее время в ВС США находятся 7 самолетов EC-130J Commando Solo 3. При выполнении психологических операций в небе над Ираком, начиная с середины 2007 г., эти самолеты за 8 месяцев налетали в общей сложности около 1350 ч [398].

В состав экипажа EC-130J входят 10 человек: два летчика, оператор бортовых систем, оператор целевого оборудования, старший по погрузочно-разгрузочным работам и пять операторов электронных систем связи.

Бортовой комплекс обороны включает в себя: 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 [398].

В начале 2010 г. один EC-130J был передислоцирован на Гаити после произошедшего там землетрясения для трансляции правительственных сообщений и информации, призванной успокоить население. Для этих целей на подвергшейся разрушениям территории распространялись радиоприемники с питанием от солнечных батарей и встроенных динамо-машин. Кроме доведения до населения важной информации от гавайского правительства аппаратура Commando Solo 3 использовалась для извещения людей на частотах местных широковещательных радиостанций о том, где они могут найти помощь, а также воду, питание и медикаменты. С борта самолета трансляция велась ежедневно по 14 ч [398].

В бюджете МО США на 2011 г. было заложено 6,7 млрд долларов на модернизацию средств ПсО в течение 5 лет. При этом значительная часть данной суммы предназначена для обновления парка машин типа С-130 путем поставок самолетов новых модификаций [398].

Как показал опыт применения самолетов психологических операций EC-130 Commando Solo в локальных войнах и в конфликтах, они по своей боевой эффективности не уступают стратегическим бомбардировщикам. Боевое применение B-1, B-52 и даже B-2 просто приводит к гибели солдат и офицеров противника. Передачи же EC-130E (J) сокрушают веру в цели борьбы и грядущую победу, без которой любая воюющая сторона теряет волю к сопротивлению [397, 398].

В настоящее время планируется расширение авиационных средств ведения ПсО и использование для этих целей БПЛА. Так, в интересах проведения ПсО планируется использовать БПЛА 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 [393].

5.5.2.2. 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 два основных модуля [394]:

- мобильной системы радиовещания (Mobile Radio Broadcast System);
- мобильной системы телевещания (Mobile Television Broadcast System).

Каждый из этих модулей смонтирован на двух бронемашинах HMMWV (Hummer): аппаратной и грузовой. Кроме того, в состав каждого модуля входят 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 телевизионное и радиовещание в СВ-, КВ- и УКВ-диапазонах [394].

5.6. Способы информационно-психологического воздействия в военных конфликтах

5.6.1. Способы информационно-психологического воздействия на основе листовок и других печатных материалов

Американское руководство придает большое значение информационному обеспечению своих внешнеполитических инициатив, особенно если речь идет о применении национальных ВС. Учитывая негативный опыт войны во Вьетнаме, в конфликтах конца XX и начала XXI в. США уделяют пристальное внимание заблаговременной подготовке мирового и национального общественного мнения к предстоящим военным операциям. В этой работе принимают участие представители Белого дома, специализированные структуры Пентагона, сотрудники ЦРУ, федеральных агентств и представители американских СМИ.

Далее представлены основные способы информационно-психологического воздействия на основе листовок и других печатных материалов на примере действий подразделений ПсО ВС США в Ираке в 2003 г.

5.6.1.1. Операция США и их союзников «Иракская свобода» («Шок и трепет») в Ираке в 2003 г.

Наиболее широко подразделения ПсО ВС США в операции «Иракская свобода» («Шок и трепет») в Ираке в 2003 г. применяли «классические» формы психологических операций — радиовещание и печатную пропаганду [396].

На предварительном этапе операции печатная пропаганда велась в значительных масштабах, и к началу боевой фазы операции общее число распространенных на территории Ирака листовок достигло 20 млн. На начальном этапе операции основными направлениями содержания в материалах печатной пропаганды были: необходимость капитуляции, недопустимость применения оружия массового поражения и сохранение нефтедобывающей инфраструктуры [396].

Одной из главных целей иракской кампании, равно как и всей политики США на Ближнем Востоке, являлся доступ к месторождениям энергоресурсов. Поэтому американское командование опасалось повторения событий 1991 г., когда иракцы подорвали сотни нефтяных вышек и сбросили значительные объемы сырой нефти в море. В связи с этим в печатных пропагандистских материалах постоянно звучала тема экологического ущерба, нанесенного тогда Ираку, и недопустимости повторения такого сценария. Кроме того, упор был сделан на то, чтобы убедить работников нефтяной индустрии в крайней необ-

ходимости сохранения объектов нефтедобычи и переработки для экономики страны и будущего ее граждан. О важности этого направления информационно-психологического воздействия для Вашингтона говорит количество распространенных листовок соответствующего содержания, которое составило около 40 млн единиц [396].

По оценкам ветеранов войны в Ираке, психологические операции, направленные на сохранение нефтедобывающего комплекса страны в неприкосновенности, были достаточно успешными. Иракцы минировали вышки, подчиняясь приказам руководства страны, но не подрывали их, осознавая пагубные последствия для своего будущего. Утверждается, что к таким действиям их побудила именно американская пропаганда [396].

С началом боевых действий тезисы воздействия были скорректированы: иракских военнослужащих призывали к сдаче в плен и дезертирству, а гражданское население — избегать нахождения в районах боевых действий, оставаться в своих домах, не пользоваться автомобильным транспортом в ночное время. Наряду с этим была активизирована работа по дискредитации С. Хусейна. С этой целью распространялись листовки, демонстрирующие роскошную жизнь иракского лидера на фоне нищеты и голода рядовых граждан страны. Следует отметить, что на ранних этапах листовки ВС США были цветными, но с ростом масштабов боевых действий, когда на первое место вышла оперативность, они стали черно-белыми, что позволило сократить сроки их производства [396].

Распространяемые американскими войсками листовки предназначались как для иракских военнослужащих, так и для мирного населения. Первые были ориентированы на снижение боевого духа, отказ от боевых действий и сдачу в плен. Вторые направлены на создание в лице ВС США образа освободителя, дискредитацию руководства страны, а также на разъяснение действий гражданского населения в условиях войны. Отдельное внимание уделялось распространению цветных книг и буклетов для детей [396].

Различные листовки и плакаты были выполнены в форме объявлений о «награде за голову» С. Хусейна и его министров. Они также сообщали о денежном вознаграждении за предоставление информации о действиях военно-политического руководства страны и командования республиканской гвардии.

Наряду с листовками, содержащими призывы к конкретным действиям, в Ираке массово распространялись печатные материалы с указанием частот и времени вещания американских радиостанций — так называемые радиолистовки. Учитывая низкий уровень грамотности местного населения, специалисты ПсО США стремились таким образом максимально привлечь граждан к прослушиванию радиопередач [396].

Для распространения пропагандистских материалов привлекались силы авиации ВМС США. Типографское оборудование корабля было задействовано в тиражировании листовок, количество которых за период с 17 декабря 2002 г. по 17 апреля 2003 г. составило 5,5 млн. Такая же работа велась на борту авианосца Theodore Roosevelt [396].

Помимо авиационных средств распространения печатной пропаганды листовки раздавались местному населению тактическими командами ПсО и подразделениями сил специальных операций в ходе выполнения боевых задач [396].

В ходе боевой фазы операции было осуществлено свыше 150 залистований авиационными средствами, посредством которых распространено почти 32 млн листовок [396].

Власти Ирака, в свою очередь, предпринимали активные меры по противодействию американской пропаганде. С этой целью был создан комитет психологических операций, в задачи которого входили [396]:

- сбор и уничтожение американских и «натовских» листовок;
- оценка эффективности воздействия ПсО западной коалиции на иракцев;
- выработка рекомендаций и непосредственное проведение контрпропагандистских мероприятий.

Иракским гражданам было запрещено подбирать, хранить и распространять печатные материалы коалиции под угрозой тюремного заключения и смертной казни. Кроме того, официальный Багдад потребовал от сотрудников американской телекомпании CNN покинуть территорию страны, обвинив их в дезинформации мирового сообщества и распространении сфабрикованной информации [396].

Отдельно следует отметить ожесточенное информационно-пропагандистское противоборство между американскими и иракскими органами ПсО в области привлечения гражданского населения Ирака к боевым действиям. В американских листовках и радиопередачах содержались призывы оказывать помощь сбитым пилотам ВВС США за денежное вознаграждение. Со своей стороны иракское радио объявило о выплатах крупных денежных сумм за убийство либо пленение американских солдат (14 000 и 28 000 долларов соответственно) [396].

5.6.2. Способы информационно-психологического воздействия на основе средств телерадиовещания

Рассмотрим основные способы информационно-психологического воздействия на основе радио- и телевещания на примере действий подразделений ПсО ВС США в операциях в Ираке в 2003 г. и в Афганистане в период 2001–2014 гг. Также рассмотрим способы информационно-психологического воздействия, используемые в 2008 г. в операции ВС Израиля против группировки «Хамас» и в операции по принуждению Грузии к миру, проводимой ВС России.

5.6.2.1. Операция США и их союзников «Иракская свобода» («Шок и трепет») в Ираке в 2003 г.

Началу военной стадии операции «Иракская свобода» («Шок и трепет») в 2003 г. предшествовал хорошо спланированный подготовительный этап — информационно-психологическая операция, когда США, опираясь на глобаль-

ную информационную сеть Интернет и международные телевизионные СМИ, сумели в кратчайший срок убедить мировое сообщество в агрессивных устремлениях Ирака, откровенно игнорирующего действующие международные соглашения. Посредством мощного информационного воздействия через СМИ американские структуры, специализирующиеся на информационной обработке населения, настроили мировое сообщество, включая исламские государства, против Ирака, создав таким образом благоприятную обстановку для вторжения [13].

Белый дом сделал упор на эмоциональное восприятие мировым сообществом «иракской угрозы», а не на ее рациональную оценку. Этому способствовали негативное отношение к исламу и мусульманскому миру в западном сообществе, а также рост ненависти к выходцам из стран Ближнего Востока и Афганистана на фоне масштабного освещения в американских телевизионных СМИ террористических актов, совершённых исламистами. У рядового американца был сформирован образ внешнего врага в лице абстрактного «мусульманина-террориста», который ненавидит США и весь западный мир и представляет угрозу для безопасности самих американцев. Такие психологические установки были необходимы Вашингтону для оправдания перед собственным населением и рядовыми военнослужащими необходимости военной операции. В таких условиях «назначить» конкретного исламистского лидера, ликвидация которого устранила бы угрозу американцам, было вопросом техники [396].

Наиболее ярким примером американской дезинформации в преддверии вторжения в Ирак можно считать выступление государственного секретаря США К. Пауэлла на специальном заседании Совета Безопасности ООН 5 февраля 2003 г., где он представил «доказательства» наличия у Ирака оружия массового поражения. Американский политик для придания наглядности своим заявлениям продемонстрировал некую пробирку, якобы содержащую споры сибирской язвы. А спустя год К. Пауэлл признал, что обнародованные им данные были во многом неточными, а иногда и сфальсифицированными. Подделкой оказалась и ампула с образцом биологического оружия. Более того, многочисленные американские и международные комиссии уже в 2004 г. пришли к выводу, что на момент начала военного вторжения Багдад не располагал оружием массового поражения [396].

Американский центр гражданской ответственности совместно с Фондом за независимость журналистики провел исследование, в ходе которого было подсчитано, что с сентября 2001 г. по сентябрь 2003 г. руководство США сделало 935 ложных заявлений по Ираку, преимущественно через телевизионные международные СМИ. Своего рода лидером стал американский президент Дж. Буш: 260 ложных высказываний, 232 из которых — якобы о наличии у С. Хусейна оружия массового поражения и 28 — о связях руководства Ирака с Аль-Каидой. Госсекретарь К. Пауэлл сделал 254 недостоверных заявления. Подобные исследования нанесли ущерб имиджу США, однако Вашингтон к тому времени уже успел сформировать на Западе атмосферу ненависти к иракскому лидеру. В немалой степени это позволило американскому руководству

парировать на начальном этапе аргументы противников военной операции и избежать активных антивоенных выступлений американского населения [396].

С началом военного этапа операции многонациональные силы блокировали практически всю информационную систему Ирака (радио, телевидения, Интернет), используя средства РЭП в сочетании с традиционным огневым поражением. Это обеспечило монопольное использование многонациональными силами средств телерадиовещания для информационно-психологического воздействия на население и военнослужащих Ирака [396].

При этом радиопропаганда на территории Ирака велась в основном с борта самолета психологических операций EC-130E Commando Solo, базировавшегося в Катаре, на коммерческих AM- и FM-частотах. Поначалу самолет EC-130E находился вне иракского воздушного пространства, однако с развитием операции экипажу было дано указание обеспечить трансляцию радиосигнала на западный Ирак. Таким образом, EC-130E выполнял задачи непосредственно в иракском воздушном пространстве, что было сопряжено с существенным риском из-за низкой маневренности самолета [396].

Наиболее типичные радиообращения, транслировавшиеся с борта EC-130E, звучали следующим образом: *«Граждане Ирака. Ваш уровень жизни существенно упал с момента прихода Саддама Хусейна к власти. Каждую ночь дети Ирака ложатся спать голодными. Люди страдают от заболеваний, которые с легкостью лечатся во всём остальном мире. Саддам строит дворец за дворцом и покупает шикарные машины на деньги иракского народа, которые можно было бы потратить с пользой, например на строительство библиотек и школ. Саддам и его окружение купаются в роскоши и считают себя выше законов. Саддам живет как король, в то время как его солдаты не получают ни денег, ни обмундирования. Как долго этому несостоятельному главе будет позволено править? Сколько солдат он еще готов отдать в жертву? Станет ли следующей жертвой твое подразделение? Когда армия Ирака будет служить своему народу и перестанет играть роль телохранителей»?* [396].

В апреле 2003 г. на самолет EC-130E была также возложена функция трансляции телевизионной передачи «Вперед, к свободе», в рамках которой с речью к иракскому населению обращались президент США Дж. Буш и премьер-министр Великобритании Т. Блэр [396].

Помимо EC-130E Commando Solo для ведения радиопропаганды и телевещания использовались мобильные медийные комплексы специальных операций SOMS-B. Всего было развернуто три таких комплекса, первый из которых начал вещание с территории Кувейта в декабре 2002 г. На тот момент продолжительность эфира составляла 5 ч в сутки, но к февралю 2003 г. она была доведена до 18 ч. Второй комплекс был придан 3-й пехотной дивизии ВС США, третий — развернут в международном аэропорту Багдада сразу после его захвата войсками коалиции. Таким образом, три комплекса SOMS-B и самолет EC-130E Commando Solo обеспечивали вещание на всю территорию Ирака. Радиостанции авианосцев, дислоцированных в Персидском заливе, также использовались для ретрансляции радиопередач [396].

В непосредственных боевых операциях, проводимых подразделениями сухопутных войск США, активное участие принимали тактические команды ПсО, оснащенные звуковещательными станциями. При этом наряду с небольшими звуковещательными станциями ранцевого типа использовались мощные станции, которые устанавливались преимущественно на военной технике, в частности, на таких платформах, как джип M102 HMMWV Hummer, основной боевой танк M1A1 Abrams, БТР M113, вертолет UH-60 Black Hawk и патрульные катера PBR Mk 2. Отмечены также случаи оборудования в виде звуковещательных станций ранцевого типа трофейных иракских мотоциклов [396].

Во время сеансов звуковещания американские военнослужащие призывали бойцов иракской армии к сдаче в плен, «выманивали» боевиков из засад, сообщали правила поведения для мирного населения. В некоторых случаях при осаде укреплений иракцев солдаты США при помощи звуковещательных станций выкрикивали оскорбления в адрес своих противников, провоцируя их атаковать на открытой местности. Помимо этого, звуковещательные станции активно использовались в операциях по введению противника в заблуждение путем воспроизведения звуков стрельбы, перемещения военной техники, приближения авиации и т. д. Различные звуковые эффекты и громкая музыка применялись также для деморализации противника. По некоторым данным, тяжелая музыка эффективно использовалась при допросе пленных иракцев [396].

Одним из нестандартных способов оказания информационно-психологического воздействия в ближневосточной кампании можно назвать так называемую «демонстрацию поддержки народом смены режима». В эфире телевидения были показаны кадры сноса памятника С. Хусейну иракскими гражданами в апреле 2003 г. Комментатор объявил о том, что это волеизъявление народа, которое свидетельствует о его ненависти к тирану. Однако, по мнению многих экспертов, данная акция была спланирована специалистами ПсО США, которые оцепили площадь и предоставили технику для демонтажа монумента [396].

Следует отметить, что, наряду с официальной, распространяемой подразделениями ПсО ВС США, так называемой «белой» пропагандой, в иракском конфликте также применялись способы «черной» пропаганды, которая осуществлялась в основном ЦРУ. В частности, оно развернуло на территории республики радиовещательную станцию «Радио Тикрит», выдававшую себя за иракскую и изначально поддерживавшую режим С. Хусейна. С началом боевых действий тональность сообщений «Радио Тикрит» постепенно сменилась и существующий режим стал подвергаться откровенной критике. Таким образом, американские специалисты стремились продемонстрировать снижение поддержки иракского лидера со стороны населения и дискредитировать его политический курс [396].

5.6.2.2. Операция США и НАТО «Несокрушимая свобода» в Афганистане в 2001–2014 гг.

С началом антитеррористической операции «Несокрушимая свобода» в 2001 г. органы ведения психологических операций ВС США в целях информационно-психологического воздействия широко применяли авиационные сред-

ства, в том числе использовали возможности радиовещания, а также распространение печатных пропагандистских материалов.

На первом этапе операции в качестве основного средства радиовещания американское командование привлекало специально предназначенные для этих целей самолеты EC-130J Commando Solo [404].

В Афганистане вещание на население страны велось на частотах от 45 кГц до 1000 МГц. Одновременно с трансляцией радиопрограмм началось распространение первых листовок с указанием частот и времени работы радиостанции «Информационное радио» сил коалиции. С целью обеспечения своего информационного доминирования ВВС США предварительно уничтожили в Кабуле главную радиостанцию талибов — «Голос шариата» [404].

В то же время американцы столкнулись с проблемой отсутствия радиоприемников у афганского населения, так как в период правления талибов радио было запрещено. В первые недели операции командование приняло решение сбрасывать с самолетов ВВС радиоприемники вместе с листовками и продовольствием. В дальнейшем раздачей портативных устройств занимались тактические команды ПсО и представители неправительственных организаций. По данным американских СМИ, на начальном этапе афганцам было передано более 7500 транзисторных приемников [404].

Население получало в основном радиоприемники Kaito, работающие в СВ-, КВ- и УКВ-диапазонах, которые питались от встроенной или солнечной батареи и механической динамо-машины. В первую очередь они использовались в центральных районах Афганистана, где отсутствовало электроснабжение. Однако из-за низкой чувствительности приемника, которому требовался сильный сигнал с радиостанции, эффективность вещания была невысокой, особенно в горной местности.

Некоторое время в Афганистане распространяли СВ-, КВ-, УКВ-радиоприемники со встроенным источником питания». Но поставки прекратились, так как батарею нельзя было перезарядить или заменить. Поэтому впоследствии органы ПсО рекомендовали к использованию радиоприемник с подзаряжаемой динамобатареей, хорошо зарекомендовавший себя в горных районах страны. Только за период с ноября 2003 г. по апрель 2004 г. подразделения ПсО коалиционных сил раздали населению более 30 000 таких устройств [404].

В целях проведения психологических операций на оперативно-тактическом уровне в Афганистане был дислоцирован 8-й батальон ПсО ВС США, приданный Центральному командованию из состава 4-й группы ПсО (Форт-Брэгг, штат Северная Каролина). Радиоспециалистами подразделения были развернуты мобильные комплексы телерадиовещания SOMS-B. В марте 2002 г. первые модули радиовещания SOMS B были смонтированы на территории аэродромов в г. Баграм и Кандагар. Вначале трансляция велась в СВ- и УКВ-диапазонах, а впоследствии все передачи были переведены на частоты КВ — 9325, 9345 и 9365 кГц. Мощность передатчиков составляла 5 кВт, что обеспечивало прием устойчивого сигнала в радиусе 40 км в диапазоне СВ и УКВ, а на частотах КВ вещание практически покрывало всю территорию страны [404].

Основное содержание, формы и методы радиопропаганды органов ПсО ВС США и НАТО в Афганистане, в том числе и с применением средств воздушного базирования, претерпели некоторые изменения за время проведения операции. Определенно можно констатировать несколько этапов, в соответствии с которыми менялись цели и задачи ПсО [404].

На начальном этапе главными целями радиопропаганды органов ПсО ВС США были [404]:

- разъяснение населению Афганистана целей США и причин появления американских войск в регионе;
- деморализация и склонение к прекращению сопротивления и сдаче в плен членов вооруженных формирований «Талибан» и «Аль-Каида»;
- завоевание симпатий и обеспечение сотрудничества со стороны местных жителей.

С первых дней бомбардировок позиций боевиков основной формой радиопропаганды стали программы «Информационного радио», трансляция которых осуществлялась с борта самолета EC-130J Commando Solo до 10 ч в сутки. Кроме того, ретрансляцию на частотах этого комплекса вели некоторые местные радиостанции [404].

Было разработано несколько десятков радиопрограмм, предназначенных для различных аудиторий. В целом программы радиовещания можно разделить на две категории: для мирного населения и для членов вооруженных формирований [404].

Основным содержанием радиопрограмм были новостные блоки, музыка, обращения американского командования, а также сообщения, подготовленные специалистами 4-й группы ПсО. Для привлечения афганской аудитории эти программы на 3/4 состояли из местной музыки, которую запрещали во время правления талибов [404].

Причины дислокации воинского контингента США разъяснялись в радиопрограммах, транслируемых в том числе с самолетов ВВС США, в частности, путем обращений следующего типа [404].

«Уважаемые афганцы! Против Соединенных Штатов было совершено страшное преступление. Руками Усамы бен Ладена, Аль-Каиды, Талибана и их приспешников были захвачены четыре самолета, разрушены здания в наших экономических центрах, убиты более 6000 невинных людей, многие из которых были мусульманами. Мы рассматриваем эти действия как акт войны. В подобной ситуации мы не собираемся просто сидеть сложа руки и ничего не делать. Однако, в отличие от трусливых террористов, мы не будем проливать кровь невинных людей. Мы не виним мусульман Афганистана в этих атаках. Мы не будем преследовать правоверных последователей ислама. Но мы найдем и накажем настоящих террористов. Они заплатят собственной кровью. Америка не против приверженцев ислама, не против мусульман. В Соединенных Штатах живут в мире и почитают Аллаха более 6 млн мусульман, что равняется почти половине населения Афганистана. В США вместе мирно живут люди различных религий. Мусульмане имеют такое же право на вероисповедание, как и граждане — приверженцы других религий».

Одна из главных задач американской радиопропаганды в начальный период операции состояла в том, чтобы убедить широкие массы населения отказаться от поддержки боевиков группировки Талибана. Для этого в радиопрограммах использовались такие эмоциональные обращения, призывы и утверждения [404].

«Разве вы хотите жить под властью фундаменталистов Талибана?!

Разве вы гордитесь тем, что живете в страхе?!

Разве вы счастливы оттого, что землю ваших предков превратили в лагеря подготовки террористов?!

Они уничтожили ваше культурное наследие и великие монументы!

Они хотят лишить вас наследия прошлого, которое тысячелетиями созидал ваш народ!

Талибан ограбил землю ваших предков!

Они управляют с помощью принуждения, насилия и страха!»

В соответствии с установками специалистов по ведению ПсО ВС США, информационно-психологическое воздействие посредством прямых угроз и показа превосходства американского оружия было направлено на снижение боевого духа противника. Содержание устрашающих радиоматериалов было однотипно. После формального обращения боевики заранее объявлялись приговоренными к смерти. Далее обычно разъяснялись причины, по которым мировое сообщество приняло такое решение. С помощью эмоционально окрашенных эпитетов и ярких сравнений типа «прольется дождь смерти» или «высокоточные бомбы нацелены на ваши окна» описывались сила и мощь американского оружия [404].

В первые недели после начала вторжения американское командование приняло решение применять авиацию ВВС для того, чтобы сбрасывать с самолетов так называемые наборы помощи, чтобы тем самым привлечь местное население на свою сторону. Обычно такие грузы десантировали на парашютах партиями, которые состояли из медикаментов, продовольствия, воды, листовок и портативных радиоприемников. Для разъяснения целей этой акции подразделения ПсО подготовили специальные радиопрограммы. Главный пропагандистский посыл заключался в том, чтобы показать добрые намерения США по отношению к простым людям и одновременно противопоставить свою мирную политику жестокому отношению к населению талибов. Например: *«Соединенные Штаты оказывают помощь с целью выразить свою поддержку честным афганским людям. Мы не хотим, чтобы страдали ваши семьи за то, что сделали боевики из Аль-Каиды и ее лидер Усама бен Ладен!»* Кроме того, в таких программах давались детальные инструкции по содержанию грузов и безопасности при их получении [404].

В то же время анализ содержания материалов ИПВ показывает, что на первом этапе американские специалисты по ведению ПсО отождествляли менталитет населения Афганистана с европейским или американским, не учитывая его национально-психологические особенности. Ошибочен был расчет, что исламские фанатики, приученные к мысли о смерти за веру, испугаются силы американского оружия и немедленно сдадутся. Население в большинстве своем

воспринимало радиопрограммы как открытую пропаганду оккупационных войск и относилось к информации настороженно и без особого доверия. При подготовке радиопрограмм использовались однотипные сценарии, и они не отличались разнообразием [404].

Можно считать, что первый этап ПсО завершился к началу 2002 г. с окончанием бомбардировок и оккупацией территории Афганистана. В это же время прекращаются радиотрансляции с бортов самолетов EC-130J, заканчивается переброска 8-го батальона ПсО США, который развертывает мобильные системы радиовещания в г. Баграм и г. Кандагар [404].

Кроме радио- и телевещания для ведения психологических операций авиация широко применялась для распространения печатных пропагандистских материалов [404].

Основные материалы печатной пропаганды в Афганистане издавались и распространялись в форме листовок. Подготовка их текстов возлагалась на специалистов 6-го регионального батальона ПсО, а полиграфическое исполнение — на 3-й батальон подготовки и распространения материалов ПсО. Листовки распространялись с помощью авиации (самолеты С-130, С-141) и БПЛА с использованием специальных авиационных тар (вместимость от 20 000 до 40 000 листовок) и авиационных бомб (от 30 000 до 80 000 листовок) [404].

С учетом низкой грамотности населения Афганистана (менее 40%) основной упор при подготовке листовок делался на изобразительные средства наглядной агитации. Тексты были в основном предельно краткими и простыми, рассчитанными на менталитет афганцев. Американские специалисты разработали десятки вариантов адресных листовок, предназначенных для различных слоев афганского общества [404].

Все информационно-пропагандистские материалы можно условно разделить на две категории: для мирного населения и для членов вооруженных формирований [404].

В информационно-пропагандистских материалах, предназначенных для членов вооруженных формирований, преобладали листовки устрашающего содержания, из которых следовало, что они обречены, что их лагеря и базы будут «залиты смертоносным ливнем огня с вертолетов». В них всячески подчеркивалось техническое превосходство американцев: «Вы будете уничтожены до того, как ваши устаревшие радары засекут наши вертолеты», «Наши ракеты попадут точно в твое окно». В некоторых листовках говорилось, что единственный выход для боевиков — «немедленная сдача в плен», как только в Афганистане появятся американские солдаты [404].

Вместе с тем, по мнению бывшего командира 4-й группы ПсО ВС США полковника Ч. Борчини, содержание адресованных боевикам листовок, в которых «не было ничего, кроме элементарного запугивания», могло быть расценено афганцами, особенно пуштунами и белуджами, только как оскорбление и имело скорее отрицательный эффект [404].

Ошибочным был и расчет на то, что исламский фанатик, который постоянными молитвами и другими средствами самовнушения в лагерях боевиков приучает себя к мысли о гибели за веру и заранее «отдаляется от земного

мира», отреагирует на рассказ о гибели людей в Нью-Йорке и Вашингтоне так же, как американец или европеец, и осудит действия террористов. По его убеждению, террористы были «борцами за веру», а она позволяет мусульманину совершать любые действия против иноверцев; если же среди погибших неверных «торгашей» в небоскребах были добропорядочные люди, то они попали в рай (а недобропорядочные за свою мученическую смерть получили дополнительную возможность не попасть в ад) [404].

В листовках, предназначенных для мирного населения, предлагалось большое вознаграждение за информацию о местонахождении террористов. Делались попытки дискредитировать руководство талибов и Аль-Каиды в глазах населения и боевиков. Кроме листовок и плакатов подразделения ПсО ВС США выпускали газеты. Так, ежемесячная газета «Мир», которая издавалась на трех языках (дари, пушту и английском), освещала все новости в Афганистане, а также содержала материалы, оказывающие информационно-психологическое воздействие на различные категории населения. Газеты раздавались в местах большого скопления людей, а также доставлялись в местные школы с учетом того, что многие из них не имели учебного материала для чтения [404].

Летом 2006 г. органы ПсО ВС США приступили к созданию общей радиосети психологических операций для сил альянса. Задачей новой структуры радиовещания стало «создание атмосферы доверия между населением, национальными властями и войсками НАТО для достижения всестороннего урегулирования ситуации в Афганистане». Общие и местные программы вещания для новой радиосети готовились специалистами ПсО в Кабуле и ретранслировались в регионы, где размещены так называемые команды по восстановлению инфраструктуры PRT (Provincial Reconstruction Team). В их задачи входит реализация проектов развития и восстановления регионов под эгидой ООН, Евросоюза и НАТО. В каждой из таких команд имеется передатчик органов ПсО, который ведет радиовещание в УКВ-диапазоне 87,5–107 МГц. Таким образом, планировалось значительно улучшить качество сигнала и заменить маломощные радиостанции сил коалиции, расположенные в регионах. В частности, бундесвер осуществлял вещание в районе Кабула с помощью радиостанции «Голос Свободы», британский контингент — в провинции Гельменд, а канадская станция «Рана-ФМ» — в Кандагаре [404].

Таким образом, органы ПсО в ВС США и НАТО в Афганистане развернули масштабную информационно-пропагандистскую обработку населения, осуществляемую посредством печатной и устной, в том числе радиопропаганды, а также телевещания, чему в немалой степени способствовали военно-воздушные силы. При этом благодаря совершенствованию содержания и форм радио- и телепропаганды органы ПсО во многом добились доверительного отношения к информации со стороны целевой аудитории. В то же время обострение ситуации в Афганистане и рост враждебности населения по отношению к военнослужащим коалиционных сил свидетельствуют о том, что органы ПсО пока недостаточно эффективно используют возможности ВВС для информационно-психологического воздействия в целях обеспечения выполнения войсками НАТО поставленных перед ними задач [404].

5.6.2.3. Операция Израиля «Расплавленный свинец» против группировки «Хамас» в 2008 г.

В подготовительный период операции генеральный штаб ВС Израиля сосредоточил усилия на обеспечении тактической внезапности. Нестандартные шаги по вводу противника в заблуждение включали: поездки официальных лиц и политиков в район Газы, а также визит министра иностранных дел Израиля в Египет, которые сопровождались успокаивающими репортажами в СМИ: показ находящихся в увольнении израильских солдат; демонстрация выпускных церемоний в военных колледжах перед началом операции [407].

Первый, самый сокрушительный удар по объектам группировки «Хамас» был нанесен 27 декабря 2008 г. в 11:30. Самолеты для нанесения удара заходили со стороны Средиземного моря по маршрутам, используемым гражданской авиацией. Выбор этого времени также не случаен. Первоначально была сделана контролируемая утечка сведений о плане начала операции в пятницу, 26 декабря 2008 г. Однако затем, по сообщению телевидения, израильтяне якобы наметили новый раунд переговоров по урегулированию проблемы с помощью Египта. Когда в указанный срок боевые действия не начались, исламисты сочли, что в субботу (священный для иудеев выходной день) они маловероятны, и массово покинули свои ранее занятые укрытия [407].

Замысел информационной операции предусматривал минимальное медиаосвещение хода боевых действий, чтобы исламисты не могли черпать сведения из СМИ. Журналисты в зону военных действий не допускались. К общению с ними в виде ежедневных пресс-конференций были привлечены соответствующим образом подготовленные генералы. Пресс-служба министерства обороны готовила ежедневные бюллетени и репортажи, где, однако же, приводились значительно преуменьшенные данные о своих потерях, превозносились мощь израильского оружия и успехи группировки без детализации по подразделениям и привязки к местности. Цензура не пропускала сообщений в СМИ о похоронах убитых израильских солдат, заявлений правозащитников, а темы потерь от исламистов и обстрелов ими населенных пунктов, наоборот, представлялись в гипертрофированном виде [407].

5.6.2.4. Вооруженный конфликт в Южной Осетии в 2008 г.

С первых часов конфликта грузинским руководством сразу же было организовано информационно-психологическое воздействие на население как внутри страны, так и за рубежом с использованием международного телевидения. Например, сразу же после начала боевых действий 8 августа 2016 г. в офисе телекомпании «Триалети» (г. Гори) открылся медиацентр, круглосуточно обслуживавший грузинских и зарубежных журналистов. Большинство основных грузинских электронных СМИ, в частности «Грузия on-line», телекомпания «Рустави-2», информагентство «Интерпресс Ньюс», радиостанция «Имеди», включились в активное распространение информационных материалов, в том числе и видеосъемок с мест противостояния [408].

Следует также отметить и мощнейшую поддержку усилий Тбилиси по проведению информационной операции со стороны ведущих англосаксонских СМИ (прежде всего таких информационных агентств, как CNN, BBC, Reuters, Bloomberg и др.). С началом боевых действий «Голос Америки» удваивает объем вещания на Грузию. В сообщении этой радиостанции было сказано, что «вместо 30-минутных ежедневных передач теперь в эфир будут выходить часовые программы, в том числе новости, информация, интервью, аналитика и реакция на кризис из бывших советских республик». Исполнительный редактор «Голоса Америки» С. Редишия заявил: «Мы хотим быть уверенными, что грузинский народ полностью информирован о том, что происходит в его стране» [408].

Что касается содержания и формы подачи материалов информационно-психологического воздействия, то здесь можно отметить как удачи, так и неудачи.

С самого начала боевых действий серьезнейшей ошибкой англоязычных СМИ было их замалчивание. Такая «информационная тактика» могла бы иметь успех, если бы в современном мире кроме них не было бы других источников информации либо разговор шел не о полномасштабном боестолкновении, а о «рядовой» перестрелке на грузино-югоосетинской границе. Однако сами грузинские СМИ «подвели» своих коллег: они не только показывали обстрел г. Цхинвал с использованием своих установок «Град» и движение автомобильных колонн с грузинскими войсками в сторону столицы Южной Осетии, но и «вывешивали» на своих сайтах картины расстрелов из танков и бронемашин безоружных людей и домов мирных жителей. Фактически американцы и англичане не учли особенности менталитета грузинской нации [408].

Неудачны были также и репортажи о вводе на территорию Южной Осетии частей 58-й армии ВС России. На основных английских и американских каналах демонстрировалась почти статичная картинка, сопровождающаяся одними и теми же комментариями. В этом отношении действия грузинских СМИ были, как это ни покажется парадоксальным, более профессиональными. Очень профессионально был смонтирован материал о налете спецназа Грузии на колонну российской бронетехники с попыткой пленения командующего 58-й армией СКВО. Ранение, гибель или пленение генерала, тем более занимающего такой высокий пост, очень серьезно сказывается на состоянии воинского духа противостоящей стороны, вид пленных врагов всегда вдохновляет собственную армию и союзников, а также деморализует противника [408].

К плюсам прогрузинской пропаганды англоязычных СМИ следует отнести показ выступлений президента Грузии М. Саакашвили. Прежде всего, следует отметить тот факт, что президент Грузии все свои публичные выступления записывал на фоне флага ЕС. Для массовой аудитории, которая вряд ли знает, какие страны входят в ЕС, создавалось впечатление, что воюет страна, входящая в Евросоюз. Фактически заведомо подготавливалась позиция, что Европа поддерживает Грузию. М. Саакашвили и другие грузинские официальные и неофициальные лица буквально «оккупировали» экраны и страницы ведущих

англоязычных СМИ. Односторонняя подача информации в них упорно выставляет Грузию в виде жертвы российской «военной машины» [408].

При этом, если грузинская сторона построила свою стратегию ведения информационной операции на официальном уровне, пытаясь выиграть за счет массовости в популярных, прежде всего англоязычных изданиях, то южноосетинская сторона сделала ставку на вовлечение в собственную информационную операцию как можно большего числа своих сторонников в сети Интернет [408].

5.6.3. Способы информационно-психологического воздействия на основе электронных коммуникаций и сети Интернет

Далее представлены типовые способы использования электронных каналов информационно-психологического воздействия и сети Интернет в интересах проведения ПсО в вооруженных конфликтах последних десятилетий. В качестве примера рассмотрены способы воздействий через Интернет, используемые в операциях в Ираке в 2003 г., в Афганистане в период 2001–2014 гг., в операции ВС Израиля против группировки «Хамас» в 2008 г. и в операции по принуждению Грузии к миру, проводимой ВС России, в 2008 г.

5.6.3.1. Операция НАТО «Решительная сила» против Югославии в 1999 г.

Агрессия НАТО на Балканах (1999 г.) впервые за всю историю существования альянса сопровождалась мощнейшей информационной поддержкой в Интернете, для чего использовалось множество сайтов, освещавших военную операцию. Большинство из них было создано непосредственно американскими специалистами по компьютерным технологиям или с их помощью. В течение только первых двух недель операции в Косово американское информационное агентство CNN подготовило более 30 статей, размещенных затем во всемирной сети. В среднем в каждой из них около 10 раз встречались слова «беженцы», «этнические чистки», «массовые убийства» [95].

5.6.3.2. Операция США и их союзников «Иракская свобода» («Шок и трепет») в Ираке в 2003 г.

В операции в Ираке (2003 г.) наряду с «классическими» средствами ПсО начали применяться и перспективные методы информационно-психологического воздействия. Так, практиковалась рассылка электронных писем на почтовые ящики иракского руководства, а также SMS-сообщений на мобильные телефоны. Ввиду того, что Интернет был слабо распространен на территории Ирака, а доступ к его ресурсам имелся у незначительной части населения, спецслужбы страны не уделяли должного внимания контролю над электронной перепиской. Это позволяло практически беспрепятственно осуществлять информационно-психологическое воздействие на высокопоставленное политическое и военное руководство Ирака [396].

Высокая эффективность информационно-психологического воздействия через сеть Интернет в военных конфликтах побудила США создать современный высокотехнологичный комплекс электронных СМИ для сил специальных операций (Special Operations Forces Media Operations Complex). Такой комплекс был создан в пункте постоянной дислокации 4-й группы ПсО в Форт-Брэгге (шт. Северная Каролина) в целях оснащения сил ПсО новейшими техническими средствами подготовки и распространения электронных материалов информационно-пропагандистского воздействия. Фактически данный комплекс объединил в одном здании площадью около 5000 кв. м все технические возможности группы ПсО в области электронных средств массовой информации. В частности, он включает оборудование для производства материалов для электронных СМИ (теле-, видео- и аудио), а также техническое оборудование, предназначенное для распространения материалов ПсО через сеть Интернет [95].

Создание такого комплекса оказалось полезным при начале боевых действий в Афганистане и Ираке. Специалисты ПсО США и НАТО формировали на официальных сайтах Министерства обороны специальные разделы, посвященные проводимым операциям. На этих сайтах предоставлялась в максимальной степени полная информация по ситуации, претендовавшая на роль «единственно правдивой» [13].

5.6.3.3. Операция Израиля «Расплавленный свинец» против группировки «Хамас» в 2008 г.

В подготовительный период операции в ВС Израиля был принят ряд ограничительных мер: установлен высокий уровень секретности и разграничения доступа к сведениям для исключения их утечки, у рядового состава частей изъяты мобильные телефоны, так как была известна способность боевиков перехватывать информацию, передаваемую по линиям сотовой связи [407].

Новыми моментами в военной операции являются: открытие новых пропагандистских интернет-ресурсов патриотической направленности; прямая трансляция в сеть Интернет хода авиаударов по наземным объектам. Таким путем демонстрировались возможности средств ВТО (реклама вооружения, психологическое подавление противника), подтверждалась избирательность ударов (контртезис на обвинения об избыточном применении силы), укреплялся моральный дух войск и обеспечивалась поддержка населения [407].

Кроме того, велись взлом и искажение содержания исламистских сайтов, которые высказывались в поддержку «Хамас», а также доведение нужной информации путем массовой рассылки SMS-сообщений жителям Газы. Характерно, что только после этого пропагандистского SMS-вброса на телефоны арабов израильтяне уничтожили станции мобильной связи с целью срыва управления отрядами исламистов [407].

Следует также отметить проведение израильтянами активной радиоразведки и перехвата сообщений в сетях сотовой связи. Так, в условиях затрудненного объективного контроля результатов огневого воздействия значительную часть подобных сведений удавалось получать из перехвата переговоров боевиков, чья радиодисциплина была очень низкой [407].

5.6.3.4. Вооруженный конфликт в Южной Осетии в 2008 г.

Новейший опыт ведения психологических операций с использованием сети Интернет связан с боевыми действиями в Южной Осетии в 2008 г. При начале операции российских войск в Южной Осетии по принуждению Грузии к миру военно-политическое руководство Грузии при поддержке США развернуло информационную войну, противопоставить которой в первое время российская сторона ничего не смогла. В большинстве случаев ситуация складывалась таким образом, что российская сторона упускала инициативу и лишь «отвечала» на домыслы враждебной пропаганды.

Информационная война Грузии против Южной Осетии и Абхазии началась задолго до перехода к активным боевым действиям. Она велась преимущественно на информационно-психологическом поле, хотя периодически стороны пытались заблокировать работу сайтов противника. В этой войне на одной стороне активно выступали Грузия, США, Великобритания, а также страны Прибалтики и Восточной Европы, а на другой — самопровозглашенные республики. Страны Западной Европы в основном соблюдали нейтралитет, хотя и «сочувствовали» Тбилиси. Ключевыми темами информационной войны в это время были историческая (являются ли «сепаратистские регионы» исторически частью Грузии или нет) и правовая (имеют ли эти регионы право на самостоятельное существование или только в пределах Грузии) [408].

Грузинской стороной постоянно устраивались антироссийские провокации с целью оказания информационно-психологического воздействия на мировое общественное мнение (обсуждение падения «российской» ракеты на территорию Грузии с привлечением международных экспертов, скандал вокруг БПЛА грузинских ВС, сбитого над территорией Абхазии, арест российского вооружения, якобы запрещенного к использованию в зоне конфликта, у миротворцев и др.) [408].

Перед началом боевых действий резко активизировалось использование информационно-технических и информационно-психологических воздействий через Интернет.

Так, 8 августа 2008 г. массированной DDoS-атаке подверглись практически все южноосетинские сайты, размещавшие сведения о ходе боев. В частности, некоторое время были недоступны сайты главного информационного агентства «ОСинформ», а также «Осетинского радио и телевидения». Кроме того, в ночь с 7 на 8 августа 2008 г. была нарушена работа официального сайта Государственного комитета по информации и печати Республики Южная Осетия [408].

С грузинской стороны DDoS-атаке подверглись интернет-ресурсы МИДа, МВД, МО, практически всех других национальных министерств и ведомств, а также многих информационных агентств. К примеру, был взломан и практически уничтожен один из ведущих грузинских интернет-ресурсов страны «Грузия on-line». Атакована была и веб-страница национальной телекомпании «Рустави-2». В результате этих действий МИД Грузии вынуждено было завести интернет-дневник на популярном блог-сервисе Blogspot.Com, мотивируя свои

действия невозможностью работы на своем сайте из-за DDOS-атак российской стороны. Массированные атаки на сайты заставили владельцев ряда грузинских сайтов перенести хостинг в США, на площадку американской компании TULIP Systems, однако это мало помогло. По словам специалистов TULIP Systems, начиная с 9 августа 2008 г. они с большим трудом блокировали массированные DDoS-атаки [408].

Начиная с 9 августа 2008 г. массированной хакерской атаке подверглись уже новостные агентства, освещающие события с российской стороны. В частности, на следующий день жертвами атаки хакеров стало РИА «Новости», что затруднило работу практически всех служб агентства и осложнило доступ на сайт www.rian.ru. Кроме того, хакерским атакам подверглись сайты ИТАР-ТАСС, ИА «REGNUM», Lenta.ru, газет «Известия» и «Твой день», а также радиостанции «Эхо Москвы» [408].

Очень важным «полем» информационной войны в Интернете являлись различные форумы и онлайн-голосования. Здесь победа явно осталась на стороне противников США и Грузии, причем не только на русскоязычных сайтах. Примером является флешмоб-накрутка в онлайн-голосовании на сайте CNN. Этот ресурс предложил аудитории оценить действия России по отношению к Грузии. Примерно 92% голосов (более 329 000 человек) было отдано за вариант ответа, признававший поведение России миротворческим, и всего 8% оценили происходящее между двумя странами как вторжение в Грузию. После получения такого результата CNN оперативно закрыла это онлайн-голосование [408].

Южноосетинская сторона изначально была поставлена в гораздо менее комфортные условия для ведения «официальной» информационной войны против Грузии. Кроме российских СМИ и СМИ еще нескольких государств, никто не предоставил возможность для выступления президентов и официальных лиц непризнанных республик. Поэтому основным полем проведения информационных операций для непризнанных республик стал Интернет. В глобальной сети буквально с первого дня агрессии появились фотографии и видеоролики с показом зверств грузинских войск. Гораздо более убедительными, чем прогрузинские, были и выступления представителей южноосетинской стороны на форумах, и их материалы в блогах, причем как на русском, так и на английском языках. Весьма оперативно появились карикатуры и комедийные видеомонтажные ролики на руководящих лиц противостоящей стороны [408].

Не менее активно велась южноосетинской стороной и контрпропагандистская работа. Буквально на следующий день после появления в Интернете фотографий, якобы свидетельствующих о зверствах южноосетинских войск, там же появились их разоблачения как постановочных. Довольно оперативно разоблачались и попытки некоторых англоязычных СМИ выдать фотографии разрушений в Южной Осетии за разрушения в Грузии [408].

По итогам анализа информационно-психологического противоборства можно сделать вывод, что на протяжении пяти дней «горячей войны» в большинстве своем мировое общественное мнение склонялось всё-таки на сторону Южной Осетии. Это говорит о том, что использование «массовых информаци-

онных агентов влияния», ведущих прямой диалог с людьми через Интернет, более эффективно, чем «опосредованный» диалог руководителей государств с народами мира через официальные телевизионные СМИ [408].

5.7. Перспективные технологии способов и средств информационно-психологического воздействия (на основе анализа проектов DARPA)

Разработка новых способов и средств информационного противоборства в психологической сфере требует существенного научно-технического задела во многих областях фундаментальной и прикладной науки. Тенденции перспективных исследований, проводимых в интересах совершенствования способов и средств информационно-психологического воздействия, можно оценить путем анализа проектов, выполняемых Агентством передовых оборонных исследовательских проектов Министерства обороны США — DARPA. Ниже представлена краткая характеристика проектов DARPA за 2015 г., которые напрямую или опосредованно ориентированы на формирование научно-технического задела в области информационно-психологических воздействий.

Графо-теоретические исследования алгоритмов представления эффективной архитектуры для социальных сетей — Graph-theoretical Research in Algorithm Performance & Hardware for Social networks (GRAPHS). Последние события в мире доказывают, что анализ социальных сетей может иметь критическое значение для безопасности государства. В сетевой парадигме узлы представляют собой людей, а их отношения или взаимодействия образуют рёбра графа. В настоящее время методы анализа социальных сетей находятся в начальном состоянии, когда реальные сети представляются в виде грубых и недостаточно адекватных графовых моделей. Программа ориентирована на разработку научного аппарата формализации тонкой математической структуры социальных сетей. Это позволит более точно описать социальные сети, а также их изменения в пространстве и во времени [234].

Социальные СМИ в стратегической коммуникации — Social Media in Strategic Communication (SMISC). Программа направлена на разработку алгоритмов выявления, отслеживания, формирования, развития и распространения идей и понятий «мемов» в социальных сетях. Это позволит в дальнейшем самостоятельно инициировать сообщения и дезинформацию в целях проведения информационных операций в 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 кампаний;
- противодействие враждебным кампаниям с помощью контрсообщений.

Выявление аномалий поведения — Anomaly Detection at Multiple Scales (ADAMS). Программа ADAMS разрабатывает приложения, предназначенные для выявления аномальных процессов, происходящих в обществе, наблюдения за неадекватным поведением отдельных индивидуумов и групп людей [234].

Big Mechanism. 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].

Глобальная количественная аналитика — Quantitative Global Analytics. Программа QGA предусматривает разработку и интеграцию технологий анализа большого объема данных в целях превентивного обнаружения опасных тенденций и глобального прогнозирования. Исходными данными для алгоритмов прогнозирования служит социально-экономическая информация: рыночные цены, уровни производства, показатели международной торговли и уровни экспорта. Предполагается использовать сочетание количественного анализа глобальных и региональных экономических и финансовых данных с математическими методами анализа социальных сетей, количественной социологии и методами климатических исследований. Разработанные технологии позволят повысить ситуационную осведомленность и формировать прогнозы о новых классах политических, экономико-социальных и экологических угроз [234].

Поиск в Интернете — Memex. В рамках программы Memex 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 мощную поисковую систему на основе новых поисковых программ, которая будет способна вести поиск в самых отдаленных уголках Сети, которые недоступны для современных интернет-поисковиков, обеспечивая своим пользователям технологическое превосходство в области индексации контента и веб-поиска [234].

Обработка больших данных — XDATA. В рамках программы XDATA разрабатываются вычислительные методы и программные инструменты анализа больших объемов данных — как «полуструктурированных», так и неструктурированных. Планируется решить следующие основные задачи: создать масштабируемые алгоритмы обработки «сырых» данных в распределенных хранилищах, а также создать эффективные средства взаимодействия чело-

века с компьютером, помогающие с помощью настраиваемой визуализации делать логические выводы из данных, полученных из различных источников [234].

Глобальная система сбора информации, наблюдения и разведки — Worldwide Intelligence Surveillance and Reconnaissance (WISR). Данная система обеспечит выполнение разведывательных задач в недоступных ранее районах. Войска США ограничены в использовании традиционных средств разведки и наблюдения во многих 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-реконструкции событий. Методы WISR также могут быть использованы для отслеживания культурных и социальных изменений при подготовке к вводу на территорию экспедиционных войск [234].

6. Примеры ведения информационного противоборства и радиоэлектронной борьбы в сетецентрических войнах начала XXI века

Наиболее явно сетецентрический характер войн нового поколения проявился в ходе вооруженных конфликтов в Югославии, Ираке, Афганистане, Ливии, в которых участвовали США и НАТО, а также их союзники в конце XX — начале XXI в. 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 сетецентрических войн на примере военных конфликтов конца XX — начала XXI в. с упором на практические аспекты применения в них способов и средств информационного противоборства и систем РЭБ.

6.1. Общие закономерности ведения сетецентрических войн, роль информационного противоборства и радиоэлектронной борьбы в них

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. Вооруженные силы, предназначенные для ведения сетецентрических войн, 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 информационного противоборства и систем РЭБ, действующих в соответствии с законами войны нового поколения [163, 165].

Анализ конкретных военных конфликтов, в которых принимали участие ВС США и ВС стран НАТО и в которых использовались элементы сетецентрической войны, позволили 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 ВС развертывают разветвленные системы информационного обеспечения и мониторинга (преимущественно в космическом и информационном пространствах), а также обеспечивают передовое присутствие своих ВС в местах проекции силы и потенциальных конфликтов. В этот же период производятся накопление запасов дорогостоящего высокоточного оружия дальнего действия и наращивание современных видов ВВТ в количествах, достаточных для ведения крупномасштабной войны.

На начальных этапах конфликта (его 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 уровень жизни населения и формируют благоприятную атмосферу по проведению информационных и психологических 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. Информационные и 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, транспорта, системы государственного и военного управления).

На следующих этапах конфликта (обострение, кризис) 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 оптико-электронная разведка дислокации сил и средств противника, в особенности систем ПВО, а также объектов критической инфраструктуры. Одновременно ведутся создание и поддержка оппозиционных сил в стране-противнике, создание вооруженного ядра оппозиции, основу которого составляют силы специальных операций активной стороны.

Проводятся информационные и психологические операции по дискредитации государственных институтов власти в глазах населения, а также по дезорганизации личного состава вооруженных сил, а также подавления 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 нанесением 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 у ВС средств ВТО 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 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.

6.2. Операция НАТО «Решительная сила» против Югославии в 1999 г.

6.2.1. Общая характеристика операции

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. 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 ВТО 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 рассматривает 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 США и НАТО по применению систем ВТО 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 не готовой 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 до известной степени даже более предпочтительной [173, 174].

По утверждению некоторых средств массовой информации, в ходе ударов югославские ВС потеряли более 10 000 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 Косово 60 единиц уничтоженной бронетехники и артиллерии. Отсутствие достоверной информации о потерях Югославии свидетельствует о плохо налаженном документировании результатов ударов. Уровень и порядок потерь югославских ВС позволяют сделать совершенно иные выводы. Достоверно известно, что до начала войны у сербов имелось 1025 танков и 3750 артиллерийских орудий. Значит, в ходе всей войны силами НАТО 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 и военные источники неоднократно критически оценивали результативность действий НАТО именно в связи с неспособностью альянса нанести решительное поражение ВС Югославии. Однако такая цель и не преследовалась. Главной задачей альянса являлось разрушение экономической инфраструктуры страны и системы ее государственного и военного управления [173].

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 ВС 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 ВС 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 ВС 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 средств ВТО 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 ВС. Однако даже в наиболее развитых странах структура ВС, формы и способы их применения будут меняться не сразу, а по мере принятия на вооружение и накопления достаточного количества ВТО. В течение некоторого времени ВС 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 противосто-

ять ВС 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 признаётся, что войска НАТО были вынуждены прибегнуть к неоптимальным методам нападения в силу необходимости минимизировать собственные потери [2, 29].

6.2.2. Применение средств РЭБ

В ходе воздушно-космическо-морской операции силами НАТО одновременно проводилась операция РЭБ, которая, кроме мощного помехового заградительного и прицельного подавления РЭС государственного и военного назначения Югославии, 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 РЭБ, 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 включавшаяся на излучение, 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, поскольку 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].

6.2.3. Информационно-психологические операции

Для обеспечения военной кампании против Югославии до ее начала НАТО развернуло полномасштабную 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, по крайней мере, к тому, чтобы оно не препятствовало вооруженному вторжению НАТО на Балканы. Активное применение сил и средств психологических операций ВС 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 по 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 — от 20 000 до 40 000 листовок) и авиационных бомб (от 30 000 до 80 000 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 Rammstein (Германия) два самолета EC-130E/J 193-го авиакрыла Национальной гвардии ВВС США. Самолеты ежесуточно барражировали в сопровождении истребителей по периметру югославской границы на высоте 9–10 км и вели трансляцию радио- и телепередач на сербскохорватском и албанском языках в течение 2,5 ч [95].

Основным посылом радио- и 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 количество радиоприемников с фиксированными частотами. Запасы таких радиоприемников были созданы на авиабазах ВВС США в ФРГ [95].

6.3. Операция США и их союзников «Иракская свобода» («Шок и трепет») в Ираке в 2003 г.

6.3.1. Общая характеристика операции

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, будто бы 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, ставило 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 ВС 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 штабы, которые 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 1200 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 ВС 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 р. Тигр и р. 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 решала 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 осуществлялись с широким использованием космических средств. Количество выпущенных КРВБ и КРМБ 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 средств ВТО. В частности, в операции против Ирака в 2003 г. этот показатель был в 8,5 раза больше, чем в 1991 г. [95].

С началом наземной 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 быстрого 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].

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), средств ВТО, средств РЭБ с одновременным проведением мероприятий стратегической и/или оперативной (тактической) маскировки, дезинформации и психологической войны [95].

Анализ применения оружия в военных действиях показывает постоянно растущую роль авиации и высокоточных крылатых ракет различных видов, особенно морского базирования, 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 — 26 600 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 порядка 35 000 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 крылатых ракет, особенно КРМБ, резко возросла. По имеющимся данным, за первые трое суток войны против Ирака было 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 таблице 6.1 приведен вариант расчетов по определению доли составных элементов в первой операции воздушно-космического нападения (ВКН). Как видно из таблицы 6.1, основная роль в достижении целей ВКН принадлежит военной авиации — до 60% объема решаемых задач, вслед за ней идут высокоточные КРМБ и КРВБ [269].

Таблица 6.1 — Соотношение сил и средств ВКН в операции (вариант) [269]

Общее количество сил и средств, привлекаемых к 1-ой 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 РКО, 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-РКО является чрезвычайно трудным, учитывая, что 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, ЗРК и зенитной артиллерии 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 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 МО 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 МО 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 МО США в среднем будет равен 15% от уровня предыдущего года. По другим оценкам, потребность МО 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 — АСУ 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 6.2) показывает, что именно на них придется основная нагрузка при передаче информации. 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 бóльшая часть трафика будет приходиться на арендуемые системы незащищенной широкополосной широковещательной спутниковой связи, предназначенные для вторичного распределения разведывательной информации, графической информации, изображений и видеозаписей [291].

Таблица 6.2 — 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%

6.3.2. Применение средств РЭБ

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, 8 батальонов раз-

ведки 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 7–9 самолетов 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 с технологией 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 ACM-86C бомбардировщики B-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 [16, 292].

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 подобные боеприпасы могли появиться не ранее 2005 г. Это позволяет говорить о том, что по итогам компании 1999 г. против Югославии, в которой впервые были применены средства вывода из строя систем энергоснабжения типа графитовых бомб, руково-

дством 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 не достаточно 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 разрушить коммуникации и каналы связи. Однако уже в последующие дни войны они нарастили средства подавления систем радиосвязи, за счет чего иракские соединения и части практически 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].

6.3.3. Применение средств информационно-технических воздействий

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].

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].

6.3.4. 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].

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 3 из 7 армейских корпусов не принимали активного участия в боевых действиях. ЦРУ оплатило предательство командующих военными округами и обеспечило 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].

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 всё 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 3250 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 РЭБ 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 ВС США и, по замыслу авторов, должны были разъяснять цели и задачи военной операции США, побуждать иракских военнослужащих к отказу от участия в боевых 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 разработанные программы по работе с военнопленными** были реализованы в развернутых объединенным центральным командованием лагерях, а также на корпусных и дивизионных пунктах сбора пленных. Для работы с военнопленными широко 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 порядка 3000 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 задач в ходе войны в Ираке.

Дополнительные сведения о способах используемых в информационно-психологических операциях в войне в Ираке в 2003 г. представлены в подразделах 5.6.2.1 и 5.6.3.2 раздела 5 «Информационное противоборство в психологической сфере».

6.4. Операции США и НАТО «Одиссея. Рассвет» и «Союзный защитник» в Ливии в 2011 г.

6.4.1. Общая характеристика операции

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 использование 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].

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, особенностями операции в Ливии стали 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 ВТО; 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, БПЛА и со средствами ВТО. Данные проблемы стали прямым следствием растущего разрыва между боевыми возможностями ВС США и ВС 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 ВС стран НАТО, 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 НАТО «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 самолетовылетов коалиционной авиации было соразмерно численности правительственных войск (на двух военнослужащих армии М. Каддафи пришлось по одному самолетовылету). 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 БПЛА. 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 полутора месяцев ведения боевых действий запасы авиационных боеприпасов в ВВС Франции сократились до критического уровня, что вынудило руководство Министерства обороны этой страны ввести режим экономии боеприпасов и приступить к экстренным закупкам управляемых ракет и бомб [310].

Еще одним фактором, негативно повлиявшим 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 РЭБ, сил специальных операций, задействованием потенциала частных военных компаний, использованием мобильных возможностей тыла. Результаты такой оценки показывают, что с появлением в ВС основных государств НАТО средств ВТО 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 противником 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 задействованы 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].

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 мероприятия, 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 выходят 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 ВС 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 страны;
- создание и поддержку антиправительственных и националистических 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 в и отношении Сирии.

6.4.2. 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 оценке ряда экспертов, антиправительственные выступления в Ливии (как, впрочем, и в других арабских 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].

Доказательств 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, Франция, Италии и США [309–311].

Ливийские власти в условиях массовых акций гражданского неповиновения и провокаций со стороны воинских формирований оппозиции, когда обычными правоохранительными мерами стабилизировать обстановку не удалось, прибегли к применению против «оппозиции» национальных ВС, включая

боевую авиацию. Это позволило западным странам начать информационную кампанию 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, в причинах столь быстрого обострения обстановки, в источниках и происхождении оружия у оппозиции, и принадлежности членов боевых отрядов к 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 решили дистанцироваться от непосредственного участия в боевой части операции и уступили общее командование коалиционными силами НАТО. В НАТО отказались от американского названия операции и дали 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 Средиземноморского побережья Ливия была блокирована военно-морскими силами США и НАТО, осуществлявшими 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].

6.4.3. Информационно-психологические операции

В составе психологических операций, ориентированных на элиту страны, широкое распространение получили финансово-экономические способы воздействия, включая расширение практики подкупов и шантажа влиятельных лиц. Уникальность Ливийской войны заключается и в том, что не менее эффективно, чем боевые действия, использовались финансовый подкуп и финансирование побега генеральских семей. Как полагают на Западе, задействование финансовых способов позволяет экономить значительные средства на проведение военной операции. В XXI веке это уже вторая операция (после Ирака), где финансовым оружием достигался прогресс, сопоставимый с эффектом воздушной операции [314].

Страны 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 высокопоставленными 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 неформальном табеле 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 Триполи и перешел в Бенгази, уведя с собой лично созданные им подразделения военной полиции [314].

В результате этих действий к февралю 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. офицеры бросали свои подразделения, исчезая в неизвестном направлении, а среди солдат, не понимающих, за что они воюют, началось повальное дезертирство. При этом недовольство большей части ливийских военнослужащих и успешность финансовых операций были вызваны еще и тем, что М. Каддафи выделял среди них «своих» и, соответственно, платил им больше [314].

Непосредственно в ходе операции для психологического воздействия на рядовой и офицерский состав ВС, а также на мирных жителей 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 ВС 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 ВС 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].

6.4.4. Применение средств РЭБ

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 М. Каддафи.

К решению задач РЭБ при проведении операции были привлечены самолеты разведки и радиоэлектронной борьбы RC-135, EC-130H, 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 РЭБ 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, задействуются 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].

6.4.5. Применение средств информационно-технических воздействий

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 ВС 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, информационно-технический доступ 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].

Заключение

На протяжении 80–90-х гг. прошлого века информационные технологии за счет своего революционного развития проникали во все сферы жизнедеятельности человека. Это в конечном итоге привело к тому, что уровень использования новых информационных возможностей, степень развитости информационных сетей и систем, а также степень их интеграции стали важными показателями развитости государства. В этих условиях возникли новые, специфичные именно для информационной эпохи угрозы и, как следствие, новые формы ведения боевых действий. При этом именно информационные технологии обеспечили прорывное развитие средств вооружений и систем управления ими. 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 армии. Это, в свою очередь, обусловило и изменение подходов к ведению войны. В условиях «тотальной информатизации» получила распространение концепция сетецентрической войны как стратегического взгляда на ведение войны в новых военно-технических условиях. Вместе с тем эта концепция является уязвимой для средств информационного воздействия — систем радиоэлектронной борьбы, систем и способов информационного противоборства. Именно эти системы и способы могут обеспечить решительный перевес в будущей сетецентрической войне и нивелировать преимущество технологически более развитого противника. Таким образом, концепция сетецентрических войн выводит на новый качественный уровень как новую среду ведения военного противоборства — информационное пространство, так и новый вид вооружения — информационное оружие. В настоящей работе, по мнению автора, были глубоко проанализированы роль и место радиоэлектронной борьбы и информационного противоборства в современной сетецентрической войне. Проведен анализ тенденций развития систем радиоэлектронной борьбы и информационного противоборства, а также типовых способов их применения на основе анализа вооруженных конфликтов в Югославии, Ираке и Ливии.

В настоящее время радиоэлектронная борьба является наиболее старейшей и в наибольшей степени методически развитой областью ведения противоборства за счет воздействия на информационные параметры конфликтующих военно-технических систем. По глубокому убеждению автора, именно теория радиоэлектронной борьбы за более чем вековую историю своего активного развития содержит многократно апробированные и высокоэффективные способы воздействия на информационно-технические системы, основанные на дестабилизации информационного обмена. И развитие теории информационного противоборства (особенно в технической сфере) должно быть основано на научно-методическом заделе в этой области.

В свою очередь, развитие теории информационного противоборства привело к декомпозиции ее по сферам применения — психологическую и техническую. В настоящее время, на взгляд автора, теория информационного противо-

борства в психологической сфере является в большей степени развитой, нежели теория противоборства в технической сфере. Возможно, это объясняется общей гуманитарной направленностью данных исследований, а также существенным научным заделом, сформированным в теории психологии, в поведенческих, а также в когнитивных науках к концу XX в. Вместе с тем теория информационного противоборства в технической сфере в настоящее время еще находится в стадии становления и развития. Терминологический аппарат в этой области отличается противоречивостью и неоднозначностью, а для ее методов зачастую характерен эмпирический, а не системный подход. В соответствующем разделе работы представлен авторский взгляд на классификацию средств и способов информационно-технических воздействий, которая в дальнейшем может быть использована для развития отдельных аспектов информационного противоборства в технической сфере.

Автор выражает надежду на то, что результат его работы будет встречен с интересом широким кругом специалистов. Он надеется на то, что материал, обобщенный им в монографии, вызовет благосклонное внимание соискателей ученых степеней, военных и технических специалистов, которые выбрали сложные и увлекательные проблемы радиоэлектронной борьбы и информационного противоборства в качестве области своих интересов.

Список используемых сокращений

AARGM — Advanced Anti-Radiation Guided Missile — перспективная управляемая противорадиолокационная ракета;

ABL — Airbome Laser — проект «воздушный лазер»;

ALOHA — протокол случайного множественного доступа в спутниковых сетях связи;

ARP — Address Resolution Protocol — протокол разрешения адресов;

AWACS — Airborne Warning and Control System — система дальнего радиолокационного обнаружения и управления;

AEA — Airborne Electronic Atack — программа по применению авиационных групповых средств РЭБ в рамках единого комплекса;

AMMP — AEA Mission Management Processing — подсистема обработки и управления комплексом РЭБ AEA;

BIOS — Basic Input-Output System — базовая система ввода-вывода;

BND — Bundesnachrichtendienst — Федеральная разведывательная служба Германии;

C3CM — Command, Control and Communication Counter Measures — борьба с системами боевого управления (концепция);

C4ISR — Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance — системы управления, связи, компьютерного обеспечения, разведки и наблюдения (концепция);

CAPEC — Common Attack Pattern Enumeration and Classification — общий каталог и классификатор атак;

CASE — Computer-Aided Software Engineering — набор инструментов и методов программной инженерии для проектирования программного обеспечения, который помогает обеспечить высокое качество программ, отсутствие ошибок и простоту в обслуживании программных продуктов;

CBU — Cluster bomb units — авиационные кассетные бомбы;

CCJ — Core Component Jammer — ядро компонент для создания нового комплекса радиоэлектронной борьбы (для ВС США);

CEASAR — Communications Electronic Attack with Surveillance and Reconnaissance — комплекс РЭБ и радиоэлектронной разведки (в ВС США);

CHAMP — Counter-electronic High Power Microwave Advanced Missile Project — проект демонстрационного образца нелетального СВЧ-оружия, размещаемого на воздушной платформе (для ВС США);

CIWS — Close-In Weapon System — орудийная система ближнего боя;

COIL — Chemical Oxygen Iodine Laser — химический лазер;

DARPA — Defense Advanced Research Projects Agency — Управление перспективных исследовательских проектов Министерства обороны США;

DCC — Defensie Cyber Command — подразделение для ведения кибероперациий (Нидерланды);

DDoS — Distributed Denial of Service — распределенная компьютерная атака «отказ в обслуживании»;
DEA — Defensive Electronic Attack — комплекс радиоэлектронной защиты (в ВС США);
DNS — Domain Name System — система доменных имен в сети Интернет;
DoS — Denial of Service — компьютерная атака «отказ в обслуживании»;
DRFM — Digital Radio Frequency Memory — цифровое устройство запоминания радиочастот;
DVB — Digital Video Broadcasting — стандарт цифрового видеовещания;
DVB-RSC — Digital Video Broadcasting with Return Satellite Chanel — стандарт спутниковой цифровой передачи данных с обратным каналом через спутник;
DVB-S — Digital Video Broadcasting — Satellite — стандарт спутниковой цифровой передачи данных;
DWS — Distributed Wargaming System — система, объединившая модели различных уровней;
EBO — Effect-based Operations — действия на основе эффектов (концепция);
EFVS — Electronic Fight Vehicle System — мобильная система радиоэлектронной борьбы;
EIGRP — Enhanced Interior Gateway Routing Protocol — дистанционно-векторный протокол динамической маршрутизации;
EVFS — Encrypted Virtual File System — зашифрованная виртуальная файловая система;
EWPMT — Electronic Warfare Planning and Management Tools — комплекс планирования и управления радиоэлектронной борьбой;
FCS — Future Combat Systems — Боевые системы будущего (программа ВС США);
FEL — Free Electron Laser — лазер на свободных электронах;
FSD — Federal Service of Data — Федеральная служба данных (США);
FSRS — Frequency Selective Receiver System — частотно-избирательная приемная система;
FTP — File Transfer Protocol — протокол передачи файлов;
GCCS — Global Command Control System — глобальная система оперативного управления (в ВС США);
GCHQ — Government Communications Headquarters — центр правительственной связи (Великобритания);
GIG — Global Information Grid — глобальная информационно-управляющая сеть (в ВС США);
GSM — Global System for Mobile Communications — глобальный стандарт цифровой мобильной сотовой связи;
HARM — High-speed Anti-Radar Missile — высокоскоростная противорадиолокационная ракета;

HEL MD — High Energy Laser Mobile Demonstrator — опытный высокоэнергетический мобильный лазер;

HIRAT — High-power Ram Air Turbine — высокомощные генераторные турбины набегающего потока;

HMMWV — High Mobility Multipurpose Wheeled Vehicle — высокоподвижное многоцелевое колесное транспортное средство (автомобиль «Хаммер»);

HPM — High Power Microwave — СВЧ или микроволновое оружие;

HTTP — HyperText Transfer Protocol — протокол для передачи гипертекстовых документов;

ICDT — Integrated Capabilities Development Team — группа по развитию комплексных возможностей;

ICMP — Internet Control Message Protocol — протокол межсетевых управляющих сообщений;

IEWCS — Intelligence and Electronic Warfare Common Sensor — единые средства разведки и электронной войны (программа в ВС США);

IEWS — The Integrated Electronic Warfare System — интегрированная система радиоэлектронной борьбы;

IM — Internet Massager — Интернет-пейджер;

INCANS — INterference CANcellation System — устройство исключения собственных помех;

INSCOM — Intelligence and Security Command — Командование разведки и безопасности;

IP — Internet Protocol — Интернет-протокол;

IRC — Internet Relay Chat — протокол для обмена информацией в чатах и форумах;

IS-IS — Intermediate System to Intermediate System — протокол динамической маршрутизации, основанный на технологии оценки состояния каналов;

JIVC — Joint IT branch — объединенный центр информационных технологий;

JMCIS — Joint Military Command Information System — система информационного обеспечения объединенного командования;

JOTS — Joint Operational Tracking System — объединенная система оперативного отслеживания обстановки (в ВС США);

JTIDS — Joint Tactical Information Distribution System — объединенная распределенная боевая информационная система (в ВС США);

JTLS — Joint Theater Level Simulation — имитационная система моделирования боевых действий;

JWARS — Joint Warfare System — объединенная система моделирования боевых действий;

LAN — Local Area Network — компьютерная сеть;

LAR — Leaflet Artillery Round — листовочный артиллерийский снаряд;

LaWS — Laser Weapon System — лазерная система вооружения;

LBU — Leaflet Bomb Unit — листовочный авиационный боеприпас;

MALD — Miniature Air-Launched Decoy — миниатюрная воздушная ложная цель;

MEII — Minimum Essential Information Infrastructure — минимально необходимая информационная инфраструктура;

MFEW — Multi-Function Electronic Warfare — многофункциональный комплекс радиоэлектронной войны;

MIMO — Multiple Input — Multiple Output — система «множество входов — множество выходов»;

MISO — Military Information Support Operation — подразделение информационного обеспечения (в ВС США);

MLD — Maritime Laser Demonstrator — опытный морской лазер;

NCE JFC — Net-Centric Environment Joint Functional Concept — концепция объединенной функциональной сетецентрической среды;

NCSC — National Cyber Security Centre — национальный центр компьютерной безопасности;

NCSS — National Cyber Security Strategy — государственная политика кибербезопасности (в США);

NCW — Network-Centric Warfare — сетецентрическая война;

NERO — Networked Electronic Warfare, Remotely Operated — сетевой комплекс радиоэлектронной войны с дистанционным управлением;

NGJ — Next Generation Jammer — система радиоэлектронного подавления следующего поколения;

NSA — National Security Agency — агентство национальной безопасности (США);

OADV — Ad hoc On-Demand Distance Vector — протокол динамической маршрутизации для мобильных ad-hoc сетей (MANET) и других беспроводных сетей;

OSI — Open System Interconnection — эталонная модель взаимодействия открытых систем;

OSINT — Open Source Intelligence — разведка на основе анализа открытых источников информации;

OSPF — Open Shortest Path First — протокол динамической маршрутизации, основанный на технологии оценки состояния каналов;

P2P — Pear-to-Pear — пиринговая файлообменная сеть;

PDU — PSYOP Dispensing Unit или Printed Data Unit — боеприпас для распространения печатных материалов;

PGP — Pretty Good Privacy — протокол с открытым ключом для шифрования сообщений;

PSYOP — Psychological Operations — подразделения психологических операций (в ВС США);

RAND — Research and Development — Центр стратегических исследований и разработок (в США);

RAT — Ram Air Turnbine — генераторная турбина набегающего потока;

RDO — Rapid Decisive Operations — быстрые решающие действия (концепция в ВС США);

RFW — Radio Frequency Weapon — радиочастотное оружие;
SINCGARS — Single Channel Ground and Airborne Radio System — система бортовой связи и связи с Землей;
SIRPA — Service d Information et de Relations Publiques des Armées — служба информации и общественных связей (Франция);
SOMS — Special Operations Media System — мобильные комплексы телерадиовещания;
SPEAR — Special Purpose Emitter Array — комплекс радиоэлектронного подавления УКВ-средств радиосвязи и навигации;
SPIN — Segmented, Polycentric, Ideologically Integrated Network — сегментированная, полицентрическая, идеологизированная сеть;
SSL — Secure Sockets Layer — криптографический протокол шифрования данных в рамках соединения;
TCP — Transmission Control Protocol — протокол управления передачей данных;
TDMA — Time Division Multiple Access — множественный доступ с разделением по времени;
TLS — Tactical Laser System — тактическая лазерная система;
TRACS — Tactical Radio Acquisition and Countermeasures Subsystem — тактическая система радиоразведки и радиоэлектронного подавления;
TRADOC — (United States Army) Training and Doctrine Command — Командование по боевой подготовке и доктринам сухопутных войск (США);
TTD — True Time Delay — задержка сигнала в реальном масштабе времени;
UDP — User Datagram Protocol — протокол передачи пользовательских данных;
USB — Universal Serial Bus — интерфейс универсальной последовательной шины;
USCYBERCOM — United States Cyber Command — Кибернетическое командование ВС США;
USIA — United States Information Agency — Информационное агентство США;
VGA — Video Graphics Array — компонентный видеоинтерфейс, используемый в мониторах и видеоадаптерах;
VPN — Virtual Private Network — виртуальная частная сеть;
WWW — World Wide Web — распределенная система (паутина), предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключенных к Интернету;
АЛВЦ — автономная ложная воздушная цель;
АМ — амплитудная модуляция;
АНБ — агентство национальной безопасности (США);
АСУ — автоматизированная система управления;
АФАР — активная фазированная антенная решетка;
АФМ — автофукусировка матрицы;

АЦП — аналогово-цифровой преобразователь;
БД — база данных (по контексту);
БД — боевые действия (по контексту);
БИС — большая интегральная схема;
БПЛА — беспилотный летательный аппарат;
БР — баллистическая ракета;
БРЛС — бортовая радиолокационная станция;
БРЭО — бортовое радиоэлектронное оборудование;
БТР — бронетранспортер;
БЦВМ — бортовая цифровая вычислительная машина;
БЧ — боевая часть;
ВВС — Военно-воздушные силы;
ВВТ — вооружение и военная техника;
ВКН — воздушно-космическое нападение;
ВМБ — военно-морская база;
ВМГ — взрывомагнитный генератор;
ВМС — Военно-морские силы;
ВПК — военно-промышленный комплекс;
ВС — Вооруженные силы;
ВТА — военно-транспортная авиация;
ВТО — высокоточное оружие;
ВЦ — воздушная цель;
ВЧ — высокие частоты (диапазон радиосвязи);
ГСН — головка самонаведения;
ДКМ — декаметровый (диапазон радиосвязи);
ДРЛО — (самолет) дальнего радиолокационного обзора;
ЕС — Европейский союз;
ЗА — зенитная артиллерия;
ЗАК — зенитно-артиллерийский комплекс;
ЗПП — забрасываемый передатчик помех;
ЗРВ — зенитно-ракетные войска;
ЗРК — зенитно-ракетный комплекс;
ЗУР — зенитная управляемая ракета;
ИА — истребительная авиация;
ИД РЛС — импульсно-доплеровская радиолокационная станция;
ИК — инфракрасный (диапазон электромагнитных волн);
ИПВ — информационно-пропагандистское воздействие;
ИС — интегральная схема;
ИТ — информационные технологии;
ИТВ — информационно-техническое воздействие;
КА — космический аппарат;
КВ — короткие волны (диапазон радиосвязи);
КНДР — Корейская Народно-Демократическая Республика;
КНР — Китайская Народная Республика;
КНШ — Комитет начальников штабов (ВС США);

КПД — коэффициент полезного действия;
КР — крылатая ракета;
КРВБ — крылатая ракета воздушного базирования;
КРМБ — крылатая ракета морского базирования;
КШУ — командно-штабные учения;
ЛА — летательный аппарат;
ЛВС — локальная вычислительная сеть;
ЛВЦ — ложная воздушная цель;
ЛПР — лицо, принимающее решение;
ЛРС — линия радиосвязи;
ЛЦ — ложная цель;
ЛЧМ — линейная частотная модуляция (вид радиосигнала);
МВ — метровые волны (диапазон радиосвязи);
МВД — Министерство внутренних дел;
МИД — Министерство иностранных дел;
ММВ — миллиметровые волны (диапазон электромагнитных волн);
МО — Министерство обороны;
МОП — металл-оксид-полупроводник;
МППУ — малогабаритные приемопередающие устройства;
МСВЧ — монолитные сверхвысокочастотные (интегральные схемы);
МСД — множественный случайный доступ;
МТС — материально-технические средства;
МФ РЛС — многофункциональная радиолокационная станция;
НАТО — Организация Североатлантического договора;
НИОКР — научно-исследовательские и опытно-конструкторские работы;
НИР — научно-исследовательская работа;
НЛЦ — низколетящая цель;
НОАК — Народно-освободительная армия Китая;
НЦ — надводная цель;
ОБЧ — обычная боевая часть;
ОВС — объединенные вооруженные силы;
ОВЦ — обнаружение воздушных целей;
ОВЧ — очень высокие частоты (диапазон радиосвязи);
ОНЦ — обнаружение надводных целей;
ООН — Организация Объединенных Наций;
ООФ — объединенное оперативное формирование;
ОПК — оборонно-промышленный комплекс;
ОС — операционная система;
ОСШП — отношение сигнал/(шум+помеха);
ОЭА — оптико-электронное оборудование;
ОЭР — оптико-электронная разведка;
ОЭС — оптико-электронное средство;
ПВО — противовоздушная оборона;
ПЗС — прибор с зарядовой связью;
ПК — персональный компьютер;

ПКР — противокорабельная ракета;
ПЛИС — программируемая логическая интегральная схема;
ПО — программное обеспечение;
ПОИ — передатчики одноразового использования;
ПРО — противоракетная оборона;
ПсО — психологическая операция;
ПУ — пункт управления;
ПЭМИН — побочные электромагнитные излучения и наводки;
РИО — радиоэлектронно-информационное обеспечение;
РЛП — радиолокационный пост;
РЛР — радиолокационная разведка;
РЛС ММ — радиолокационная станция миллиметрового диапазона;
РЛС СЦ — радиолокационная станция слежения за целью;
РЛС УО — радиолокационная станция управления оружием;
РЛС ЦР — радиолокационная станция целераспределения;
РЛС — радиолокационная станция;
РР — радиоразведка;
РРЛ — радиорелейная линия (радиосвязи);
РРТР — радио- и радиотехническая разведка;
РСЗО — ракетная система залпового огня;
РТВ — радиотехнические войска;
РТР — радиотехническая разведка;
РУК — разведовательно-ударный комплекс;
РФ — Российская Федерация;
РЭА — радиоэлектронная аппаратура;
РЭБ — радиоэлектронная борьба;
РЭВ — радиоэлектронная война;
РЭЗ — радиоэлектронная защита;
РЭК — радиоэлектронный комплекс;
РЭО — радиоэлектронное оборудование;
РЭП — радиоэлектронное подавление;
РЭПр — радиоэлектронное поражение;
РЭР — радиоэлектронная разведка;
РЭС — радиоэлектронное средство;
САОРИ — системы с апостериорной обработкой результатов измерения;
СБ — Совет безопасности (ООН);
СБИС — сверхбольшие интегральные схемы;
СВ — средние волны (диапазон радиосвязи);
СВ — Сухопутные войска (по контексту);
СВЧ — сверхвысокая частота (диапазон радиосвязи);
СМИ — средства массовой информации;
СНР — система наведения ракет;
СОЦ — система отслеживания цели;
СПО — станция предупреждения об облучении;
СПС — специальные программные средства;

ССО — силы специальных операций;
ССС — система спутниковой связи;
СССР — Союз Советских Социалистических Республик;
СУБД — система управления базой данных;
СУВО — система управления войсками и оружием;
СУРН — система управления ракетным нападением;
США — Соединенные Штаты Америки
ТА — тактическая авиация;
ТВД — театр военных действий;
ТНК — транснациональная корпорация;
ТРЛ — тропосферная радиолиния (радиосвязи);
ТТХ — тактико-технических характеристики;
УВД — управление воздушным движением;
УВЧ — ультравысокие волны (диапазон радиосвязи);
УИС — управление информационными системами;
УКВ — ультракороткие волны (диапазон радиосвязи);
УО — управление оружием;
УС — узел связи;
УФ — ультрафиолетовый (диапазон электромагнитных волн);
ФА — фронтовая авиация;
ФАР — фазированная антенная решетка;
ФБР — Федеральное бюро расследований (США);
ФКМ — фазово-кодовая модуляция (сигнала);
ФМ — фазовая модуляция (сигнала);
ФП ЭМИ — функциональное поражение электромагнитным излучением;
ФРГ — Федеративная Республика Германия;
ФРЭПр — функциональное радиоэлектронное поражение;
ФСТЭК — Федеральная служба по техническому и экспортному контролю (России);
ЦАП — цифро-аналоговое преобразование;
ЦРУ — Центральное разведывательное управление (США);
ЧМ — частотная модуляция (сигнала);
ЭВМ — электронно-вычислительная машина;
ЭВС — электронно-вычислительное средство;
ЭДС — электродвижущая сила;
ЭЛТ — электронно-лучевая трубка;
ЭМ — электромагнитный;
ЭМВ — электромагнитная волна;
ЭМИ — электромагнитное излучение;
ЭМО — электромагнитное оружие;
ЭМП — электромагнитное поле;
ЭПР — эффективная площадь рассеивания;
ЭЦП — электронная цифровая подпись.

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. № 048. 14.03.1996.
13. Буренок В. М., Ивлев А. А., Корчак В. Ю. Развитие военных технологий XXI века: проблемы планирование, реализация. — Тверь: Издательство ООО «КУПОЛ», 2009. — 624 с.
14. Буренок В. М., Ляпунов В. М., Мудров В. И. Теория и практика планирования и управления развитием вооружения / Под ред. А.М. Московского. — М.: Изд-во «Вооружение. Политика. Конверсия», 2005. — 418 с.
15. Гуржеянц Т. В., Дербин Е. А., Крылов Г. О., Кубанков А. Н. Информационные операции современности: учеб. пособие. — М.: ВАГШ, 2003. — 286 с.
16. Бедрицкий А. В. Информационная война: концепции и их реализация в США / Под ред. Е.М. Кожокина. — М.: РИСИ, 2008. — 187 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. Слипченко В. И. Войны нового поколения: дистанционные бесконтактные. — М.: ОЛМА-ПРЕСС Образование, 2004. — 382 с.

19. Мир после кризиса. Глобальные тенденции — 2025: меняющийся мир. Доклад национального разведывательного совета США. — М.: Издательство «Европа», 2009. — 188 с.

20. Кара-Мурза С. Г. Манипуляция сознанием. — М., 2000. — 490 с. — URL: http://kob.in.ua/pictures/knigi/murza/manipulation.pdf (дата обращения: 22.01.2014).

21. Лавренов С. Я. Война XXI века: Стратегия и вооружение США. — М.: ООО «Издательство АСТ», 2005. — 314 с.

22. Микрюков В. Ю. Война: наука и искусство. Монография в 4 кн. — М.: Издательство «Русайнс», 2016.

23. Попов И. М., Хамзатов М. М. Война будущего: концептуальные основы и практические выводы. Очерки стратегической мысли. — М.: Кучково поле, 2016. — 832 с.

24. Хазматов В. В. Влияние концепции сетецентрической войны на характер современных операций // Военная мысль. 2006. № 7. С. 13-17.

25. Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография / Под общ. ред. С.Ф. Боева — Иннополис: Афина, 2017. — 440 с.

26. Грачев Г. В., Мельник И. К. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. — М.: ИФ РАН, 1999.

27. Вихров В. Доктрина Обамы: контроль над потоками энергоносителей в Китай // Центр 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.: Издательство «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. Щекотихин В. М., Королёв А. В., Королёва В. В. и др. Информационная война. Информационное противоборство: теория и практика. Монография / Под общ. ред. В.М. Щекотихина. — М.: Академия ФСО России, ЦАТУ, 2010. — 999 с.

33. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. — М.: Изд-во РАГС, 1998. — 125 с.

34. Бухарин С. Н., Цыганов В. В. Методы и технологии информационных войн. — М.: Академический проект, 2007. — 382 с.

35. Цыганов В. В., Бухарин С. Н. Информационные войны в бизнесе и политике: теория и методология. Монография. — М.: Академический проект, 2007. — 336 с.

36. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь. 2011. № 3. С. 41-47. — URL: https://cyberleninka.ru/article/n/problemy-i-perspektivy-primeneniya-kiberneticheskogo-oruzhiya-v-sovremennoy-setetsentricheskoy-voyne (дата обращения: 17.01.2017).

37. Модестов С. А. Информационное противоборство как фактор геополитической конкуренции. — М.: Издательский центр учебных и научных программ, 1998. — 63 с.

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. Сб. статей. 2011. [Электронный ресурс]. — 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. Сб. 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., 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).

47. Кондратьев А. Е. Общая характеристика сетевых архитектур, применяемых при реализации перспективных сетецентрических концепций ведущих зарубежных стран // Военная мысль. 2008. № 12. С. 63-74.

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. Е. Трансформация ВВС США в рамках концепции «сетецентрическая война» // Аэрокосмическое обозрение: Аналитика, комментарии, обзоры. 2007. № 6. С. 54.

52. Панарин И. Н.Информационная власть и война: монография. — М.: Мир безопасности, 2001. — 224 с.

53. Панарин И. Н. Информационная война и геополитика: монография. — М.: Поколение, 2006. — 560 с.

54. Лисичкин В. А., Шелепин Л. А. Третья мировая (информационно-психологическая) война. — М.: Институт социально-политических исследований АСН, 1999. — 304 с.

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. 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.

66. 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.

67. 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.

68. Гречишников Е. В., Добрышин М. М. Оценка эффективности деструктивных программных воздействий на сети связи // Системы управления, связи и безопасности. 2015. № 2. С. 135-146. — URL: http://journals.intelgr.com/sccs/archive/2015-02/05-Dobrushin.pdf (дата обращения: 18.01.2017).

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. Расторгуев С. П. Математические модели в информационном противоборстве. Экзистенциальная математика. — М.: АНО ЦСОиП, 2014. — 260 с.

80. Караяни А. Г., Зинченко Ю. П. Информационно-психологическое противоборство в войне: история, методология, практика: учебник для курсантов и студентов вузов. — М.: МГУ, 2007. — 172 с.

81. Волкогонов Д. А. Психологическая война. — М. Воениздат, 1984. — 320 с.

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. Волковский Н. Л. История информационных войн. — СПб.: ООО Издательство «Полигон», 2003. — 630 с.

84. Арзуманян Р. В. Кромка Хаоса. Сложное мышление и сеть: парадигма нелинейности и среда безопасности XXI века. — М.: Издательский Дом «Регнум», 2012. — 600 с.

85. Минаев В. А., Овчинский А. С., Скрыль С. В., Тростянский С. Н. Как управлять массовым сознанием: современные модели. — М., 2012. — 213 с.

86. Новиков В. К. Информационное оружие — оружие современных и будущих войн. — М.: Горячая линия – Телеком, 2011. — 264 с.

87. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия // Труды Института системного анализа Российской академии наук. 2009. Т. 41. С. 104-146.

88. Давыдов А. Е., Максимов Р. В., Савицкий О. К. Безопасность ведомственных интегрированных инфокоммуникационных систем. — СПб.: ФГУП «НИИ «МАСШТАБ», 2011. — 192 с.

89. Коцыняк М. А., Кулешов И. А, Лаута О. С. Устойчивость информационно-телекоммуникационных сетей. — СПб.: Издательство Политехнического университета, 2013. — 93 с.

90. Коцыняк М. А., Осадчий А. И., Коцыняк М. М., Лаута О. С., Дементьев В. Е., Васюков Д. Ю. Обеспечение устойчивости информационно-телекоммуникационных систем в условиях информационного противоборства. — СПб.: ЛО ЦНИИС, 2015. — 126 с.

91. Климов С. М. Методы и модели противодействия компьютерным атакам. — Люберцы: Каталист, 2008. — 316 с.

92. Климов С. М., Сычев М. П., Астрахов А. В. Противодействие компьютерным атакам. Методические основы: Электронное учебное издание. — М.: МГТУ имени Н.Э. Баумана, 2013. — 108 с.

93. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов / Под ред. О.И. Шелухина. — М.: Горячая линия-Телеком, 2013. — 220 с.

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. Гриняев С. Н. Системы обнаружения вторжений и реагирования на компьютерные инциденты на основе мобильных программ-агентов. — М.: АНО ЦСОиП, 2005. — 46 с.

97. Семенов С. С., Гусев А. П., Барботько Н. В. Оценка информационно-боевого потенциала сторон в техносферных конфликтах // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 6. С. 10-21.

98. Емелин В. И. Методы и модели оценки и обеспечения информационной безопасности автоматизированных систем управления критическими системами. Дисс. … докт. техн. наук. — СПб: СПИИРАН, 2012. — 239 с.

99. Белоножкин В. И., Остапенко Г. А. Информационные аспекты противодействия терроризму. — М.: Горячая линия – Телеком, 2009. — 112 с.

100. Бутузов В. В., Бурса М. В., Остапенко А. Г., Калашников А. О., Остапенко Г.А. Информационные риски флуд-атакуемых компьютерных систем / Под ред. Д.А. Новикова. — Воронеж: Научная книга, 2015. — 160 с.

101. South Korea raises alert after hackers attack broadcasters, banks // Reuters [Электронный ресурс]. 20.03.2013. — URL: http://www.reuters.com/article/net-us-korea-cyber-outage-idUSBRE92J06F20130320 (дата обращения: 19.01.2016).

102. Korean military to prepare with U.S. for cyber warfare scenarios // Yonhap News Agency [Электронный ресурс]. 01.04.2013. — URL: http://english.yonhapnews.co.kr/national/2013/04/01/20/0301000000AEN20130401004000315F.HTML (дата обращения: 19.01.2016).

103. APT1: разоблачение китайской организации, занимавшейся промышленным кибершпионажем // Хабрахабр. Блог компании ESET NOD32 [Электронный ресурс]. 23.02.2013. — URL: https://habrahabr.ru/company/eset/blog/170285/ (дата обращения: 19.01.2016).

104. Stokes M. A., Lin J., Hsiao L. C. R. The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure [Электронный ресурс]. 2011. — 11 p. — URL: http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf (дата обращения: 19.01.2016).

105. In North Korea, hackers are a handpicked, pampered elite // Reuters [Электронный ресурс]. 05.12.2014. — URL: http://www.reuters.com/article/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205 (дата обращения: 19.01.2016).

106. Gardner J. Inside the secretive world of Bureau 121: The North Korean genius state-sponsored hackers believed to be behind the Sony take-down // The Daily Mail [Электронный ресурс]. 05.12.2014. — URL: http://www.dailymail.co.uk/news/article-2861724/In-North-Korea-hackers-handpicked-pampered-elite.html (дата обращения: 19.01.2016).

107. Власти США назвали акцию хакеров против Sony крупнейшей в истории // Интерфакс [Электронный ресурс]. 08.01.2015. — URL: http://www.interfax.ru/world/416965 (дата обращения: 19.01.2016).

108. Chinese Army Unit Is Seen as Tied to Hacking Against U.S. // New York Times [Электронный ресурс]. 18.02.2013. — URL: http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?emc=na&_r=1& (дата обращения: 19.01.2016).

109. Chinese military unit behind 'prolific and sustained hacking' // BBC News [Электронный ресурс]. 19.02.2013. — URL: http://www.bbc.com/news/world-asia-china-21502088 (дата обращения: 19.01.2016).

110. US embassy cables: China uses access to Microsoft source code to help plot cyber warfare, US fears // The Guardian [Электронный ресурс]. 04.12.2010. — URL: https://www.theguardian.com/world/us-embassy-cables-documents/214462 (дата обращения: 19.01.2016).

111. Fritz J. How China will use cyber warfare to leapfrog inmilitary competitiveness // Culture Mandala. The Bulletin of the Centre for East-West Cultural and Economic Studies. Vol. 8. № 1. Pp. 28-80. — URL: http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm (дата обращения: 19.01.2016).

112. 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).

113. Bodnar J. W. The Military Technical Revolution — From Hardware to Information // Naval War College Review. 1993. Vol. 46. p. 7.

114. Defensie Cyber Strategie // Ministerie van Defensie [Электронный ресурс]. 2012. — URL: https://www.defensie.nl/onderwerpen/cyber-security/inhoud/defensie-cyber-strategie (дата обращения: 19.01.2016).

115. Cyber commando // Ministerie van Defensie [Электронный ресурс]. 2016. — URL: https://www.defensie.nl/onderwerpen/cyber-security/inhoud/cyber-commando (дата обращения: 19.01.2016).

116. Китай впервые признал наличие хакерских подразделений в армии // Xakep [Электронный ресурс]. 19.03.2015. — URL: https://xakep.ru/2015/03/19/china-cyberwar/ (дата обращения: 19.01.2016).

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. IDF Record Book 2010 // Bamahane. 2010. № 3052.

120. Израиль намерен вложить миллионы долларов в кибервойска // Securitylab.ru [Электронный ресурс]. 02.11.2012. — URL: http://www.securitylab.ru/news/432017.php (дата обращения: 23.02.2016).

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. Fischer M. German armed forces equipping for cyber war // Stars and Stripes [Электронный ресурс]. 22.05.2013. — URL: http://www.stripes.com/german-armed-forces-equipping-for-cyber-war-1.222156 (дата обращения: 19.01.2017).

123. Hackers wanted to man front line in cyber war // The Local [Электронный ресурс]. 24.03.2013. — URL: http://www.thelocal.de/20130324/48723 (дата

обращения: 21.06.2014).

124. Germany to expand Internet surveillance // Deutsche Welle [Электронный ресурс]. 16.06.2013. URL: http://www.dw.com/en/der-spiegel-germany-to-expand-internet-surveillance/a-16885711 (дата обращения: 19.01.2017).

125. Germany to invest 100 million euros on internet surveillance: report // Kazinform [Электронный ресурс]. 18.06.2013. — URL: http:/www.inform.kz/eng/article/2567203 (дата обращения: 19.01.2017).

126. Попсулин С. Британская спецслужба научилась шпионить через роутеры Cisco и пыталась взломать продукты «Касперского» // CNews [Электронный ресурс]. 16.01.2015. — URL: http://www.cnews.ru/news/top/britanskaya_spetssluzhba_nauchilas_shpionit (дата обращения: 19.01.2017).

127. Еремеев М. А., Ломако А. Г., Овчаров В. А., Акулов С. А., Коротков В. С., Свергун Н. В. Метод адаптивного управления активным сетевым оборудованием телекоммуникационной сети в условиях компьютерных атак // Информационное противодействие угрозам терроризма. 2012. № 19. С. 136-146.

128. Бирюков Д. Н., Ломако А. Г. Подход к построению ИБ-систем, способных синтезировать сценарии упреждающего поведения в информационном конфликте // Защита информации. Инсайд. 2014. № 6 (60). С. 42-49.

129. Тарасов А. А. Функциональная отказоустойчивость систем обработки информации. Монография. — М.: МИНИТ ФСБ России, 2009. — 181 с.

130. Жуматий В. П., Будников С. А., Паршин Н. В. Угрозы программно-математического воздействия. — Воронеж: ЦПКС ТЗИ, 2010. — 230 с.

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 будут оснащать военные корабли лазерным оружием // РИА Новости [Электронный ресурс]. 09.04.2013. — URL: https://ria.ru/world/20130409/931642162.html (дата обращения: 19.01.2017).

134. ВМС США вооружились лазерной пушкой, чтобы сбивать дроны, сообщают СМИ // 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/press-releases/2012/november/1127-ss-adam.html (дата обращения: 19.01.2017).

137. Чукляев И. И. Нечеткая оценка взаимосвязей системных факторов информационно-управляющей системы в интересах повышения защищенности информационных ресурсов // Системы управления, связи и безопасности. 2015.

№ 1. С. 4-15. — URL: http://journals.intelgr.com/sccs/archive/2015-01/01-Chuklyaev.pdf (дата обращения: 18.01.2017).

138. ГОСТ 50992-96. Защита информации. Основные термины и определения. — М.: Стандартинформ, 2008. — 12 с.

139. Толстых Н. Н. Павлов В. А. Воробьева Е. И. Введение в теорию конфликтного функционирования информационных и информационно-управляющих систем: учебное пособие. — Воронеж: ВГТУ, 2003. — 168 с.

140. Алферов А. Г., Власов Ю. Б., Толстых И. О., Толстых Н. Н., Челядинов Ю.В. Формализованное представление эволюционирующего информационного конфликта в телекоммуникационной системе // Радиотехника. 2012. № 8. С. 27-33.

141. Алферов А. Г., Белицкий А. М., Степанец Ю. А., Толстых Н. Н. Перехват управления инфокоммуникационных систем // Теория и техника радиосвязи. 2014. № 4. С. 5-13.

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.defense-aerospace.com/article-view/release/130594/rheinmetall-shoots-down-uav-with-laser.html (дата обращения: 19.08.2017).

144. Бойко А. А., Храмов В. Ю. Модель информационного конфликта информационно-технических и специальных программных средств в вооруженном противоборстве группировок со статичными характеристиками // Радиотехника. 2013. № 7. С. 5-10.

145. Козирацкий Ю. Л., Ерофеев А. Н., Соколовский С. П. Модель конфликтного взаимодействия «нарушитель - подсистема защиты информации автоматизированной системы управления» // Вестник Военного авиационного инженерного университета. 2012. № 1 (15). С. 210-217.

146. Ухин А. Л., Козирацкий Ю. Л. Вероятностная модель конфликта радиоэлектронных систем управления и телекоммуникации в условиях деструктивных воздействий // Системы управления и информационные технологии. 2014. Т. 57. № 3.2. С. 281-286.

147. Котенко И. В., Саенко И. Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. № 3 (22). С. 84-100.

148. Arquilla J. Ronfeldt D. F. Networks and netwars: the future of terror, crime, and militancy. — Santa-Monica: Rand Corporation, 2001. — 380 p.

149. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2012. № 2. С. 57-68.

150. Котенко И. В., Уланов А. В. Команды агентов в киберпространстве: моделирование процессов защиты информации в глобальном Интернете //

Труды Института системного анализа Российской академии наук. 2006. Т. 27. С. 108-129.

151. Котенко И. В., Уланов А. В. Компьютерные войны в интернете: моделирование противоборства программных агентов // Защита информации. Инсайд. 2007. № 4 (16). С. 38-45.

152. Cebrowski A. K., Garstka J. J. Network-Centric Warfare: Its Origin and Future // U.S. Naval Institute Proceedings. — Annapolis (Maryland), 1998.

153. Hersprin D. R. Rumsfeld's Wars: The Arrogance of Power. Lawrence, Kans.: University Press of Kansas, 2008.

154. Хореев А. А. Технические средства и способы промышленного шпионажа. — М.: ЗАО «Дальснаб», 1997. — 230 с.

155. Хореев А. А. Способы и средства защиты информации. — М.: Минобороны, 2000. — 320 с.

156. Вакин С. А., Шустов Л. Н. Основы радиопротиводействия и радиотехнической разведки. — М.: Сов. радио. 1968. — 448 с.

157. Максимов М. В., Бобнев М. П., Кривицкий Б. Х., Горгонов Г.И., Степанов Б. М., Шустов Л. Н., Ильин В. А. Защита от радиопомех / Под ред. М.В. Максимова. — М.: Сов. радио, 1976. — 496 с.

158. Дружинин В. В., Конторов Д. С. Конфликтная радиолокация. — М.: Радио и связь, 1982. — 288 с.

159. Палий А. И. Радиоэлектронная борьба. — М.: Воениздат, 1989. — 350 с.

160. Цветнов В. В., Демин В. П., Куприянов А. И. Радиоэлектронная борьба: радиоразведка и радиопротиводействие. — М.: МАИ, 1998. — 248 с.

161. Цветнов В. В., Демин В. П., Куприянов А. И. Радиоэлектронная борьба: радиомаскировка и помехозащита. — М.: МАИ, 1999. — 240 с.

162. Куприянов А. И., Сахаров А. В. Радиоэлектронные системы в информационном конфликте. — М.: Вузовская книга, 2003. — 528 с.

163. Андриевский И.А. Некоторые аспекты современных форм и способов враждебного противостояния и вооруженного противоборства // Экономические отношения. 2012. № 1. С.46-63.

164. Будников С. А., Гревцев А. И., Иванцов А. В., Кильдюшевский В. М., Козирацкий А. Ю., Козирацкий Ю. Л., Кущев С. С., Лысиков В. Ф., Паринов М. Л., Прохоров Д. В. Модели информационного конфликта средств поиска и обнаружения. Монография / Под ред. Ю.Л. Козирацкого — М.: Радиотехника, 2013. — 232 с.

165. Бобриков А. А. Методика обоснования решений по огневому поражению противника // Военная мысль. 2011. № 11. С. 43-53.

166. Никольский Б. А. Основы теории систем и комплексов радиоэлектронной борьбы: электрон. учеб. пособие. — Самара: Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т), 2012. — 174 с.

167. Современная радиоэлектронная борьба. Вопросы методологии / Под ред. В.Г. Радзиевского. — М.: Радиотехника, 2006. — 424 с.

168. Владимиров В. И., Лихачев В. П., Шляхин В.М. Антагонистический конфликт радиоэлектронных систем. — М.: Радиотехника, 2004. — 384 с.

169. Меркулов В. И., Чернов В. С., Дрогалин В. В., Канащенков А. И., Самарин О. Ф., Алексеев Ю. Я., Громов М. В., Дудник П. И., Жибуртович Н. Ю., Ильчук А. Р., Родзивилов В. А., Слукин Т. П., Федоров И. Б., Францев В. В., Чернов М. В., Шуклин А. И. Помехозащищенность радиолокационных систем. Состояние и тенденции развития / Под ред. А.И. Канащенкова, В.И. Меркулова. — М.: ИПРЖР, 2003. — 464 с.

170. Борисов В. И., Зинчук В. М. Лимарев А. Е., Немчилов А. В., Чаплыгин А. А. Пространственные и вероятностно-временные характеристики эффективности станций ответных помех при подавлении систем радиосвязи / Под ред. В.И. Борисова. — Воронеж: ОАО «Концерн «Созвездие», 2007. — 354 с.

171. Путин: агент влияния или компрадор? Часть 2. // Сайт 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. Чуднов А. М. Помехоустойчивость линий и сетей связи в условиях оптимизированных помех. — Л.: ВАС, 1986. — 84 с.

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://nash-suvorov.ru/upload/userfiles/10/voruzhenaja-borba-i-e-razvitie-v-xxi-veke-ch1.pdf (дата обращения: 22.08.2017).

175. Кузнецов В. И. Радиосвязь в условиях радиоэлектронной борьбы. — Воронеж: ВНИИС. 2002. — 403 с.

176. Дятлов А. П., Дятлов П. А., Кульбикаян Б. Х. Радиоэлектронная борьба со спутниковыми радионавигационными системами. Монография. — М.: Радио и связь, 2004. — 226 с.

177. Вартанесян В. А. Радиоэлектронная разведка. — М.: Воениздат, 1991. — 254 с.

178. Марчук Л. А. Пространственно-временная обработка сигналов в линиях радиосвязи. — Л.: ВАС, 1991. — 136 с.

179. Смирнов Ю. А. Радиотехническая разведка. — М.: Воениздат, 2001. — 456 с.

180. Радзиевский В. Г., Сирота А. А. Теоретические основы радиоэлектронной разведки. 2-е изд. — М.: Радиотехника, 2004. — 432 с.

181. Мельников Ю. П. Воздушная радиотехническая разведка (методы оценки эффективности). — М.: Радиотехника, 2005. — 304 с.

182. Дятлов А. П., Кульбикаян Б. Х. Радиомониторинг излучений спутниковых радионавигационных систем. Монография. — М.: Радио и связь, 2006. — 270 с.

183. Дворников С. В. Теоретические основы частотно-временного анализа кратковременных сигналов. Монография. / Под ред. А.М. Кудрявцева. — СПб.: ВАС, 2010. — 240 с.

184. Меньшаков Ю. К. Виды и средства иностранных технических разведок: учебное пособие / Под ред. М.П. Сычева. — М.: МГТУ им. Н.Э. Баумана, 2009. — 656 с.

185. Рембовский А. И., Ашихмин А. В., Козьмин В. А. Радиомониторинг - задачи, методы, средства. 2-е изд. — М.: Горячая линия-Телеком, 2010. — 624 с.

186. Одоевский С. М., Калюка В. И. Адаптивно-игровое моделирование военных сетей беспроводного абонентского доступа. В 2-х частях. Часть 1. — Новочеркасск: УПЦ «Набла» ЮРГТУ (НПИ), 2009. — 216 с.

187. Радиоэлектронная борьба. От экспериментов прошлого до решающего фронта будущего / М.С. Барабанов, С.А. Денисенцев, В.Б. Кашин, А.В. Лавров, Р.Н. Пухов, Д.В. Федутинов, А.А. Хетагуров, М.Ю. Шеповаленко / Под ред. Н.А. Колесова и И.Г. Насенкова. — М.: Центр анализа стратегий и технологий, 2015. — 248 с.

188. Михайлов Р. Л. Помехозащищенность транспортных сетей связи специального назначения. Монография. — Череповец: ЧВВИУРЭ, 2016. — 128 с.

189. Михайлов Р. Л. Модели и алгоритмы маршрутизации в транспортной наземно-космической сети связи военного назначения // Системы управления, связи и безопасности. 2015. № 3. С. 52-82. — URL: http://journals.intelgr.com/sccs/archive/2015-03/04-Mikhailov.pdf (дата обращения: 20.01.2017).

190. Макаренко С.И. Оценка качества обслуживания пакетной радиосети в нестационарном режиме в условиях воздействия внешних дестабилизирующих факторов // Журнал радиоэлектроники. 2012. № 6. С. 2. — URL: http://jre.cplire.ru/jre/jun12/9/text.pdf (дата обращения: 26.08.2016).

191. Макаренко С.И. Подавление пакетных радиосетей со случайным множественным доступом за счет дестабилизации их состояния // Журнал радиоэлектроники. 2011. № 9. С. 2. — URL: http://jre.cplire.ru/jre/sep11/4/text.pdf (дата обращения: 26.08.2016).

192. Макаренко С. И., Михайлов Р. Л., Новиков Е. А. Исследование канальных и сетевых параметров канала связи в условиях динамически изменяющейся сигнально-помеховой обстановки // Журнал радиоэлектроники. 2014. № 10. — URL: http://jre.cplire.ru/jre/oct14/3/text.pdf (дата обращения: 01.08.2016).

193. 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).

194. Макаренко С. И., Михайлов Р. Л. Информационные конфликты — анализ работ и методологии исследования // Системы управления, связи и безопасности. 2016. № 3. С. 95-178. — URL: http://sccs.intelgr.com/archive/2016-03/04-Makarenko.pdf (дата обращения: 17.09.2016).

195. Макаренко С. И. Радиоэлектронные информационные воздействия на сети связи сетецентрической системы управления // Вестник Военно-воздушной академии. 2016. № 3 (27). С. 108-117.

196. Макаренко С. И., Афанасьев О. В., Баранов И. А., Самофалов Д. В. Экспериментальные исследования реакции сети связи и эффектов перемаршрутизации информационных потоков в условиях динамического изменения сигнально-помеховой обстановки // Журнал радиоэлектроники. 2016. № 4. — URL: http://jre.cplire.ru/jre/apr16/4/text.pdf

197. 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.

198. Михайлов Р. Л., Макаренко С. И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. № 4. С. 69-79.

199. Макаренко С. И. Время сходимости протоколов маршрутизации при отказах в сети // Системы управления, связи и безопасности. 2015. № 2. С. 45-98. — URL: http://sccs.intelgr.com/archive/2015-02/03-Makarenko.pdf (дата обращения: 01.08.2016).

200. Макаренко С.И., Михайлов Р.Л. Адаптация параметров сигнализации в протоколе маршрутизации с установлением соединений при воздействии на сеть дестабилизирующих факторов // Системы управления, связи и безопасности. 2015. № 1. С. 98-126. — URL: http://sccs.intelgr.com/archive/2015-01/07-Makarenko.pdf (дата обращения: 01.08.2016).

201. Макаренко С. И. Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122-185. — URL: http://journals.intelgr.com/sccs/archive/2015-03/07-Makarenko.pdf (дата обращения: 03.04.2016).

202. 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).

203. Панов М., Маневич В. Военные конфликты на рубеже 2030 года // Зарубежное военное обозрение. 2008. № 1. С. 3-15.

204. Макаренко С. И. Преднамеренное формирование информационного потока сложной структуры за счет внедрения в систему связи дополнительного имитационного трафика. // Вопросы кибербезопасности. № 3 (4). 2014. С. 7-13.

205. Макаренко С. И., Коровин В. М., Ушанев К. В. Оператор преобразования трафика для преднамеренного повышения структурной сложности информационных потоков // Системы управления, связи и безопасности. 2016. № 4. С. 77-109. — URL: http://sccs.intelgr.com/archive/2016-04/04-Makarenko.pdf (дата обращения: 20.01.2017).

206. Arquilla J., Ronfeldt D., Zanini M. Networks, Netwar, and Information — Age Terrorism // The Changing Role of Information in Warfare. — Rand Corporation. 1999. Pp. 88-89.

207. Arquilla J., Ronfeldt D. The Advent of Netwar // In Athena's Camp. — Rand Corporation. 1997. Pp. 275-279.

208. Stein G. J. Information Attack: Information Warfare in 2025, research paper presented to 'Air Force 2025'. 1996.

209. Szafranski R. Harnessing Battlefield Technology: Neocortical Warfare: The Acme of Skill. Military Review. 1994.

210. Szafranski R. Parallel War and Hyperwar: Is Every Want a Weakness? Chapter 5 in Air Chronicles compilation on Battlefield of the Future. 1996.

211. Jensen O. E. Information warfare: Principles of third-wave war // Airpower Journal. 1994. Pp. 35-43.

212. Libicki M. What is Information Warfare. — National Defense University. ACIS paper 3, 1995.

213. 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).

214. 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).

215. 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).

216. 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).

217. Франция создаст полностью электрический корабль // Lenta.ru [Электронный ресурс]. 28.10.2010. — URL: https://lenta.ru/news/2010/10/28/advansea/ (дата обращения: 21.01.2017).

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. 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).

221. Electronic Weapons: Caesar Turns Into Nero // Strategy Page [Электронный ресурс]. 2015. — URL: https://www.strategypage.com/htmw/htecm/articles/20140804.aspx (дата обращения: 19.07.2016).

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. Исаков Е. Е, Петухов В. Г., Хохлов В. А. Материалы исследований реальной помехозащищенности линий тропосферной связи на горном ТВД в условиях РЭП. Отчет по испытаниям. — Тбилиси, 1976. — 56 с.

227. 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).

228. Judson J. Will Russian Aggression Ramp Up US Army Focus on Electronic Warfare Needs? // Defense News. 07.03.2016. — URL: https://www.defensenews.com/digital-show-dailies/global-force-symposium/2016/03/07/will-russian-aggression-ramp-up-us-army-focus-on-electronic-warfare-needs/ (дата обращения: 19.07.2016).

229. 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).

230. 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).

231. 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).

232. Osborn Kr. Adaptive electronic warfare // Army AL&T. 2013. № 1. pp. 44-48.

233. Акбашев Б. Б., Балюк Н. В., Кечиев Л. Н. Защита объектов телекоммуникаций от электромагнитных воздействий. — М.: Грифон, 2014. — 472 с.

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. 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. — М.: НИИ «Аргон», 2014. — 390 с.

237. 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).

238. Маевский Ю. И. Научно-технические проблемы развития систем и средств радиоэлектронной борьбы // Тем. сборник «Радиоэлектронная борьба в Вооруженных Силах Российской Федерации». — М.: ООО «Компания «Информационный мост», 2013. — С. 122-124.

239. Савин Л. В. Сетецентричная и сетевая война. Введение в концепцию. — М.: Евразийское движение, 2011. — 130 с.

240. Гриб В. Н. Проблемные вопросы создания авиационных комплексов радиоэлектронной борьбы // Сб. докл. Всероссийской научно-практической конференции «Академические Жуковские чтения». — Воронеж: ВУНЦ ВВС «ВВА», 2013. — С. 71-77.

241. Козлов С. В., Карпухин В. И., Лазаренков С. М. Модели конфликта авиационных систем радиоэлектронной борьбы и противовоздушной обороны. Монография. — Воронеж: ВУНЦ ВВС «ВВА», 2013. — 468 с.

242. Лобанов Б. С. 70 лет на фронте радиоэлектронной борьбы // Тем. сб. «Радиоэлектронная борьба в Вооруженных Силах Российской Федерации». — М.: ООО «Компания «Информационный мост», 2013. — С. 142-143.

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. Баринов С. П., Карпухин В. И. Методы обоснования и направления развития техники радиоподавления радиолокации // Радиотехника. 2010. № 6. С. 74-79.

245. Куприянов А. И., Шустов Л. Н. Радиоэлектронная борьба. Основы теории. — М.: Вузовская книга, 2011. — 800 с.

246. Артюх С. Н., Лаптев И. В., Глебов Е. В., Пахомов Л. А. Анализ возможностей и направлений развития средств защиты летательных аппаратов от управляемых ракет // Сб. статей по материалам Жуковских чтений, посвященных 165-летию со дня рождения Н.Е. Жуковского «Авиация России: от Жуковского до сегодняшних дней». — Воронеж: ВАИУ, 2012. — С. 3-11.

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. 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).

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. 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).

259. 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).

260. 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).

261. Евграфов В. Перспективы использования зарубежными вооруженными силами беспилотных летательных аппаратов для решения задач РЭБ // Зарубежное военное обозрение. 2009. № 10. С. 53-59. — URL: http://pentagonus.ru/publ/perspektivy_ispolzovanija_zarubezhnymi_vooruzhjonnymi_silami_bespilotnykh_letatelnykh_apparatov_dlja_reshenija_zadach_rehb/24-1-0-1407 (дата обращения: 10.03.2013).

262. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. — Washington D.C.: The White House, 2009.

263. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. — Washington D.C.: The White House, 2011.

264. Department of Defense Strategy for Operating in Cyberspace. — Washington D.C.: U.S. Department of Defense, 2011.

265. AFDD 3-12. Cyberspace Operations. — USAF, 2010. — 60 p.

266. AFDD 3-13. Information Operations. — USAF, 2011. — 65 p.

267. AFPD 10-7. Information Operations. — USAF, 2006. — 29 p.

268. DoDD 3600.1. Information Operations. — US DoD, 2013. — 12 p.

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. 2014. № 1 (2). С. 13-21. — URL: http://cyberrus.com/wp-content/uploads/2014/03/13-21.pdf (дата обращения: 10.01.2017).

271. Information Operations Primer: Fundamentals of Information Operations. — U.S. Army War College, 2011. — 204 p.

272. Почепцов Г. Г. Информационные войны. — М.: Рефл-бук, К.: Ваклер, 2000. — 576 с.

273. Шептура В. Н. Архитектура перспективной системы связи группировки войск (сил) для обеспечения управления адаптивными действиями войск (сил) [Доклад] // Мат-лы 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 «Созвездие», 2013. — С. 16-20.

274. JP 3-13. Information Operations. — US Joint Chiefs of Staff, 2012. — 69 p.

275. JP 3-13.1. Electronic Warfare. — US Joint Chiefs of Staff, 2007. — 115 p.

276. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. — СПб.: Свое издательство, 2013. — 166 с.

277. Расторгуев С. П. Информационная война. — М: Радио и связь, 1999. — 416 с.

278. Стандарт ISO/IEC 27032:2012. Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности. 2012.

279. 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).

280. 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).

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. Антонович П. И., Шаравов И. В., Лойко В. В. Сущность операций в кибернетическом пространстве и их роль в достижении информационного превосходства // Вестник Академии военных наук. 2012. № 1 (38). С. 41-45.

284. Антонович П. И. Изменение взглядов на информационное противоборство на современном этапе // Вестник Академии военных наук. 2011. № 1 (34). С. 43-47.

285. Антонович П. И. О современном понимании термина «кибервойна» // Вестник Академии военных наук. 2011. № 2 (35). С. 89-96.

286. Антонович П. И. О сущности и содержании кибервойны // Военная мысль. 2011. № 7. С. 39-46.

287. 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.

288. Зубарев И. В., Жидков И. В., Кадушкин И. В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1 (1). С. 10-16.

289. Конвенция ООН об обеспечении международной информационной безопасности (концепция). 2011. — URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 20.08.2017).

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. Шеховцов Н. П., Кулешов Ю. Е. Информационное оружие: теория и практика применения в информационном противоборстве // Вестник Академии военных наук. 2012. № 1 (38). С. 35-40. — URL: http://pentagonus.ru/publ/materialy_posvjashheny/2000_nastojashhij_moment/informacionnoe_oruzhie_teorija_i_praktika_primenenija_v_informacionnom_protivoborstve/122-1-0-2215 (дата обращения: 23.01.2017).

293. Присяжнюк С. П., Сидак А. А. Анализ современного состояния теории и практики построения моделей систем защиты информации // Тезисы докл. III Межведомственной НТК «Проблемные вопросы сбора, обработки и передачи информации в сложных радиотехнических системах». — Пушкин, ПВИРЭ КВ, 1997.

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. Прокофьев В. Ф. Тайное оружие информационной войны. Воздействие на подсознание. — М.: Синтег, 2003. — 430 с.

304. 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.: Издательство «Экзамен», 2003. — 560 с.

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. Абдурахманов М. И., Баришполец В. А., Баришполец Д. В., Манилов В. Л. Геополитика, международная и национальная безопасность. Словарь основных понятий и определений / Под общей ред. В.Л. Манилова. — М.: РАЕН, 1998. — 256 с.

308. Война в Ливии. США применили новейший самолет радиоэлектронной борьбы // Оружие России [Электронный ресурс]. 03.04.2011. — URL: http://www.arms-expo.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 кампании 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. Цыгичко В. Н., Вотрин Д. С., Крутских А. В., Смолян Г. Л., Черешкин Д. С. Информационное оружие — новый вызов международной безопасности. — М.: ИСА РАН, 2000. — 52 с.

313. Попов И. М. Война будущего: взгляд из-за океана. Военные теории и концепции современных США. — М.: ООО «Издательство АСТ», 2004. — 444 с.

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. Шейнов В. П. Психотехнологии влияния. — М.: АСТ; Мн.: Харвест, 2005. — 448 с.

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. 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).

319. Колин К. К. Социальная информатика. — М.: Академический проект, 2003. — 432 с.

320. Проблемы безопасности программного обеспечения / Под ред. П.Д. Зегжды. — СПб.: ГТУ, 1995. — 200 с.

321. Куприянов А. И., Сахаров А. В., Шевцов В. А. Основы защиты информации: учебное пособие. — М.: Издательский центр «Академия», 2006. — 256 с.

322. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. — Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. — 372 с.

323. Марков А. С., Фадин А. А. Организационно-технические проблемы защиты от целевых вредоносных программ // Вопросы кибербезопасности. 2013. № 1 (1). С. 28-36.

324. 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).

325. Вирус Regin // Security Lab [Электронный ресурс]. 28.05.2015. — URL: http://www.securitylab.ru/analytics/473080.php (дата обращения: 14.08.2016).

326. Киви Б. Кивино гнездо: государственный троянец // Компьютера [Электронный ресурс]. 21.10.2011. — URL: http://old.computerra.ru/own/kiwi/641530/ (дата обращения: 10.09.2017).

327. 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).

328. «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).

329. 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).

330. "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).

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. 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).

335. 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).

336. 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).

337. 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).

338. Щербинин Р. Перспективные боевые части высокоточного оружия США // Зарубежное военное обозрение. 2010. № 4. С. 58-63.

339. Дождиков В. Г., Салтан М. И. Краткий энциклопедический словарь по информационной безопасности. — М.: ИАЦ Энергия, 2010. — 240 с.

340. Зайцев О. Современные клавиатурные шпионы // Компьютер Пресс [Электронный ресурс]. 2006. № 5. — URL: http://compress.ru/article.aspx?id=15847 (дата обращения: 14.08.2017).

341. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2 (3). С. 60-65.

342. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 2. Рабочее место оператора // Вопросы кибербезопасности. 2014. № 4 (7). С. 60-68.

343. Виноградов А. А. Функциональность, надежность, киберустойчивость в системах автоматизации критических инфраструктур [Доклад] // Конференция «Региональная информатика-2012». — СПб.: ОАО «НПО «Импульс», 2012.

344. 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).

345. Марков А. С., Цирлов В. Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42-48.

346. 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.

347. Шурдак М. О., Лубкин И. А. Методика и программное средство защиты кода от несанкционированного анализа // Программные продукты и системы. 2012. № 4. С. 176-180.

348. 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.

349. 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.

350. 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.

351. Сердечный А. Л. Инновационный подход к защите информации в виртуальных вычислительных сетях, основанный на стратегии обмана // Информация и безопасность. 2013. № 3. С. 399-403.

352. 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).

353. Резяпов Н., Чесноков С., Инюхин С. Имитационная система моделирования боевых действий JWARS // Зарубежное военное обозрение. 2008. № 11. С. 27-32. — URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2008-zvo/7599-imitacionnaja-sistema-modelirovanija-boevyh (дата обращения: 30.07.2014).

354. Резяпов Н. Развитие систем компьютерного моделирования в вооружённых силах США // Зарубежное военное обозрение. 2007. № 6. С. 17-23. — URL: http://pentagonus.ru/publ/11-1-0-222 (дата обращения: 18.08.2016).

355. Мединa 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).

356. Мединa 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).

357. Мединa 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).

358. Новиков Д. А. Иерархические модели военных действий // Управление большими системами. 2012. № 37. С. 25-62.

359. Меньшаков Ю. К. Теоретические основы технических разведок: учеб. пособие / Под ред. Ю.Н. Лаврухина. — М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. — 536 с.

360. Чукляев И. И., Морозов А. В., Болотин И. Б. Теоретические основы оптимального построения адаптивных систем комплексной защиты информа-

ционных ресурсов распределенных вычислительных систем: монография. — Смоленск: ВА ВПВО ВС РФ, 2011. — 227 с.

361. 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.

362. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. — К.: Юниор, 2003. — 504 с.

363. Емельянов С. Л. Техническая разведка и технические каналы утечки информации // Системи обробки інформації. 2010. № 3 (84). С. 20-23.

364. 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.

365. 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.

366. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description // Cigital Inc. 2008. Vol. 3.

367. O'Neill J. Echelon: Somebody's Listening. — Tarentum: Word Association Publishers, 2005. — 347 p. — URL: http://books.google.com/books?id=1x6Akzkxv5IC&printsec=frontcover&source=gbs_summary_r&cad=0 (дата обращения: 30.11.2016).

368. PRISM_(surveillance_program) // Wikipedia [Электронный ресурс]. 2016. — URL: https://en.wikipedia.org/wiki/PRISM_(surveillance_program) (дата обращения: 30.11.2016).

369. Stellar Wind // Wikipedia [Электронный ресурс]. 2016. — URL: https://en.wikipedia.org/wiki/Stellar_Wind (дата обращения: 30.11.2016).

370. 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).

371. 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. — URL: http://www.avnrf.ru/attachments/article/669/AVN-3(48)_001-184.pdf (дата обращения: 23.01.2017).

372. Dropmire // Wikipedia [Электронный ресурс]. 2016. — URL: https://en.wikipedia.org/wiki/Dropmire (дата обращения: 30.11.2016).

373. X-Keyscore // Wikipedia [Электронный ресурс]. 2016. — URL: https://en.wikipedia.org/wiki/Dropmire (дата обращения: 30.11.2016).

374. Tempora [Электронный ресурс]. 2017. — URL: https://en.wikipedia.org/wiki/Tempora (дата обращения: 23.01.2017).

375. 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).

376. 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).

377. Разведка средствами Интернет // IT-сектор [Электронный ресурс]. — URL: http://it-sektor.ru/razvedka-sredstvami-internet.html (дата обращения: 17.08.2016).

378. Ларина Е. С., Овчинский В. С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. — М.: Книжный мир, 2014. — 352 с.

379. Thaler R. H., Sunstein C. R. Nudge: Improving decisions about health, wealth, and happiness. — Yale: Yale University Press, New Haven, CT, 2008. — 293 p.

380. Медведовский И. Д., Семьянов П. В., Платонов В. В. Атака через Интернет / Под ред. П.Д. Зегжды. — СПб.: Изд. НПО «Мир и семья-95», 1997.

381. Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны — реальная угроза национальной безопасности. — М.: КРАСАНД, 2011. — 96 с.

382. 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).

383. Горбачев Ю. Е. Кибервойна уже идет // Независимое военное обозрение [Электронный ресурс] 12.04.2013. — URL: http://nvo.ng.ru/armament/2013-04-12/1_cyberwar.html (дата обращения: 20.01.2017).

384. Qiao Liang, Wang Xiangsui. Unrestricted Warfare. — PLA Literature and Arts Publishing House, Beijing, 1999.

385. Sobiesk E. Redefining the Role of Information Warfare in Chinese Strategy. — SANS Institute, 2003.

386. Yoshihara Toshi Chinese information warfare: a phantom menace or emerging threat? — U.S. Army War College, Strategic Studies Institute, 2001.

387. Buchan G. C. Implications of Information Vulnerabilities for Military Operations // The Changing Role of Information in Warfare. — RAND Corporation. 1999. Pp. 290-293.

388. 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).

389. Иванов И. Некоторые аспекты деятельности Сил психологических операций Вооруженных сил США // Зарубежное военное обозрение. 2010. № 11. С. 29-34. — URL: http://pentagonus.ru/publ/nekotorye_aspekty_dejatelnosti_sil_psikhologicheskikh_operacij_vooruzhjonnykh_sil_ssha/3-1-0-1632 (дата обращения: 17.08.2016).

390. Баришполец В. А. Информационно-психологическая безопасность: основные положения // Информационные технологии. 2003. Том 3. № 2. С. 69-104.

391. 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).

392. Карякин В. Наступила эпоха следующего поколения войн — информационно-сетевых // Независимое военное обозрение [Электронный ресурс]. 22.04.2011. — URL: http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html (дата обращения: 17.08.2016).

393. Китов П. Совершенствование способов и средств ведения психологических операций Вооружённых 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).

394. 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).

395. 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).

396. Савельев А. Информационное обеспечение применения вооружённых 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).

397. 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).

398. 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).

399. Паршакова Е. Д. Информационные войны: учебное пособие. — Краматорск: ДГМА, 2012. — 92 с.

400. 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).

401. 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).

402. Воронцова Л. В., Фролов Д. Б. История и современность информационного противоборства. — М.: Горячая линия — Телеком, 2006. — 192 с.

403. 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).

404. 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).

405. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт). — Мн: Харвест, 1999. — 448 с. — URL: http://www.e-reading.club/bookreader.php/1005378/Vladimir_-_Sekrety_psihologicheskoy_voyny.html (дата обращения: 30.06.2016).

406. 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).

407. 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).

408. 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).

409. Паршуткин А. В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем // Вопросы кибербезопасности. 2014. № 5 (8). С. 2-6.

410. Паршуткин А. В., Святкин С. А., Бажин Д. А., Сазыкин А. М. Радиоэлектронные информационные воздействия в конфликтах информационных и телекоммуникационных систем // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2015. № 5-6. С. 13-17.

411. 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).

412. Макаренко С. И., Синицин И. А. Инженерная методика оценки качества обслуживания системы массового обслуживания M/M/n/q с ненадежными

каналами и ее приложение для анализа функционирования систем многоканальной связи в условиях помех // Инфокоммуникационные технологии. Т. 12. № 4. 2014. С. 24-32.

413. Макаренко С. И., Михайлов Р. Л. Модель функционирования маршрутизатора в сети в условиях ограниченной надежности каналов связи // Инфокоммуникационные технологии. 2014. Т. 12. № 2. С. 44-49.

414. Макаренко С. И., Рюмшин К. Ю., Михайлов Р. Л. Модель функционирования объекта сети связи в условиях ограниченной надежности каналов связи // Информационные системы и технологии. 2014. № 6 (86). С. 139-147.

415. Ушанев К. В. Имитационные модели системы массового обслуживания типа Pa/M/1, H2/M/1 и исследование на их основе качества обслуживания трафика со сложной структурой // Системы управления, связи и безопасности. 2015. №4. С. 217-251. — URL: http://journals.intelgr.com/sccs/archive/2015-04/14-Ushanev.pdf (дата обращения: 25.01.2017).

416. Ушанев К. В., Макаренко С. И. Показатели своевременности обслуживания трафика в системе массового обслуживания Pa/M/1 на основе аппроксимации результатов имитационного моделирования // Системы управления, связи и безопасности. 2016. № 1. С. 42-65. — URL: http://sccs.intelgr.com/archive/2016-01/03-Ushanev.pdf (дата обращения: 25.01.2017).

417. Шеремет И.А. Угрозы техносфере России и противодействие им в современных условиях // Вестник академии военных наук. 2014. № 1 (46). С. 27-34.

418. Михайлов Д. М., Жуков И. Ю., Шеремет И. А. Защита автоматизированных систем от информационно-технологических воздействий. — М.: НИЯУ МИФИ, 2014. — 184 с.

419. Шеремет И. А., Дворянкин С. В., Евсеев В. Л., Савельев И. А., Камнева Е. В., Минаев В. А., Овчинский А. С., Ненашев С. М., Козлов Ю. Е., Воеводин А. Е., Викторов Ю. А. Комплекс методов противодействия информационно-психологическому воздействию на поведение социальных групп. Отчет о НИР. — М.: Финансовый университет при Правительстве РФ, 2016. — 192 с.

420. Семашко К. В., Шеремет И. А. Математическое моделирование информационно-психологических отношений в социумах. — М.: Наука, 2007. — 156 с.

421. Климов С. М., Сычёв М. П. Стендовый полигон учебно-тренировочных и испытательных средств в области обеспечения информационной безопасности // Информационное противодействие угрозам терроризма. 2015. № 24. С. 206-213.

422. Климов С. М., Сычев М. П. Научно-методические подходы к созданию комплекса (полигона) учебно-тренировочных средств в области обеспечения информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 1. № 25. С. 200-206.

423. Климов С. М., Черноскутов А. И., Мукминов В. А. Оценка эффективности защиты информации в автоматизированных системах военного назначения // Стратегическая стабильность. 2008. № 1. С. 34-38.

424. Белый А. Ф., Климов С. М.Алгоритм принятия решений по оценке функциональной устойчивости средств автоматизации в условиях компьютерных атак // Информационное противодействие угрозам терроризма. 2011. № 16. С. 101-105.

425. Белый А. Ф., Климов С. М., Котяшев Н. Н. Модель формирования игровой обстановки для оценки функциональной устойчивости средств автоматизации // Информационное противодействие угрозам терроризма. 2011. № 16. С. 105-108.

426. Климов С. М. Проблемы создания компьютерных стратегических игр для оценки защищенности критически важных информационных сегментов // Информационное противодействие угрозам терроризма. 2009. № 12. С. 46-56.

427. WannaCry и всё о крупнейшей всемирной вирусной кибератаке всего Интернета // Avast Forum [Электронный ресурс]. 13.04.2017. — URL: https://forum.avast.com/index.php?topic=202335.0 (дата обращения: 13.04.2017).

428. Гонка противорадиолокационных ракет // Военное обозрение [Электронный ресурс]. 12.04.2017. — URL: https://topwar.ru/113006-gonka-protivoradiolokacionnyh-raket.html (дата обращения: 15.04.2017).

429. Дроботун Е. Б. Риск-ориентированный подход к формированию функциональных требований к системам защиты от компьютерных атак для автоматизированных систем управления: монография. — Тверь: Издатель А.Н. Кондратьев, 2017. — 195 с.

430. Война в эфире. Часть 2 // Военное обозрение [Электронный ресурс]. 30.05.2017. — URL: https://topwar.ru/116560-voyna-v-efire-chast-2.html (дата обращения: 15.08.2017).

431. RQ-4 Global Hawk оснастят боевым лазером // Военное обозрение [Электронный ресурс]. 29.08.2017. — URL: https://topwar.ru/123590-rq-4-global-hawk-osnastyat-boevym-lazerom.html (дата обращения: 29.08.2017).

Макаренко Сергей Иванович

Информационное противоборство и радиоэлектронная борьба
в сетецентрических войнах начала XXI века
Монография

Научное издание

Корректура: В.В. Вересиянова

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 978-5-9909412-1-2

Гарнитура «TimesNewRoman». 34,6 п.л.
Тираж 600 экз. Подписано в печать 25.12.2017.

Макаренко Сергей Иванович – кандидат технических наук, доцент. Профессор Академии военных наук.

Родился в 1980 году в г. Ставрополе. 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 в Ставропольском высшем военном авиационном инженером училище 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 на должностях научного и преподавательского состава: в Ставропольском высшем военном авиационном инженером училище, в ВУНЦ ВВС «Военно-воздушная академия имени проф. Н.Е. Жуковского и Ю.А. Гагарина», в Военно-космической академии имени А.Ф. Можайского.

Основные научные результаты связанны с разработкой теоретических основ динамического многоуровневого информационного конфликта, а также способов функционального подавления телекоммуникационных систем за счет совместного использования средств радиоэлектронного подавления, средств функционального поражения электромагнитным излучением и информационно-технических воздействий. Обосновал способы обеспечения устойчивости телекоммуникационных систем специального назначения в подобных условиях.