ТЮТЮННИКОВ Николай Николаевич
Родился 29 ноября 1964 г. в городе Москве. Окончил Московский институт электронного машиностроения в 1987 г. Ученая степень – кандидат технических наук, ученое звание – старший научный сотрудник. С 1989 г. по 1999 г. проходил службу на офицерских должностях в 27 ЦНИИ МО РФ. После увольнения в отставку в воинском звании подполковник работал и продолжает работать на должностях предприятий оборонно-промышленного комплекса. Автор более 130 научных работ.

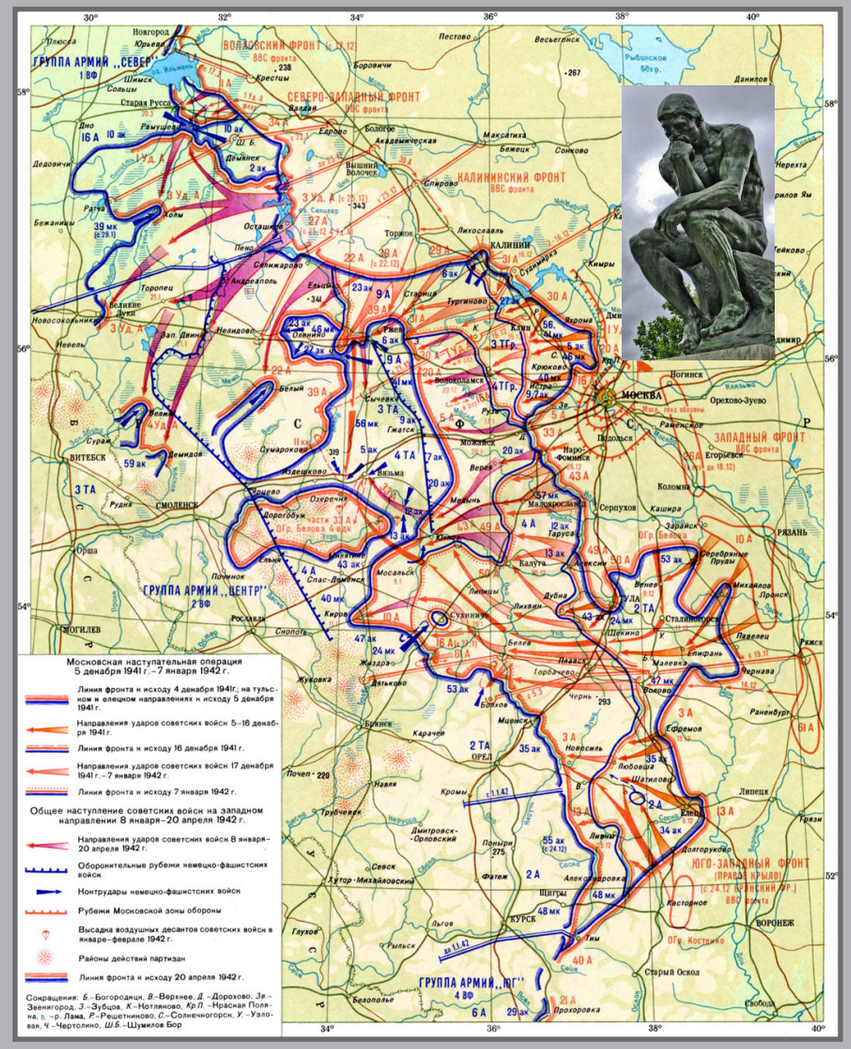
ISBN 978-5-00122-142-5

ВОЕННАЯ МЫСЛЬ В ТЕРМИНАХ И ОПРЕДЕЛЕНИЯХ

3

ВОЕННАЯ МЫСЛЬ

В ТЕРМИНАХ И ОПРЕДЕЛЕНИЯХ



№ 3

Информатизация Вооруженных Сил

Н.Н. Тютюнников

ВОЕННАЯ МЫСЛЬ В ТЕРМИНАХ И ОПРЕДЕЛЕНИЯХ

В трех томах

Том 3

Информатизация Вооруженных Сил

Москва
«Перо»
2018

УДК 355/359
ББК 68я2
Т 98

Тютюнников, Н.Н.
Т 98 Военная мысль в терминах и определениях : в 3 т. / Сост. Н.Н. Тютюнников. — Т. 3. Информатизация Вооруженных Сил. — М.: Издательство «Перо», 2018. — 472 с.

ISBN 978-5-00122-142-5 (Т.3)
ISBN 978-5-00122-139-5 (Общ.)

Словарь составлен на основе терминов и определений, содержащихся в статьях различных авторов, опубликованных в журнале «Военная мысль» за последние 20 лет. Представленные в книге термины и их толкования не следует рассматривать в качестве базовых понятий. Они в большинстве случаев отражают точку зрения авторов статей. Часть терминов и определений носит частный характер. Некоторые определения являются производными от установленных в нормативных документах. Многие словарные статьи уже потеряли свою актуальность. Данная книга является хорошим аналитическим материалом для проведения исследований в различных областях военного дела.

Словарь содержит 2778 словарных статей, систематизированных в 459 рубриках. Словарь создан на основе 740 публикаций.

Третий том словаря включает в себя словарные статьи в области информатизации ВС РФ, в том числе отражающие роль и место информации в военном деле, посвященные информационной и сетецентрической войне, описывающие автоматизированные системы управления войсками (силами).

Книга предназначена в первую очередь для военнослужащих, военных ученых и специалистов, занимающихся вопросами обеспечения безопасности и обороны Российской Федерации. В то же время она рассчитана на широкий круг читателей, интересующихся вопросами военного дела.

УДК 355/359
ББК 68я2

ISBN 978-5-00122-142-5 (Т.3)
ISBN 978-5-00122-139-5 (Общ.)

СОДЕРЖАНИЕ

ТЕМАТИЧЕСКИЙ ПЕРЕЧЕНЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

информационное общество — социальная общность, в которой одним из основных предметов труда большей части людей являются информация и знания, а орудием труда — информационные технологии.

Общественные отношения в информационном обществе будут во многом определяться именно этими обстоятельствами, а экономика общества ориентироваться на производство продуктов информационной и интеллектуальной деятельности, связанных с новой информацией и новыми знаниями.

Такое общество на первом этапе, видимо, будет представлять собой некоторую ассоциацию стран, достигших определенных экономических и социальных параметров — прежде всего высокого уровня информатизации жизни граждан и общества, управления государством, развития науки, образования и культуры, значительной степени интегрированности в мировую экономику. Достижение этих параметров представляет собой одно из важных условий экономического процветания и духовного развития государств — членов международного сообщества и сохранения стратегической стабильности в мире [226] (2003).

информационный потенциал государств — возможность государства обеспечить *информатизацию* общества.

Формирование информационного потенциала государства осуществляется за счет развития научно-технического и экономического потенциалов в ходе информатизации страны. При этом взаимное влияние потенциалов приводит к повышению эффективности влияния каждого из них на процесс наращивания военной мощи государства.

В информационном потенциале государства можно выделить три основных компонента: инфраструктурный, управленческий и собственно информационный.

Инфраструктурный компонент объединяет научно-исследовательские организации и центры анализа информации, вырабатывающие аналитико-прогностическую информацию и подготавливающие сведения для системы подготовки и принятия решений; органы научно-технической, экономической, политической и другой информации, обеспечивающие или непосредственно осуществляющие информаци-

онное оповещение специалистов; базы данных, осуществляющие сбор, обработку, индексацию, каталогизацию и хранение информации в различных областях знаний; информационные и телекоммуникационные системы, осуществляющие сбор, каталогизацию, хранение и циркуляцию всех видов информации собственно в информационной инфраструктуре государства.

Управленческий компонент включает специалистов, обладающих специальными знаниями и навыками в области сбора, переработки, хранения, поиска и распространения информации. К нему же относятся и органы управления, принимающие решения по вопросам информационного обеспечения, а также информационно-поисковые системы и системы управления базами данных, обеспечивающие их эффективное использование.

Информационный компонент представляет собой наличные и доступные знания, зафиксированные на материальных носителях и передаваемые по системе телекоммуникаций с целью их восприятия и использования в системах подготовки и принятия решений. Эти знания образуют *информационный ресурс*. Наиболее значимыми составляющими информационного ресурса государства являются информационные ресурсы государственных органов, коммерческих организаций, неправительственных общественных организаций, а также частных лиц [148] (2008).

информатизация[1] — организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов [24, 148] (2008).

информатизация[2] — процесс внедрения информационных технологий и средств сбора, передачи, хранения и обработки информации во все сферы деятельности человека и общества в целом [91] (2000).

информатизация Вооруженных Сил[1] — организованный процесс создания оптимальных условий для удовлетворения информационных потребностей личного состава ВС, должностных лиц штабов и других органов управления на основе формирования и рационального

использования информационных ресурсов в новой технологической среде.

Процессы информатизации ВС РФ существенно отличаются от рыночных и требуют более жесткого управления [24] (1999).

информатизация Вооруженных Сил[2] — организованный процесс создания, широкомасштабного внедрения и применения в различных областях их деятельности в мирное и военное время методов и средств сбора, передачи, переработки, хранения и использования информации в целях повышения эффективности деятельности Вооруженных Сил и удовлетворения информационных потребностей должностных лиц органов военного управления на основе формирования и использования информационных ресурсов [91] (2000).

информатизация ВС РФ — недостаточно поставить современную технику, надо еще научиться грамотно ее применять. Именно поэтому необходимо продолжать активное внедрение информационных технологий в повседневную деятельность, а также в обязательном порядке ввести систему электронного документооборота, чтобы не только командиры, но и весь личный состав получали необходимые знания и опыт работы с современными информационными системами. Их действия должны быть отработаны до автоматизма, как при работе с телевизором, сотовым телефоном или компьютером. Только в этом случае информационные системы и средства превратятся из непонятной дорогостоящей аппаратуры в настоящего помощника в решении поставленных боевых задач.

Работы в этом направлении достаточно, так как по уровню информатизации ВС РФ существенно отстают от американской армии:

— отсутствует **полноценная военно-научная информация**;

— не происходит **оцифровка** как **трудов военных ученых** за предыдущие годы, так и новых материалов, что усугубляет ситуацию.

Например, ни одного труда Н.И. Огаркова на многочисленных отечественных ресурсах военной направленности (включая официальный сайт Министерства обороны РФ) найти не удалось. В то же самое время на сайтах военно-научных учреждений зарубежных стран размещены переводы большинства трудов, которыми пользуются американские военные ученые.

Для ускорения процессов информатизации и реализации сетецентрических принципов в ВС РФ целесообразно также продолжить работу по:

уточнению сущности исследуемых явлений и формированию **единой терминологической базы**;

активизации поиска путей практической реализации сетецентрических принципов, разработке новых способов применения группировок войск, а также выработке современных инструментов повышения эффективности информационно-аналитической деятельности;

разработке и утверждению семейства концептуальных документов по информатизации видов и родов войск;

активизации деятельности по переходу на систему электронного документооборота, а также популяризации информатизации;

привлечению к работе по данной теме научно-исследовательских организаций РАН и специалистов из промышленности, которые уже сами выходят с практическими предложениями;

формированию из представителей науки и промышленности постоянно действующих рабочих групп по перспективным направлениям исследований [5] (2014).

военная информатизация — разработка и непрерывное совершенствование систем информационного обеспечения решений командиров (командующих) при управлении войсками (силами) [55] (2005).

военный информационный потенциал — часть информационного потенциала государства, обеспечивающая повышение качественного уровня элементов военного потенциала.

Как и в информационном потенциале государства, в военном информационном потенциале можно выделить те же три компонента: инфраструктурный, управленческий и информационный. По составу они в целом повторяют аналогичные компоненты информационного потенциала государства, которые, однако, более специализированы на решение задач обеспечения военных операций [148] (2008).

организованность информатизации — наличие и эффективная работа механизма управления информатизацией.

В сегодняшних сложных экономических условиях, как никогда, нужны ясные ориентиры в привязке процессов информатизации видов деятельности ВС к целям и задачам их реформирования.

Механизм управления представляет собой отлаженную систему федеральных и ведомственных норм, органов управления и их взаимоотношений, общепринятых правил, методик, теоретических разработок и практических мер, традиций и взглядов, позволяющую эффективно

влиять на ход процессов информатизации ВС. Он предусматривает наличие единой общепринятой содержательной основы в виде концепции информатизации, долгосрочных программ; единой административной вертикали управления процессами информатизации в масштабе ведомства; властных полномочий и возможностей концентрации ресурсов и средств для разработки и финансирования крупных проектов; опыта и методик перспективного планирования и координации научно-исследовательских и практических работ в области информатизации деятельности ВС; эффективной системы накопления и распространения опыта разработки многофункциональной информационной системы; ясной и простой системы контроля за всеми этапами движения ресурсов и средств, выделенных на реализацию проектов и программ.

Анализ реального положения дел в этой области свидетельствует, что такого механизма мы пока не имеем. Взять хотя бы концептуальные вопросы. При всеобщем понимании важности применения новых информационных технологий единых общепринятых взглядов на направления, формы и способы внедрения этих технологий в конкретные виды военной деятельности нет. Больше того — налицо различное толкование самого процесса. Одни говорят о компьютеризации, другие — об автоматизации, третьи — о математическом моделировании военных действий. Существует даже мнение ввести новый вид обеспечения операций и боевых действий — математическое [24] (1999).

информационная сфера[1] — сфера деятельности, при которой обеспечивается информационно-логическое взаимодействие пользователей при решении функциональных задач в данной предметной области (военное дело, медицина и т.д.) [53] (2012).

1. Информация в военном деле

информация[1] — сведения (сообщения, данные), независимо от формы их представления[1] [8] (2011).

информация[2] — любые сведения и данные, отражающие свойства объектов в природных (биологических, физических и других), социальных и технических системах и передаваемые звуковым, графиче-

[1] Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

ским (в том числе письменным) или иным способом без применения или с применением технических средств[2] [128] (2013).

информация[3] (от лат. informatio — разъяснение, изложение) — термин первоначально понимался как сведения, передаваемые людьми устным, письменным или другими способами.

Позднее под информацией стали понимать обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире, передачу признаков от клетки к клетке, от организма к организму.

Сегодня под информацией понимают:

— сообщения о чем-либо;

— сведения, являющиеся объектом хранения, переработки и передачи;

— количественную меру устранения неопределенности (энтропия), меру организации системы;

— свойство объектов (процессов) окружающего материального мира порождать разнообразие состояний, которые посредством отражения передаются от одного объекта к другому (пассивная форма), и свойство ограничения разнообразия и организации, т.е. управления, дезорганизации и др. (активная форма) [206] (2007).

информация[4] (от лат. information — ознакомление, разъяснение, представление) — сообщение, сведения о чем-либо, передаваемые людьми.

В настоящее время многие исследователи рассматривают информацию как самостоятельный феномен, имеющий непосредственное отношение к процессам управления и развития, обеспечивающий устойчивость и выживаемость любых систем, в том числе и политических [175] (2008).

информация[5] — ключевой элемент боевой мощи (наряду с руководством и управлением войсками, маневром, разведкой, огнем, снабжением и защитой), обеспечивающий превосходство над противником[3].

---

[2] Физическая энциклопедия : Т. 2 / Под ред. А.М. Прохорова. М.: Советская энциклопедия, 1990. С. 176.

[3] Армейская доктрина ADP 3-0 «Общевойсковые операции». Unified Land Operations. Washington: Department of the Army. 2011.

Кроме того, информация позволяет командным кадрам, с одной стороны, принимать обоснованные решения на операции (боевые действия), с другой — воздействовать на различные силы в районе военного конфликта, создавая тем самым благоприятную для успеха оперативную (тактическую) обстановку [56] (2014).

информация[6] — объем накопленных человечеством знаний об окружающем нас мире, непосредственно включенных в коммуникативный процесс в виде информационного ресурса [63] (2008).

информация[7] — содержательно-сущностная часть знаний (сведений, данных) о составах, структурах и алгоритмах предметной области, потенциально доступная для количественных оценок.

Количественной мерой информации является разность между количествами априорной и апостериорной информационных неопределенностей. Отрицательное значение этой разности часто называют дезинформацией [50] (1998).

информационное обеспечение военного управления — совокупность информационных ресурсов, средств и технологий, находящаяся в распоряжении органов управления и их должностных лиц, а также деятельность, направленная на их создание, совершенствование и обеспечение их бесперебойного функционирования.

Основной целью информационного обеспечения военного управления является повышение устойчивости управления военной организацией государства, его Вооруженными Силами в условиях информационного воздействия противника. Указанная цель достигается комплексом мер разнопланового характера.

Так, специфическими направлениями функционирования системы информационного обеспечения сферы обороны являются: выявление информационных угроз и их источников, определение практических задач по их нейтрализации; развитие специального программного обеспечения, прикладных программ и средств защиты информации в автоматизированных системах управления военного назначения; совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием; совершенствование структуры функциональных органов системы информационного обеспечения сферы обороны и координация их взаимодействия; совершенствование приемов и способов

стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы и др. [176] (2008).

информационное обеспечение применения войск (сил) — совокупность мероприятий, проводимых органами военного управления всех степеней, действий войск (в том числе космических), а также специально создаваемых органов по формированию и использованию информационной среды, интегрирующей данные о своих войсках и оружии, противнике, условиях выполнения задач и функционирующей на основе использования современных защищенных технологий и средств добывания, сбора, обработки, хранения и доведения информации в интересах эффективного применения войск (сил) [151] (2010).

информационное обеспечение управления межвидовой группировкой войск (сил) в интересах комплексной борьбы с противником — совокупность мероприятий, направленных на сбор, обработку, передачу, хранение, защиту и предоставление должностным лицам органов управления информации, необходимой для выполнения ими своих функциональных обязанностей при подготовке и в ходе операции (боевых действий) [205] (2017).

система информационного обеспечения управления межвидовой группировкой войск (сил) в интересах комплексной борьбы с противником — совокупность пунктов и средств сбора, обработки, передачи, хранения, защиты, преобразования и представления потребителям информации, необходимой для реализации ими информационно-управленческих функций [205] (2017).

данные[1] — в системном анализе и кибернетике — информация, представленная в формализованном виде, предназначенном для обработки средствами вычислительной техники или после обработки ими [151] (2010).

знания[1] — продукт деятельности людей, представляющий собой идеальное воспроизведение в языковой форме событий и закономерных связей объективного мира.

Многие научные школы мира утверждают, что знание есть сила, не абстрактная и не косвенная, а прямая. Человек может фактически властвовать над миром, и пределы этой власти определяются уровнем знаний. Он, в свою очередь, обусловливает точность и границы доступной человеку информации, содержащейся в знаниях. Если знания

— сила, то мерой этой силы является содержащееся в них количество информации. В этом смысле знание может рассматриваться в качестве информационного оружия в отношениях соперничества, особенно в военной сфере деятельности [50] (1998).

1.1. Военная информационная инфраструктура

информационная инфраструктура — целесообразным образом организованная совокупность информационных, вычислительных и коммуникационных ресурсов, которая обеспечивает возможность сбора, передачи, хранения, автоматизированной обработки и распространения информации в интересах различных пользователей [53] (2012).

военная информационная инфраструктура (ВИИ) — инфраструра, которая должна состоять из взаимодействующих между собой различных сетей связи и компьютерных сетей, баз и банков данных и знаний, локальных сетей, прикладных программ, абонентских устройств и интерфейсов боевого оружия, средств, предоставляющих услуги по безопасности и другие услуги по передаче и обработке информации во всех сферах военной деятельности.

К основным характеристикам военной информационной инфраструктуры можно отнести: количественный и качественный состав элементов инфраструктуры; пространственное расположение элементов инфраструктуры; взаимосвязь элементов инфраструктуры; информационную производительность и пропускную способность элементов и всей инфраструктуры в целом [100] (2004).

элементы военной информационной инфраструктуры — основные компоненты военной информационной инфраструктуры, такие как сети связи, информационные ресурсы, системы информационного обслуживания, системы управления и развития военной информационной инфраструктуры [100] (2004).

информационная инфраструктура системы управления войсками (силами)[1] — организованная определенным образом совокупность вычислительных средств (вычислительных ресурсов) и средств телекоммуникаций (коммуникационных ресурсов), обеспечивающая сбор, накопление, хранение, защиту и предоставление должностному лицу ОВУ формализованных информационных ресурсов для поддержки принятия решений по управлению войсками (силами) [63] (2008).

информационная инфраструктура системы управления войсками (силами)[2] (ИИ СУВ) — специальным образом организованная система ресурсов (вычислительных, коммуникационных, информационных), «заточенная» на предоставление информационных услуг, главная из которых — качественная информационная поддержка управленческих решений [51] (2010).

информатизированные объекты — объекты, конструктивно включающие информационноемкие элементы, создаваемые на основе новых цифровых технологий.

С учетом этого оружие, создаваемое с помощью таких технологий, целесообразно относить к оружию на новых технологических принципах [207] (2007).

1.2. Информационные технологии

информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[4] [122] (2015).

информационная технология — совокупность приемов, способов и методов применения средств вычислительной техники при выполнении сбора, хранения, обработки, передачи и использования информации в рамках системы [59] (2002).

информационная технология управления войсками — обоснованная совокупность способов и средств получения, обработки, накопления и представления управленческой информации.

Анализ результатов повседневной деятельности воинских частей и соединений выявил, что отсутствие обоснованных рекомендаций по применению информационных технологий приводит к следующему распределению времени цикла управления: до 60—70% времени орган управления затрачивает на сбор и обобщение исходных управленческих данных, 20—25% — на документирование принятого решения и

[4] Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации».

только 5—20% времени — на практическую и творческую работу, связанную с принятием решения и его реализацией [143] (2008).

автоматизация управления войсками (силами)[1] — процесс оснащения штабов, пунктов управления и боевых комплексов средствами электронно-вычислительной техники и использования их в работе органов управления.

Интеллектуальной составляющей комплекса средств автоматизации автоматизированной системы управления войсками является программное обеспечение, которое делится на общее, общесистемное и специальное. Специальное программное обеспечение АСУВ состоит из расчетных, информационных задач и математических моделей. Последние выполняют существенную роль в процессе планирования операций (боевых действий) и управлении войсками (силами), обеспечивая прогнозирование развития обстановки и сравнительную оценку эффективности принимаемых решений [211] (2011).

автоматизация управления войсками (силами)[2] — оснащение штабов, пунктов управления, боевых комплексов средствами электронно-вычислительной техники, сопряженными с другими техническими устройствами, и их применение органами управления в боевой работе и повседневной деятельности.

Результат этого процесса — не только разработка и внедрение автоматизированных систем связи, средств обработки информации, но и совершенствование методов работы командиров и штабов. Именно автоматизация управления служит материальной основой реализации современных форм ведения военных действий [210] (2012).

автоматизация управления войсками — комплексный процесс, нацеленный на оптимизацию управления боем путем его интеллектуально-информационного предвидения и системного моделирования в целом и его непрерывного планирования на базе перспективных высоких технологий.

Ни один род войск или служба не в состоянии в одиночку достичь победы в противоборстве с боевой системой противника. Ракетные войска и артиллерия, разведка и авиация, ПВО и РЭБ, тем более внутренние и пограничные войска могут в единой системе управления успешно выполнить боевые задачи только при совместном (истинно едином) планировании, управлении, обеспечении, целеполагании в интересах единой боевой задачи [186] (2010).

информационные технологии в военно-политических целях — главы государств — членов Шанхайской организации сотрудничества в своем Заявлении по международной информационной безопасности, сделанном 15 июня 2006 года в Шанхае, констатировали, что использование современных информационных технологий в военно-политических целях может вызывать мировые катастрофы, сопоставимые по своим разрушительным последствиям с результатом применения оружия массового уничтожения [13] (2012).

новые информационные технологии (НИТ) — совокупность программно-аппаратных средств и методов диалога человека с ними, позволяющая последнему получать необходимый информационный продукт, изменять его качество (свойства), накапливать, хранить и обмениваться информацией в различных видах деятельности.

Принципиальная особенность новых информационных технологий заключается в предоставлении пользователям прямого доступа (без посредников) к информационным, интеллектуальным, вычислительным ресурсам распределенных информационных систем и опыту экспертов. При этом пользователь вовлекается в информационное пространство, созданное программно-аппаратными средствами, и получает возможность активно добывать информацию об интересующих его объектах, самом пространстве, управлять в определенной степени их свойствами [24] (1999).

унифицированная информационная технология — ее основой является: пространственное представление информации; единая система классификации и кодирования; унификация форматов хранения и представления информации [11] (1996).

специализированные информационные технологии — технологии, автоматизирующие заданные процессы управления и решающие конкретный класс задач управления, но обладающие преимуществами базовых технологий, такими, как: реализация автоматизированных функций и задач управления в терминах, понятных должностным лицам, занятым их выполнением; гибкая настройка средств автоматизации в процессе повседневной деятельности должностных лиц при изменении условий решения задач без их дополнительной переработки; обеспечение взаимодействия с существующими АСУ и КСА по передаче и обработке информации [213] (1997).

1.2.1. Аспекты создания и применения информационных технологий в АС ВН

информационная технология в АС ВН — отраженная в соответствующих документах совокупность взаимно согласованных приемов, способов и методов обработки информации, реализуемая с применением средств автоматизации в целях рационального и эффективного решения задач при выполнении функций сбора, хранения, обработки, отображения, передачи и использования данных.

С учетом особенностей функционирования системы управления Вооруженных Сил и специфики информационных технологий проблемы их создания и применения в АС ВН целесообразно рассматривать в следующих основных аспектах: системном, функциональном, эксплуатационном (пользовательском) и организационно-технологическом [61] (2001).

системный аспект создания и применения информационных технологий в АС ВН — предполагает обеспечение единства системы управления как по «вертикали» — иерархии органов управления войсками (силами), так и по «горизонтали» (создание соответствующих контуров автоматизированного управления). Исходя из этого необходимо уточнить роль и место ИТ в АС ВН.

АС ВН создаются в целях повышения качества принимаемых решений и обеспечения устойчивости, непрерывности, оперативности и скрытности управления. В свою очередь, качество управленческих решений непосредственно зависит от информации, на основе которой они принимаются. Поэтому ИТ призваны обеспечить адекватное восприятие должностными лицами информации, циркулирующей в системе управления войсками (силами), с учетом уровня управления, полномочий лица, принимающего решение, и других факторов.

Методологически важно правильно оценивать соотношение и взаимосвязь ИТ и информационного обеспечения автоматизированных систем. ИТ базируются на информационном обеспечении системы и должны обеспечивать информационное единство в рамках предметной области создания и применения АС ВН. Это предполагает формирование (разработку) единого понятийного и терминологического аппарата; унифицированных форм документов (УФД) как средства общения должностных лиц системы управления; правил формализации информации и формирования УФД, а также средств, обеспечивающих эф-

фективность их автоматизированной обработки (систем классификации и кодирования информации, языков описания, хранения и манипулирования данными); единой системы протоколов информационного взаимодействия [61] (2001).

функциональный аспект создания и применения информационных технологий в АС ВН — отражает их способность поддерживать информационно-расчетную и аналитическую деятельность должностных лиц в условиях, с одной стороны, повышения сложности задач, решаемых органами военного управления различных уровней; разнообразия и нестандартности ситуаций, требующих нестандартных решений; возрастания объемов разнородной информации, необходимой для выработки и обоснования принимаемых решений. С другой стороны, эти условия характеризуются сокращением численности органов управления при повышении требований к оперативности их деятельности.

Как отмечают отечественные и зарубежные специалисты, в административно-управленческой деятельности должностных лиц органов военного управления в настоящее время значительную часть (до 80%) составляет переработка документальной информации. Успешное решение этой задачи возможно при комплексном применении в АС ВН так называемых интеллектуальных информационных технологий. При этом интеллектуализация предполагает поддержку именно аналитической деятельности должностных лиц, начиная с восприятия и семантического анализа разнородной информации и завершая принятием решений [61] (2001).

эксплуатационный (пользовательский) аспект создания и применения информационных технологий в АС ВН — состоит в том, что информационные технологии должны быть максимально упрощены и комфортны по способам и формам их применения, поскольку оперативный состав органов военного управления работает, как правило, в экстремальных условиях, при значительных психологических и физических нагрузках.

Следует отметить, что задача создания так называемого дружественного пользовательского интерфейса в определенной степени входит в противоречие с разнородностью обрабатываемой информации, а также с задачей интеллектуализации информационных технологий, приводящей к их значительному усложнению. Опыт применения разработанных к настоящему времени ИТ показал, что эта задача пока не

решена. Применение оперативным составом большинства таких технологий без посредничества разработчиков или специально подготовленных операторов крайне затруднительно [61] (2001).

организационно-технологический аспект создания и применения информационных технологий в АС ВН — охватывает вопросы организации процесса их программно-технической реализации, внедрения и практической эксплуатации в АС ВН, т.е. речь идет о создании эффективных технологий разработки, внедрения и сопровождения программных средств и информационных систем. С этой целью необходимо разработать пакет организационно-распорядительных и нормативно-методических документов, охватывающих все эти вопросы.

Создание и внедрение ИТ в АС ВН предполагает участие большого числа организаций как Министерства обороны (органы военного управления, заказывающие органы, научно-исследовательские организации), так и научно-исследовательских организаций Российской академии наук и промышленности. Поэтому решение приведенных выше проблем требует четкой организации процесса создания и внедрения информационных технологий как в рамках ВС РФ в целом, так и в рамках отдельных систем или даже подсистем.

Суть организационной проблемы в общем виде может быть выражена следующим образом — обеспечение единства, целенаправленности и эффективности процессов создания ИТ за счет обоснованной и согласованной политики заказов, централизованного руководства и рационального распределения работ в кооперации исполнителей, стройной и полной системы нормативно-технической документации, рационального распределения финансовых средств на различных этапах жизненного цикла систем, создаваемых с использованием этих ИТ [61] (2001).

1.2.2. Интеллектуальные технологии в информационно-аналитической деятельности ОВУ

интеллектуальные информационные технологии — информационные технологии, интегрирующие как общие технологии управления знаниями, деловой разведки, управления деловыми процессами и документами, так и ряд других интеллектуальных технологий и средств, специально развиваемых для военных приложений.

Данные технологии в настоящее время становятся базовыми для автоматизации управления большими организационными системами, к которым в первую очередь относятся ОВУ. В системах такого рода имеется возможность реализовать автоматическую подготовку информации о рассматриваемой области, предмете, процессе и осуществить интеграцию этих «формальных» знаний с неформальными знаниями группы лиц (руководителей, специалистов, экспертов), которые принимают решение. Хотя в различных источниках эти системы называются по-разному («системы поддержки принятия решений», «ситуационные центры» или «центры принятия стратегических решений» и др.), они обладают, в частности, следующими общими концептуальными свойствами:

— концентрация всей необходимой для принятия решений информации в едином информационном хранилище, повышение ее качества (полноты и достоверности), обеспечение быстрого и эффективного доступа к ней лиц, принимающих решения (ЛПР);

— автоматическое выделение критически важной информации, характеризующей качественное изменение ситуации в предметной области;

— объединение аналитических средств системы и интеллектуальных возможностей ЛПР и экспертов, включаемых в систему в качестве ее активных элементов;

— накопление коллективного опыта решения проблем, использование его для решения новых проблем, обеспечение преемственности в управлении. Такой опыт и знания должны аккумулироваться в разрабатываемых моделях предметной области, а также в регистрируемых в системе сценариях коллективного решения проблем;

— предоставление ЛПР и экспертам средств поддержки процедур коллективной выработки и принятия решений, а также широкого спектра инструментов, необходимых для создания моделей решаемых проблем;

— предоставление ЛПР и экспертам информации и результатов моделирования в виде интерактивных визуально-ориентированных динамических моделей (системы визуальных образов) решаемых проблем, позволяющее вовлекать в решение задач интуитивные возможности человека [132] (2002).

инновационные технологии — информационные технологии, которые позволяют:

во-первых, выделять полезную информацию по решаемой проблеме из огромного объема данных, имеющих к ней, казалось бы, самое отдаленное отношение;

во-вторых, собирать и обобщать информацию, необходимую для принятия стратегических решений;

в-третьих, интуитивно находить, проверять и уточнять любые гипотезы или даже не сформулированные до конца идеи о наиболее важных факторах, влияющих на решение проблемы;

в-четвертых, исследовать информацию для выявления скрытых тенденций и схем, которые невозможно обнаружить с помощью традиционных способов анализа.

Иначе говоря, такие технологии позволяют перейти от фактов и знаний типа «знать где», «знать кто» к технологичным знаниям: «знать как», «знать почему», «знать что».

В то же время эти технологии поддержки процессов получения и сохранения технологичных знаний требуют дополнительных усилий по преобразованию (форматированию, кодированию, классификации) обрабатываемой системой информации, а также создания соответствующего информационного и лингвистического обеспечения. В частности, необходимы такие средства кодирования и классификации данных, которые позволяли бы создавать так называемые многомерные кубы данных и обеспечивать основные составляющие структуры информационных хранилищ — таблицы фактов и таблицы измерений, а также тезаурусы, поддерживающие мощные системы отношений между понятиями предметной области [132] (2002).

1.2.3. Информационные отношения

информационные отношения — отношения (взаимодействия) между информационными носителями.

Внутренними будем называть информационные отношения в границах информационных систем, а внешними — информационные отношения системы с другими системами и со средой их обитания.

По характеру носителей информационные отношения могут быть разделены на три типа: объект — объект, субъект — субъект, субъект — объект.

По целям функционирования деятелей информационные отношения в условиях коалиций или конфликтов разделяют на отношения сотрудничества и соперничества, дезориентирования, дезинформирова-

ния и дезорганизации с возможностью преобразования субъекта в объект и обратно [50] (1998).

носитель информации — вещественное (бумага, металл, дерево, дорожное покрытие и т.д.), энергетическое (электромагнитное, акустическое, тепловое и т.п.) или вещественно-энергетическое образование естественного, искусственного или гибридного происхождения, способное воспринимать от источника, хранить (запоминать) и представлять (воспроизводить) пользователю информацию (дезинформацию).

Статической принято называть информацию на вещественных, а динамической — на энергетических носителях [50] (1998).

носители информации — информационно-емкие средства, способные в широких масштабах осуществлять все виды информационных процессов: сбор, хранение, накопление, обработку и передачу информации [162] (2002).

информационный деятель — носитель информации, способный вступать в информационные отношения (взаимодействия) с другими информационными носителями.

Человек и компьютер могут рассматриваться в качестве информационных деятелей, будучи включенными в соответствующие информационные отношения. Активный информационный деятель является субъектом (например, орган управления), а пассивный — объектом (например, объектом управления) в структуре информационных отношений. При этом структурированного информационного деятеля (деятеля-систему) будем называть информационной стороной [50] (1998).

информационная система — система, составленная из информационных носителей и деятелей, объединенных целесообразными информационными отношениями.

Для любой системы должны быть определены целевое значение, состав, структура и алгоритм функционирования. Упорядоченную совокупность внешних и внутренних отношений (взаимодействий) информационной системы будем называть системой информационных отношений [50] (1998).

1.2.4. Опыт создания информационных систем в интересах ОВУ

Система стандартных справок — разработка первой информационной системы (ИС) в 27 ЦНИИ МО началась в 1959 году под руководством И.А. Криницкого при активном участии В.И. Богатырева и Г.А. Миронова. В результате была создана ИС, получившая название «Система стандартных справок». В дальнейшем работы по созданию систем справочного характера были продолжены под руководством Г.Г. Белоногова. Им были разработаны теоретические основы представления информации в ИС, известные как «универсальная триада».

Практические и экспериментальные работы по созданию ИС на основе использования «универсальной триады» представления фактографической информации осуществлялись под руководством А.П. Новоселова. Активное участие в создании информационно-поисковых систем (ИПС) этого типа принимали И.И. Быстров, В.Ф. Денисов, Н.Т. Губарь, Е.И. Стогов и многие другие. ИПС имели язык запросов интерпретирующего типа, с помощью которого можно было задавать условия поиска хранимой в ИПС информации и формировать выходные сообщения требуемого содержания. В этом же коллективе создавались и первые документальные ИПС (ДИПС), в процессе разработки которых были проведены большие работы по исследованию текстовой информации, получены необходимые статистические данные, разработаны тематические словари словоформ и др. Эти работы велись на ЭВМ «Сигма» и СПЭМ [99] (2009).

Система автоматического комплексирования расчетных задач (САК РЗ) — с 1965 года коллективом под руководством Б.Н. Абрамова и Ю.И. Беззаботнова проводились исследовательские и практические работы по созданию ИС, обеспечивающей программы расчетных задач информацией в виде массивов данных требуемого содержания и структуры. В результате была создана ИС, в которой информация хранилась в структурированном виде, при этом структура хранения информации была описана на некотором языке, представляющем собой аналог языка описания данных современных систем управления базами данных (СУБД). Эта ИС получила название «Система автоматического комплексирования расчетных задач», поскольку в ее составе имелся язык описания последовательности решения комплексов задач. Фактически это была одна из первых ИС, построенная на принципах

современных СУБД. Эта ИС имела непроцедурный язык запросов (аналог современных процедурных языков манипулирования данными СУБД). Одновременно с формированием массивов данных для программ расчетных задач САК РЗ позволяла оформлять результаты их решения в виде документов табличной формы, т.е. одновременно выполняла и функции справочной системы [99] (2009).

язык «Омега» — работы по созданию первых ИС показали, что для их эффективного функционирования нужны программные средства управления работой ЭВМ (управления памятью, стандартными функциями и др.). Поэтому одновременно с ИС на ЭВМ «Сигма» разрабатывалась обслуживающая система, которая по сути являлась прототипом современных операционных систем. Эта работа велась коллективом под руководством Н.И. Рахманова. Обслуживающая система управляла внешней памятью, устройствами ввода-вывода информации, каналами связи, стандартными программами, транслятором языка «Омега», разработанного в институте, и т.д. Основной вклад в разработку языка «Омега» внесли А.М. Бухтияров, В.Л. Голубев, И.А. Милешкин, Б.И. Касьяненко и др. [99] (2009).

Автоматизированная информационно-справочная система (АИСС) — разрабатывалась под руководством Л.И. Озеранского для конкретной предметной области с набором функций по ведению базы данных, формирования на ее основе заданного перечня документов табличной формы, с высокой надежностью функционирования системы и защиты информации. Активное участие в создании системы принимали Ю.А. Тихомиров, В.А. Костиков, А.Н. Горбунов и др. АИСС была доведена до практической работы на стенде института со значительным улучшением ее временных характеристик по сравнению с возможностями используемых компонентов СУБД БАСОД [99] (2009).

1.3. Информационные ресурсы

информационный ресурс[1] — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, базах данных, других информационных системах) [148] (2008).

информационный ресурс[2] — собственно информация, а также носители, на которых она находится.

Методология количественной и качественной оценки информационных ресурсов пока не разработана. Не решена проблема их формирования.

Этому есть, на наш взгляд, вполне объективные причины. Дело в том, что информационный ресурс (как ресурс информации) — вещь абстрактная. Информация в материальном виде не существует, поэтому ее невозможно непосредственно поразить (уничтожить) в целях завоевания информационного превосходства. Говорить о поражении (или изменении) информации можно только условно, подразумевая воздействие на ее соответствующие материальные носители. Причем эта условность допустима в очень ограниченных рамках, ибо носители, например, электронной информации являются, как правило, элементами (микроцелями) на типовых объектах системы управления, вооружения и военной техники, претерпевших качественные изменения в результате информатизации. Комплексное поражение таких объектов противоборствующими сторонами с применением самых разных средств и составляет основу вооруженной (но отнюдь не информационной) борьбы. Абсолютизация же условности ведет к искажению представлений об объективной реальности в этой области [162] (2002).

информационные ресурсы — важнейший элемент информатизации.

Они поставлены в один ряд с другими ресурсами: сырьевыми, людскими, финансовыми.

Законодательно определенная ясность в отношении содержания информационных ресурсов, конечно же, не решает всех проблем, и в первую очередь их накопления в новой технологической среде. Попытки простого переноса информации в среду информационных систем в виде текстов и графики не всегда дают желаемый результат. Чаще происходит наоборот, так как разрушается важный, естественный и привычный для человека защитный барьер из «бумажных» процедур, ограничивающий информационный доступ. Лавинообразный поток сообщений, получаемых с экрана дисплея или в распечатке, подчас пугает и запутывает пользователя, лишая его возможности усвоить и оценить всю информацию. Отсюда вытекает проблема формирования информационных ресурсов. Она осложняется тем, что на сегодняшний день нет научно обоснованной, общепринятой методики описания предметной области, пригодной для переноса информации в новую технологическую среду.

Каждый эксперт описывает предметную область содержательно на основе собственных представлений о ней, что создает ряд трудностей, связанных с формализацией такой информации и ее применением как продукта, ориентированного на широкий диапазон запросов. Содержательное описание включает в основном фактографические сведения в виде общих признаков, свойств объектов, их связей с другими объектами. Как правило, этого бывает недостаточно для перевода информации в новую технологическую среду. Формализация знаний требует присвоения информационным объектам дополнительных признаков в виде понятий и процедур, ориентированных на конкретные программные средства.

Поэтому создание информационных систем, вероятно, повлечет за собой разработку определенных правил, включающих рекомендации по внедрению и применению системы описания видов деятельности в новой технологической среде; системы классификации информационных ресурсов по установленным признакам; порядка выбора соответствующих технологических элементов информационных систем, обеспечивающих получение информационных продуктов нужного качества [24] (1999).

информационные ресурсы ВС РФ[1] — отдельные документы и массивы документов в библиотеках, архивах, фондах, банках и базах данных автоматизированных систем управления войсками (силами)[5] [17] (2013).

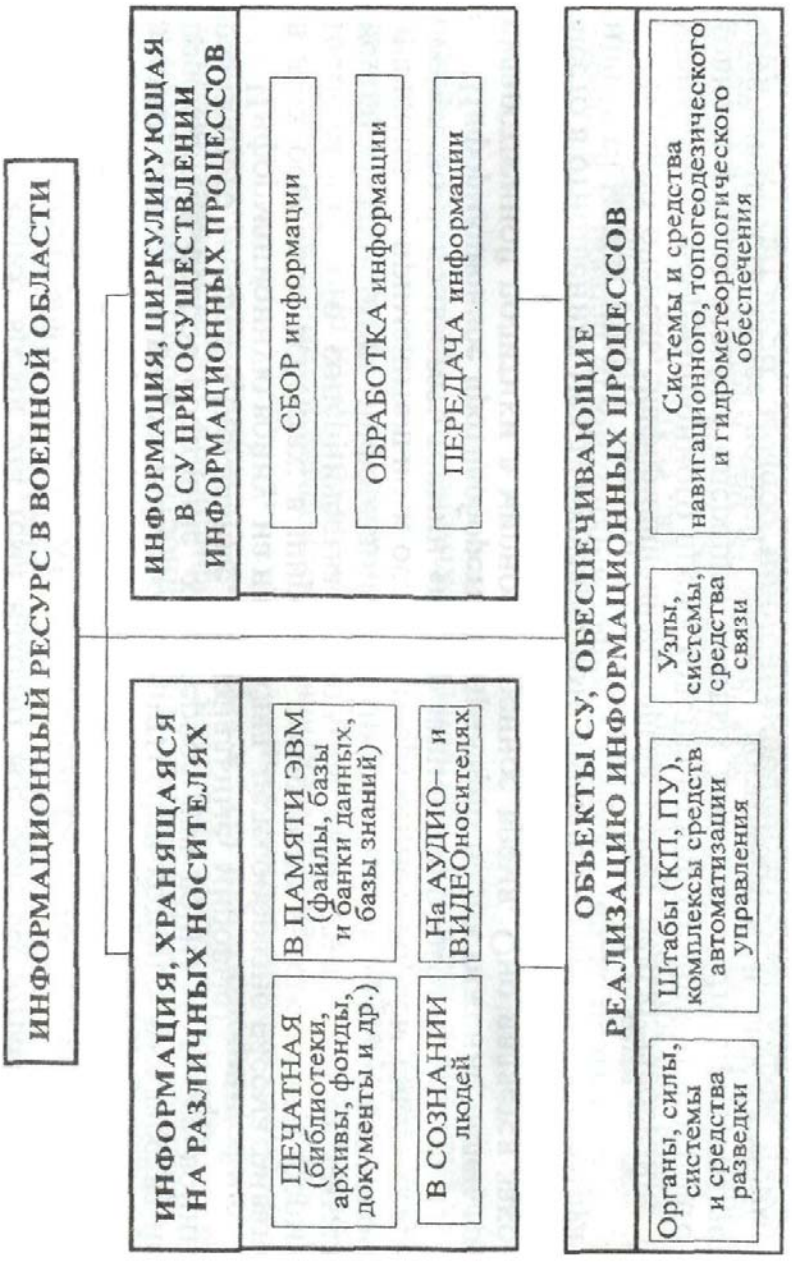
информационные ресурсы ВС РФ[2] — различные документы боевого управления (приказы, распоряжения, донесения, сводки), нормативные документы (штаты, нормы), справочная информация (классификаторы, словари), научно-техническая информация, информация, циркулирующая в автоматизированных системах военного назначения, и другие массивы информации (карты, схемы, плакаты, фонды, картотеки и др.).

Информационные ресурсы ВС РФ имеют большие объемы, они различаются по типам, формам представления, структурам, степени старения [16] (2004).

информационный ресурс в военной области — информация, хранящаяся на различных физических носителях и циркулирующая в

[5] ГОСТ РВ 52333.1—2005.

системах управления войсками (силами) при реализации информационных процессов, а также объекты инфраструктуры системы управления, обеспечивающие эти процессы (рис.) [171] (1997).



Содержание информационного ресурса в военной области

информационный ресурс инфосферы управления войсками (силами) — информация в области управления войсками (силами), которая зафиксирована на материальных носителях или в любой другой форме, обеспечивающей ее хранение и передачу во времени и пространстве между различными категориями должностных лиц ОВУ в интересах решения различных задач управления.

На практике информационные ресурсы инфосферы управления войсками (силами) представляют собой знания в области управления войсками (силами), сформированные в виде отдельных документов или массивов документов, алгоритмов, математических моделей, математических методов, программ, зафиксированных на различных материальных носителях. Кроме того, документы, входящие в состав информационных ресурсов Вооруженных Сил Российской Федерации, могут включать: документы боевого управления (боевые приказы, распоряжения, донесения, сводки), нормативные документы (приказы, нормы, штаты), справочную информацию (классификаторы, словари терминов), учетную информацию (анкеты, картотеки), научно-техническую информацию (печатные издания, отчеты о научно-исследовательских и опытно-конструкторских работах), информацию, циркулирующую в автоматизированных системах (базы данных, файлы, сообщения) и другие массивы информации (карты, фонды, схемы, плакаты, отдельные файлы и пр.) [63] (2008).

информационное обеспечение автоматизированной системы — совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в автоматизированной системе при ее функционировании [151] (2010).

информационное обеспечение — совокупность баз данных и отдельных массивов (файлов), необходимых для автоматизированного управления [160] (2015).

1.3.1. Военные документы

документ — зафиксированная в материальной среде идентифицируемая информация, созданная, полученная и сохраняемая органи-

зацией или физическим лицом в качестве доказательства при подтверждении правовых обязательств или деловой деятельности[6] [87] (2015).

электронный документ — объект, зафиксированный в материальной среде, доступный для восприятия человеком с использованием технических устройств и предназначенный для информационного взаимодействия мыслящих субъектов в социальной среде [87] (2015).

1.3.1.1. Формализация боевых документов

информация в боевых документах — отражается условными знаками, словами, словосочетаниями и предложениями. Основными их чертами являются предельная ясность изложения, сжатость и лаконичность высказываний, краткость и четкость формулировок, не допускающих различных толкований, точность содержащейся в документах информации, динамичность и экспрессивность ее передачи, однозначность восприятия. Главная причина стремления к краткости и лаконичности боевых документов заключается в необходимости экономить время, затрачиваемое на ознакомление с документами, их разработку и передачу. Сжатый текст воспринимается быстрее и запоминается в большем объеме [153] (2009).

формализация боевых документов — формализация, используемая в настоящее время должностными лицами органов управления.

Ее элементы подразделяются на структурные, условные, произвольные и семантические.

Структурная (документальная) формализация проявляется во всей номенклатурной организации языка боевых документов от принципов их классификации до внешнего оформления композиционной структуры текста. Одно из средств структурной формализации текста боевого документа — рубрикация, т.е. графическое разделение текста на составные части.

Условная формализация заключается в особом употреблении пунктуации, применении топографических, тактических и других условных знаков, символов и обозначений. Использование пунктуации обеспечивает правильную передачу информации только в том случае, если адресат и отправитель одинаково понимают значение этого свое-

[6] ГОСТ Р ИСО 15489—1—2007. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования.

образного кода. В противном случае всякая ошибка приводит к искажению в той или иной степени смысла текста или к его непониманию, т.е. к потере информации.

Произвольная формализация подразумевает замену отдельных лексических единиц (слов), а также целых предложений и понятий различными, заранее обусловленными комбинациями букв и (или) цифр.

Семантическая формализация заключается в широком использовании различных сокращений, что приводит к очень существенному сжатию текста боевого документа [153] (2009).

1.3.1.2. Автоматизированная разработка оперативных документов

методология автоматизированной разработки оперативных документов — методология, заключающаяся в переходе от обмена неформализованными или слабоформализованными документами к обмену фактографическими данными в реальном масштабе времени или близком к нему с широким использованием различных систем поддержки принятия решений, ориентированных на непрерывный мониторинг обстановки.

Необходимость перехода обусловлена тем, что неформализованные документы воспринимаются как данные, не подлежащие автоматической смысловой (семантической) обработке. Анализ и обработку их содержания может осуществлять только человек (примером может являться разработка структурированных, но неформализованных оперативных директивных текстовых документов, осуществляемых должностными лицами органов управления фактически вручную).

Основными положениями методологии являются:

— информационный обмен, осуществляемый с использованием графических и текстовых оперативных документов, порядок разработки которых определен руководящими документами (в графических оперативных документах информация в основном отображается условными знаками, словами, словосочетаниями и редко предложениями; в текстовых — в основном предложениями, при помощи которых должностные лица выражают свои мысли, обращаются друг к другу с приказаниями и т.д.);

— разработка оперативных документов с применением электронной цифровой подписи;

— разработка всего комплекта оперативных текстовых и графических документов (в первую очередь директивных и планирующих);

— разработка комплексной методики формализации информации оперативных документов;

— совершенствование геоинформационных систем военного назначения, моделирующая среда которых должна позволять автоматическое формирование данных для прогноза результатов операций (боевых действий);

— создание удобного интуитивно понятного унифицированного интерфейса на автоматизированных рабочих местах должностных лиц;

— разработка методики ввода (корректировки) должностными лицами информации, реализуемой с помощью формуляров;

— разработка технологии отображения оперативных документов, реализующая возможность отображения их содержания как в текстовом виде, так и в графическом виде на основе одних и тех же фактографических элементов данных на автоматизированных рабочих местах различных должностных лиц;

— совершенствование системы защиты информации, обеспечивающей разграничение доступа не только к различным частям (абзацам) оперативных документов, но и к их отдельным предложениям, а при необходимости и к составляющим предложения словосочетаниям (как текстовых, так и графических оперативных документов) [127] (2014).

комплексная методика формализации информации оперативных документов — методика, связанная с особенностями языка оперативных документов.

При поиске новых подходов в части формализации данных в первую очередь необходимо учитывать лексические и фразеологические особенности языка оперативных документов, т.е. словарный и фразеологический (устойчивые словосочетания) состав языка, имеющий свои определенные лексические и фразеологические особенности, обусловленные лингвистическими факторами, вытекающими из целенаправленности, характера и задач оперативных документов.

В ходе автоматизации разработки оперативных документов следует учитывать основные черты оперативных документов, в том числе: предельную ясность изложения, сжатость и лаконичность высказываний, краткость и четкость формулировок, не допускающих различных толкований, определенность содержащейся в оперативных документах

информации, динамичность и экспрессивность ее передачи, однозначность ее восприятия. Кроме этого, необходимо стремиться к краткости и лаконичности оперативных документов и необходимости экономии времени, затрачиваемого на их разработку, передачу (в том числе и на ознакомление с ними). Сжатый текст воспринимается быстрее и запоминается в большем объеме.

Для языка оперативных документов характерно использование довольно ограниченной специальной лексики, причем лексические единицы употребляются в своих основных предметно-логических значениях. Характерной чертой оперативных документов на лексическом уровне является их насыщенность специальной военной и военно-технической терминологией, широкое использование всякого рода сокращений и условных обозначений, употребление специальной военной фразеологии.

Важно исследовать особенности языка с точки зрения морфологии, синтаксиса и стилистики, так как в оперативных документах информация отображается не только условными знаками, словами, словосочетаниями, но и предложениями (грамматическими единицами, оформляющими высказывание — сообщение, побуждение).

Используемые должностными лицами органов управления в настоящее время элементы формализации языка оперативных документов можно подразделить на структурные, условные, произвольные, семантические и позадачные [127] (2014).

структурная (документальная) формализация — формализация, проявляющаяся во всей номенклатурной организации языка оперативных документов от принципов их классификации до внешнего оформления композиционной структуры текста.

Одним из средств структурной формализации выступает рубрикация, позволяющая делить текст на составные части [127] (2014).

условная формализация — формализация, заключающаяся в особом употреблении пунктуации, применении топографических, оперативно-тактических и других условных знаков, символов и обозначений [127] (2014).

произвольная формализация — формализация, подразумевающая замену отдельных лексических единиц, а также целых предложений и понятий различными, заранее обусловленными комбинациями букв и (или) цифр [127] (2014).

семантическая формализация — формализация, выражающаяся в широком использовании в текстах оперативных документов различных сокращений, ограничиваемых руководящими документами (соответствующими уставами, наставлениями и т.д.) [127] (2014).

позадачная формализация — формализация, заключающаяся в отображении неформализованной информации оперативных документов в виде упорядоченной совокупности задач (формализуемых процессов), выполняемых различными объектами последовательно и (или) параллельно и представляемых в виде множества семантически объединенных между собой элементов (подмножеств), состоящих из признаков или классификационных терминов (описываемых соответствующими классификаторами) [127] (2014).

методика ввода (корректировки) должностными лицами информации — методика, реализуемая с помощью формуляров, содержащих поля наименований характеристик и их значений, семантически объединенных между собой и отражающих какой-либо аспект предметной области.

Содержание конкретного документа может отражаться одним формуляром или их совокупностью (перечень и содержание формуляров определяется структурой и содержанием разрабатываемых оперативных документов) и представляться в различной форме (в том числе в виде словосочетаний или предложений).

Ввод (корректировку) фактографической информации следует осуществлять заполнением полей формуляров (вводом алфавитно-цифровых символов с клавиатуры или выбором необходимых данных из всплывающих меню контекстной помощи по установленным правилам формализации) и последующим сохранением данных. В зависимости от названия документа, его структуры и содержания в соответствии с методикой ввода (корректировки) перечень разрешенных для ввода (корректировки) значений должен подгружаться из контекстно-зависимых классификаторов и словарей (с реализацией возможности ввода информации средствами геоинформационной системы) [127] (2014).

1.3.1.3. Система обработки мобилизационных документов

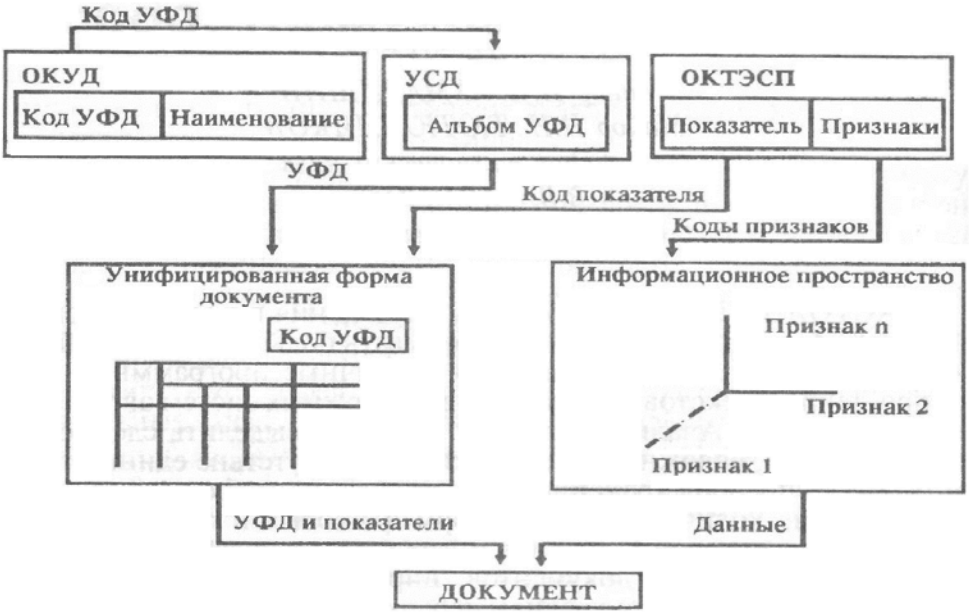
мобилизационные документы — органы управления ВС, занимающиеся мобилизационными вопросами, в процессе своей повседневной деятельности перерабатывают большие объемы информации, основным средством представления которой являются документы. Анализ показал, что более 80% мобилизационной информации является хорошо формализованной фактографической информацией, содержащейся в анкетных, линейных или табличных типах документов, в отличие, например, от организационно-мобилизационной, которая в основном представляет собой плохо формализованную документальную информацию в текстовых документах на естественном языке.

Среди всех мобилизационных документов незначительную часть составляют документы персонального учета людских и материальных ресурсов, информация в которых закодирована классификационными признаками в терминах общероссийских и ведомственных классификаторов. Около половины документов — это донесения табельной отчетности, содержащие значения различных первичных показателей, полученных путем подсчета числа объектов персонального учета по заданным признакам. Остальная часть приходится на различные аналитические документы со вторичными показателями, рассчитываемыми в процессе решения задач управления по различным математическим моделям [213] (1997).

система обработки документов (СОД) — система, предназначенная для организации сбора, контроля, обобщения и обработки поступающих донесений табельной отчетности в соответствии с требованиями по построению Единой системы классификации и кодирования информации; проектирования форм донесений согласно табелю срочных донесений, наставлений, положений и других нормативных документов в соответствии с требованиями по построению унифицированных систем документации (УСД); получения оперативных документов и различных справочных сведений по запросам должностных лиц [213] (1997).

1.3.1.4. Система автоматизации документооборота

система автоматизации документооборота — предназначена для организации ввода, обработки, хранения, поиска, передачи информации и подготовки документов.



Функциональная схема системы автоматизации документооборота

Она обеспечит: оперативное изменение действующих и разработку новых форм документов; оперативный поиск и выборку информации; обмен данными на всех уровнях иерархии системы управления в едином формате; исключение дублирования информации и устранение избыточности при хранении данных.

Система автоматизации документооборота состоит из подсистем: ввода, обработки, передачи и контроля исполнения документов; ведения унифицированных форм документов (УФД); ведения классификатора управленческой документации; ведения табеля представляемых документов; ведения раздела Общероссийского классификатора технико-экономических и социальных показателей; информационно-справочной или информационно-расчетной [11] (1996).

унифицированная система документации (УСД) — содержит данные для организации процесса документооборота и предназначена для унификации и стандартизации документов в интересах последующей обработки их средствами вычислительной техники. Ведение УСД предусматривает внесение изменений и дополнений в структуру и состав формируемых документов, разработку новых и исключение действующих в соответствии с проектом унифицированной формы документов [11] (1996).

классификатор управленческой документации (КУД) — предназначен для идентификации каждого документа в УСД, что позволит четко организовать поиск и учет документов, циркулирующих в системе управления. Объектами классификации КУД являются формы конкретных документов [11] (1996).

Общероссийский классификатор технико-экономических и социальных показателей (ОКТЭСП) — предназначен для стандартизации информационного обеспечения в системах автоматизации документооборота. Целью его создания является объединение понятий предметной области, а также общегосударственных и ведомственных классификаторов в общую систему с использованием единой системы классификации и кодирования [11] (1996).

1.3.1.5. Система электронного документооборота

автоматизированная информационная система электронного документооборота Министерства обороны Российской Федерации (СЭД МО РФ) — целью ее создания является формирование единого информационного пространства Министерства обороны в части электронного документооборота на основе единых методологических, организационных и информационно-технологических решений, учитывающих организационно-штатную структуру и особенности делопроизводства в Министерстве обороны Российской Федерации.

Уникальность такой системы заключается в ее способности обеспечивать свойство юридической значимости электронных документов, позволяющее электронному документу вызывать определенные правовые последствия и тем самым представлять одну из форм выражения права [87] (2015).

1.3.2. Справочная информация

общесистемный базовый словарь, классификаторы и унифицированные документы — в конце 1970-х годов разработчики ИС поняли, что без создания и внедрения в АСУ единых классификаторов, словарей и унифицированной системы документов невозможна информационная и терминологическая совместимость баз данных, используемых при решении информационных и расчетных задач. С этой целью в институте в ходе выполнения ряда комплексных научно-исследовательских работ были разработаны, утверждены и приняты в опытную эксплуатацию: общесистемный базовый словарь, включающий систематический и алфавитный словари; словарь аббревиатур терминов ВС; более десяти специальных классификаторов для Генерального штаба ВС и разновидности этих классификаторов для видов ВС и родов войск; системы унифицированных формализованных документов для Генерального штаба ВС и видов ВС и родов войск; методики по созданию словарей, классификаторов, унифицированных систем документации и баз данных. В этих работах активное участие принимали А.Д. Дубровин, Е.И. Пепеляев, К.Д. Денисов, А.И. Токмаков, А.И. Есаулов, Б.П. Рыбаков, Н.В. Алтухова, В.В. Баранюк, Л.И. Кундрюкова, М.Д. Гостева, М.Н. Королева, Л.С. Соколова и др.

В середине 1980-х годов сотрудниками института по заказам Генерального штаба ВС для кодирования информации были разработаны 30 словников общим объемом более 60 тыс. слов. В последующем разработанные компоненты ИЛО после опытной эксплуатации на объектах Генерального штаба ВС были тиражированы и направлены в войска для обязательного использования во всех вычислительных центрах. Одновременно сотрудниками института осуществлялась разработка средств автоматизированного ведения «Общесистемного базового словаря» и ряда классификаторов военного назначения, которые в дальнейшем использовались в создаваемых ИС. В их разработке принимали активное участие М.В. Мосолов, И.Л. Беляев, Н.В. Попов, В.В. Явкин и др. [99] (2009).

1.3.2.1. Классификаторы

классификатор — официальный документ, представляющий собой систематический свод наименований и кодов классификационных группировок или объектов классификации.

Информация в них классифицируется и кодируется различными методами (например, фасетным, регистрационным, порядково-серийным). Поэтому классификаторы часто имеют сложную структуру, которая может включать следующие компоненты: идентификационно-классификационный блок с кодом группировки и кодами объекта классификации; блок наименования, содержащий полное и сокращенное наименование объекта классификации, а также его аббревиатуру; информационный блок с признаками классификации, значения которых являются кодами других классификаторов, и дополняющие их параметры, отражающие качественные и количественные характеристики объекта классификации [25] (1996).

система классификации и кодирования оперативно-стратегической и военно-технической информации — постоянно развивалась в МО РФ, видах ВС, родах войск, в результате чего появилось более 300 классификаторов с уникальной структурой и терминологией. Следствием этого явилась разработка множества информационно несовместимых друг с другом АСУВ, что резко увеличило затраты на доработку при их сопряжении и объединении в систему.

Основными причинами такого положения являются: отсутствие единых требований к разработке и ведению классификаторов, а также их использованию при создании компонентов информационного обеспечения АСУВ; создание локальных классификаторов, дублирующих информацию в разных АСУВ; совпадение одних и тех же понятий в разных классификаторах и кодирование их разными кодами; отсутствие во многих классификаторах сокращенных наименований и устойчивых аббревиатур, которые используются в документах [25] (1996).

единая система классификации и кодирования оперативно-стратегической и военно-технической информации (ЕСКК ОС и ВТИ) — система, основанная: на методологическом единстве разработки классификаторов, совместном и согласованном их использовании во всех комплексах и задачах АСУВ; преемственности, заключающейся в поэтапной разработке и совершенствовании классификаторов при сохранении (в случае необходимости) функциональных возможностей ранее созданных классификаторов; разработке новых классификаторов, ориентированных на многоаспектное использование информации.

При создании ЕСКК ОС и ВТИ преследуется несколько целей: стандартизация информационного обеспечения процессов управления ВС на основе применения средств вычислительной техники; установление состава и содержания работ по классификации, кодированию оперативно-стратегической и военно-технической информации, единого порядка планирования и проведения этих работ в рамках ВС РФ. При создании ЕСКК ОС и ВТИ, по нашему мнению, должны решаться задачи: упорядочения, унификации, классификации и кодирования информации в системах управления ВС; обеспечения условий для автоматизации процессов управления, информационной совместимости взаимодействующих АСУ, методического единства при разработке, внедрении, ведении классификаторов и унифицированных систем документации в ВС РФ; создания комплекса взаимоувязанных классификаторов различных сфер и уровней применения, а также организации их ведения [25] (1996).

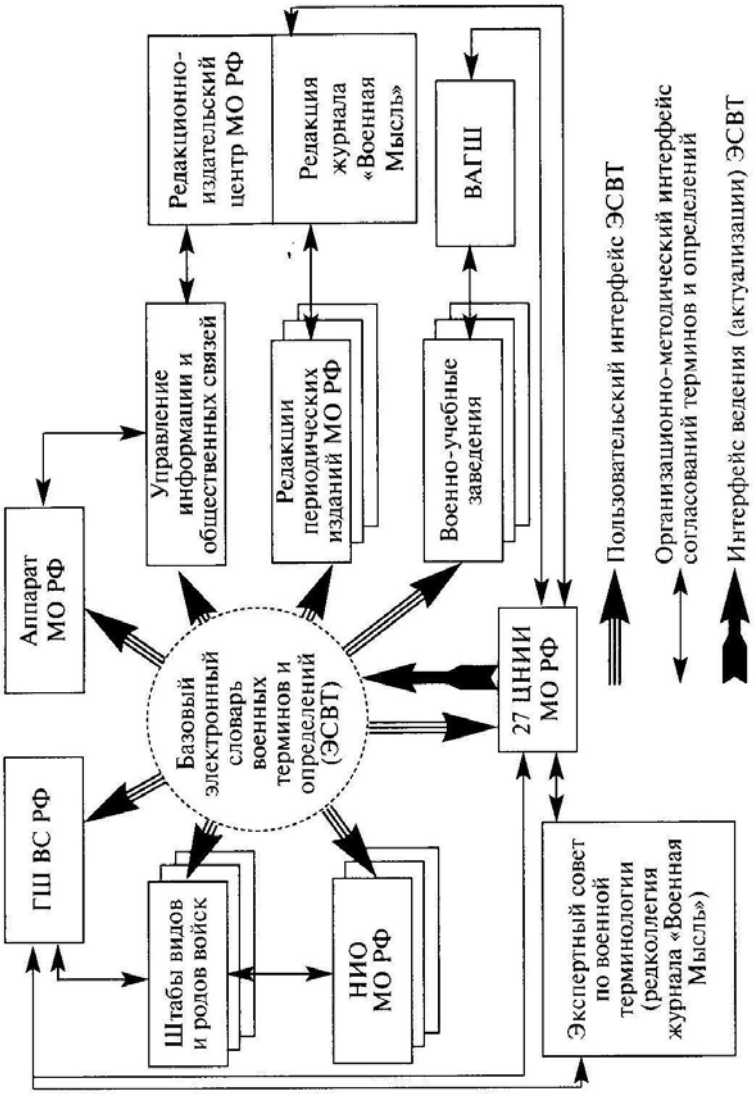
1.3.2.2. Словари

автоматизированная система терминологической экспертизы — система, обслуживающая весь документооборот в Вооруженных Силах [55] (2005).

базовый электронный словарь военных терминов и определений теории управления войсками (силами) — сердцевина автоматизированной системы терминологической экспертизы.

В самом общем виде организационно-методические аспекты функционирования этой подсистемы представлены на рис. на с. 39 [55] (2005).

базовый электронный словарь военных терминов и определений — с проблемой несогласованности понятийно-терминологической базы научно-педагогический состав Военной академии Генерального штаба Вооруженных Сил Российской Федерации столкнулся при разработке основополагающих уставных документов. Наличие большого количества различных словарей, содержащих часто противоречивые определения одних и тех же терминов, приводит к неоднозначности интерпретации и ошибочной трактовке понятий. Для решения этой



Укрупненная организационно-методическая схема использования и ведения (актуализации) ЭСВТ (вариант)

проблемы необходимо разработать базовый электронный словарь военных терминов и определений, правила включения в него терминов, а также программные средства его ведения и использования.

Задачи по ведению такого словаря целесообразно возложить на одно из подразделений службы информационных ресурсов Вооружен-

ных Сил. Для проверки обоснованности включения того или иного термина в словарь и проведения научной экспертизы понятийного аппарата в качестве экспертов могут привлекаться представители научно-исследовательских учреждений, ввузов, предприятий ОПК, а также научные редакторы военно-теоретического журнала «Военная Мысль» [120] (2011).

1.3.2.2.1. Терминологические словари

терминология — совокупность терминов, используемых в определенной области знаний (науки, техники и т.п.) [121] (2009).

терминологическая система — специальный язык обозначения знаний в сфере военного дела государства.

Сформулированная несколько десятилетий назад, терминологическая система военно-научных знаний не отвечает требованиям дня сегодняшнего, допуская неоднозначность, двусмысленность толкования как общенаучных, так и специальных военных терминов [54] (2006).

терминология боевых документов — довольно ограниченная специальная лексика, используемая в боевых документах. Причем слова употребляются, как правило, в своих основных предметно-логических значениях, хотя иногда могут употребляться и в других значениях.

Наиболее характерными чертами боевых документов являются насыщенность их специальной военной и военно-технической терминологией, широкое использование всякого рода сокращений и условных обозначений, наличие специальной военной фразеологии. Термины, как правило, употребляются только в одном, специфическом для данной информационной области значении, и именно в том, которое не вызывает двоякого толкования. Также широко применяются различные сокращения [153] (2009).

сокращения в боевых документах — отличающиеся от официально принятых и узаконенных в единых для всех видов Вооруженных Сил РФ инструкциях и наставлениях, как правило, не употребляются, поскольку это может затруднить понимание текста или сделать его совсем непонятным. Ведь даже сокращения, применяемые только в одном виде Вооруженных Сил, иногда совершенно непонятны в другом.

В лингвистической литературе сокращения принято делить в зависимости от числа и значения составляющих их компонентов на одно, двух-, трехкомпонентные и т.д. Например, однокомпонентные — А (армия), двухкомпонентные — КП (командный пункт), трехкомпонентные — ПОЗ (подвижный отряд заграждения). Более чем пятикомпонентные сокращения применяются редко. В боевых документах чаще всего встречаются двух- и трехкомпонентные сокращения [153] (2009).

требования к терминологической базе — результаты исследований показали, что в существующей системе есть серьезные недостатки общепонятийного, системного, терминологического характера, свойственные каждому из видов ВС и родов войск, поэтому при образовании новой системы важен единый подход к формулированию основных понятий и созданию новых структур технического обеспечения.

Прежде всего в системе должны быть четко определены все ее элементы и установлена взаимосвязь между ними. По нашему мнению, пока нет четкости в определении элемента, занимающего более высокий уровень по отношению к техническому обеспечению (это свойственно также системам боевого и тылового обеспечения). Таким элементом является система обеспечения боевых действий, которая сегодня не имеет ни четко сформулированной цели и вытекающих из нее задач, ни строгого распределения функций между входящими в нее подсистемами (видами обеспечения боевых действий), ни инструмента для установления взаимосвязи между ними и определения их места и роли в реализации предназначения видов ВС и родов войск.

Кроме того, всякая иерархическая структура должна быть построена на единой системе понятий. Как показывает анализ существующей в настоящее время терминологии в области технического обеспечения, иногда один и тот же термин различными источниками (энциклопедиями, словарями, ГОСТами и т.д.) трактуется по-разному. Это затрудняет выработку единых подходов, четкую формулировку основных понятий, ясную постановку задач и однозначное их понимание. Поэтому представляется важным соблюдать следующие основные требования, предъявляемые к терминологической базе.

Во-первых, каждый термин должен строго соответствовать природе явления. Так, словосочетание «вооружение и военная техника» многими воспринимается как невхождение вооружения в состав воен-

ной техники, что, естественно, не соответствует сути явления. Чтобы не нарушать данное терминологическое требование, корректнее, на наш взгляд, было бы использовать сочетание «вооружение и другая военная техника».

Во-вторых, определение термина не должно приводить к неоднозначности его трактования. Например, термин «ракета» в одних случаях понимается как ракета-носитель, в других — как ракета-носитель вместе с головной частью (космическим аппаратом).

В-третьих, термин должен соответствовать понятию конкретного иерархического уровня, при этом определения более низкого уровня (производного понятия) не должны противоречить определениям более высокого уровня (основного понятия). Например, термины «ракетное вооружение» и «специальное вооружение» противоречат понятиям более высокого уровня, а именно понятию «вооружения». Действительно, ракетное вооружение по формальным признакам не включает в себя средства поражения, а специальное вооружение — средства доставки и средства управления применением оружия. Для устранения этого недостатка следовало бы закрепить руководящими документами структурное включение ядерных боеприпасов в состав ракетного вооружения, а специальное вооружение назвать, например, «специальное оснащение» или «специальное боевое оснащение».

Следует отметить, что различные ведомства, издавая свои словари, ГОСТы, ОСТы и т.д., нередко не выполняют приведенных выше требований, нарушая тем самым единство терминологической базы [101] (2002).

1.3.2.2.1.1. Терминологические заторы военной информатизации

язык[1] — система знаковых единиц, выражающая совокупность понятий и мыслей и предназначенная для коммуникаций [53] (2012).

язык[2] — всепроникающий и фундаментальный компонент научного знания. Через систему языка субъект подключается к опыту определенного языкового коллектива, к социальной памяти общества в целом [54] (2006).

речь — конкретная реализация языка, облекаемая в устную или письменную форму [53] (2012).

слово — основная структурно-семантическая единица языка, служащая для наименования предметов и их свойств [53] (2012).

автоматизированная актуализация терминологической системы (языка) военной науки — по нашему мнению, сегодня самое время вспомнить один из основных принципов управления народным хозяйством в эпоху социализма — принцип опережающего развития производства средств производства. Не оснастив военную науку современными средствами производства и коммуникации новых военных знаний, трудно рассчитывать на положительный эффект внедрения полученных «вручную», а потому сомнительного качества, знаний в практику управления войсками. Поэтому разработка такого рода средств производства (в частности, технологий моделирования военных (боевых) действий различного масштаба) и оснащение этими средствами военно-научных организаций должно стать одной из главных стратегий научно-технической политики военной информатизации. И в составе этих средств должно быть предусмотрено достойное место для автоматизированной актуализации терминологической системы (языка) военной науки [53] (2012).

1.3.2.2.1.2. Терминосистема как важнейший элемент научно-методического аппарата военно-научных исследований

проблемы терминологии военной науки — причина проблем в неодинаковом, а порой и противоречивом толковании ряда терминов, которые приводятся в различных энциклопедиях, словарях, справочниках и порой даже в стандартах.

Часто в ходе системного научного исследования, будь то научно-исследовательская работа или разработка диссертации, возникает задача совершенствования действующей на этот период терминологии. Это подразумевает системный анализ существующих научных понятий и их взаимосвязей, а также при необходимости их корректировку, разработку новых элементов системы, а подчас и переработку всей системы терминов и определений в целом. При этом необходимо иметь в виду, что сегодня такая работа должна проводиться с учетом крайне необходимой информатизации всех сторон военного дела [121] (2009).

терминосистема — система научных понятий любой специальной сферы употребления (области знаний, ее части или раздела).

Терминосистему также определяют как понятийный аппарат конкретной науки.

При этом необходимо отметить, что терминосистема (как система понятий) является одним из основных компонентов конкретной научной теории. Вполне естественно, что принятая на тот или иной момент времени система понятий (терминосистема) отражает уровень развития изучаемой науки или ее области. Отсутствие стройной терминосистемы, как правило, говорит о проблемах и недостатках какой-либо конкретной области знаний.

В свою очередь терминосистема практически любой области знаний не является раз и навсегда установленным и непоколебимым изложением истин в последней инстанции. Ее развитие должно не только отвечать изменяющимся условиям и отражать складывающиеся реальности, но и носить прогностический (опережающий) характер. То есть практически любая терминосистема должна периодически подвергаться ревизии и претерпевать необходимые изменения с точки зрения перспектив развития науки [121] (2009).

термин[1] — слово или словосочетание, являющееся названием определенного понятия отдельной специальной области науки, техники, вооружения и т.д.

Для стандартизованной терминологии желательно, чтобы термин выражал только одно понятие, а понятие было представлено только одним термином [166] (2008).

термин[2] — слово или словосочетание специальной сферы употребления, являющееся наименованием (названием) понятия.

Термин является основным элементом терминосистемы.

В соответствии с принятыми к употреблению в России рекомендациями к термину предъявляются следующие требования.

Однозначность соответствия между термином и понятием. Термин и называемое им понятие в пределах рассматриваемой терминосистемы должны однозначно соотноситься между собой, т.е. термин должен называть только одно понятие, и, наоборот, одно понятие должно выражаться только одним термином. Омонимия (многозначность) и синонимия (определение одного понятия несколькими терминами — синонимами) в терминосистемах недопустимы.

Соответствие значения термина выражаемому понятию. Буквальное значение термина (т.е. значение входящих в его состав терминоэлементов) должно соответствовать называемому им понятию.

Системность. Термин по возможности должен отражать отношения называемого понятия со связанными понятиями.

Краткость. Термин должен иметь оптимальную длину. Недопустимо использование длинных и громоздких терминов или использование вместо термина описания понятия.

Деривационная способность. Термин должен служить основой для образования новых терминов. Термины для новых понятий должны создаваться на базе существующих терминов [121] (2009).

термин[3] (от лат. terminus — конец, предел, окончание) — слово или словосочетание, закрепленное за определенным понятием в системе понятий.

Основное в термине — его способность строго логически обозначать предметы, явления, процессы деятельности. Многие ученые считают, что однозначность является важнейшим критерием правильно построенного термина [222] (2015).

военные термины — слова или словосочетания, однозначно обозначающие понятия военного искусства [20] (2007).

определение[1] — полное описание понятия посредством известных понятий главным образом словесными средствами.

Понятия, использованные при построении определения, должны быть выражены терминами, которые либо используются в данной терминологической системе, либо хорошо известны [166] (2008).

определение[2] — логический прием, позволяющий установить четкие границы понятия и его место в системе понятий.

Другими словами, определение — это объяснение (формулировка), раскрывающее, разъясняющее содержание, смысл чего-нибудь. Определение перечисляет наиболее существенные отличительные признаки объектов, явлений и процессов, раскрывает их свойства, взаимосвязи и отношения.

Исходя из принципа системности можно сказать, что всякая сложная терминосистема состоит из ряда подсистем и сама может являться частью терминосистемы большего масштаба. При этом необходимо отметить, что определения основных терминов родственных тер-

миносистем должны быть взаимосвязаны с определениями терминов более сложных, равных или низших терминосистем. Определения научных понятий высшего уровня должны даваться с помощью терминов низшего уровня.

К определению предъявляются следующие требования.

Соразмерность определения. Определение не должно быть слишком длинным или коротким. Признаки, фиксируемые в определении, должны быть присущи только объектам, относящимся к описываемому понятию.

Включение в определение только существенных признаков. Определение должно содержать только существенные признаки понятия. Признаки, указываемые в определении, должны не только четко разграничивать данное понятие от смежных, но и отражать его общность с другими понятиями системы.

Системность определения. Определение должно отражать место данного понятия в системе, в которой оно находится, указывать на тип отношений с ближайшими понятиями.

Недопустимость «порочного круга». То есть одно понятие не должно определяться с помощью другого понятия, которое в свою очередь определяется через первое.

Недопустимость тавтологии. Тавтологичным считается такое определение, которое является развернутым повторением термина. Если в самом термине содержатся необходимые и достаточные признаки понятия, определение приводить не следует.

Недопустимость отрицательного определения для положительного понятия. То есть определение положительного понятия не должно даваться в отрицательной форме.

Однозначность понимания определения. Понятие, используемое в определении, должно быть выражено определенными в данной системе или хорошо известными и однозначно понимаемыми терминами. Давая определение, следует стремиться к тому, чтобы все слова в нем были правильно поняты.

Непротиворечивость другим терминосистемам. Термины, входящие в данное определение, должны использоваться в том же значении, в каком они зафиксированы в родственных терминосистемах.

При разработке определений соподчиненных видовых понятий или определений, выделенных по одному основанию деления в качестве видового отличительного признака, в определениях следует указывать один и тот же признак (или сочетание признаков). Определения

однотипных понятий должны быть однотипны по структуре и лексике дефиниции.

Оптимальная краткость определения. В определении не должно быть избыточной информации, оно должно состоять из одного предложения. Недопустимы выражения в скобках, перечисления понятий, относящихся к определяемому понятию, сокращения типа «и т.п.», «и т.д.», «и пр.».

Лингвистическая правильность определения. Определение должно соответствовать правилам и нормам языка. Правильно построенное определение должно однозначно характеризовать понятие.

Помимо **краткого определения** научного понятия, приводимого в стандартах, в различных научных трудах (монографиях, учебниках, учебных пособиях, энциклопедиях, энциклопедических словарях, в словарях терминов и т.п.), часто для более полного толкования и понимания смысла описываемого понятия приводится его **расширенное описание**. В таких описаниях перечисляются наиболее существенные отличительные признаки объектов, явлений и процессов, раскрываются их свойства, взаимосвязи и отношения, приводится классификация объектов или их элементов, даются различные иллюстративные материалы. Это позволяет составить наиболее полное представление о научном понятии. Такие описания также целесообразно делать исходя из требований к терминам и определениям, изложенным выше [121] (2009).

определение понятия — логическая операция, в процессе которой раскрывается его содержание.

А это означает, что нужно найти предел (границу), отделяющий предметы, охватываемые данным понятием, от сходных с ними предметов, указать отличительные существенные признаки предметов, отображенных в данном понятии.

Различают экстенсиональное и интенсиональное определения понятий. Экстенсиональное определение задает класс объектов, которые входят в содержание понятия, их перечислением. Интенсиональное определение задает значение термина описанием свойств, указанием признаков объектов, входящих в его содержание.

Например, использующиеся в настоящее время определения «военной организации государства», включая и приведенное в Военной доктрине Российской Федерации, являются экстенциональными и несут в себе все недостатки, присущие данному типу определений. В

первую очередь это касается их громоздкости (поскольку требуется перечислять все компоненты военной организации) и необходимости постоянной корректировки при изменении содержания данного понятия [23] (2006).

определение понятий военного искусства — при выработке определений следует исходить из того, что понятие является функцией одного или нескольких переменных, и его определение должно соответствовать некоторым правилам формальной логики: выделять существенные признаки, которые необходимы и достаточны для идентификации и вычленения понятия из многих других; учитывать соразмерность и отвечать масштабу рассматриваемого явления, события или процесса; исключать недопустимость логического круга (тавтологии); быть кратким, точным и ясным.

При определении понятий следует также руководствоваться правилами лингвистики (лексикологии, грамматики, семасиологии), что позволяет верно подобрать словарный состав и правильно применить его при построении определений. Правильный подбор слов означает выбор таких, толкование которых дает возможность применить их в военной лексике и грамматически точно использовать при формулировании понятий. Именно соблюдение правил лингвистики во многом определяет доступность понимания и возможность проникновения в глубинную суть явления (процесса, события) вооруженной борьбы [20] (2007).

автоматизация терминосистемы — современный научно-методический аппарат военно-научных исследований, безусловно, должен ориентироваться на новейшие информационные технологии, и успешное решение задач, например, автоматизации управления войсками (силами) невозможно обеспечить без автоматизированного совершенствования инструментария военно-научных исследований, в частности языка военной науки, ее терминосистемы.

Этот процесс целесообразно разделить (условно) на несколько этапов.

Первым этапом является сбор всех терминов и определений, используемых в выбранной предметной области. Помимо этого, отбираются и другие сведения (описания, характеристики, классификации, иллюстративные материалы), имеющиеся в различных источниках. Это, пожалуй, самый трудоемкий этап работы. О некоторых порой

весьма важных источниках разработчики терминологии могут просто не догадываться.

Следует отметить, что уже на этом этапе необходимо широкое использование средств автоматизации с целью формирования и использования формализованного (электронного) вида упомянутой информации. Это позволит впоследствии перейти от устаревшей «ручной» методики информационного обследования к автоматизированной авторской формализации знаний.

Вторым этапом работы является систематизация отобранных понятий, которая должна установить:

— полноту описания выбранной области знаний (предметной области);

— взаимосвязь выбранной терминосистемы с другими родственными терминосистемами высшего, равного и низшего порядков;

— место каждого понятия в системе, его взаимосвязь с другими понятиями;

— недостатки существующей терминологии (синонимию, многозначность, отсутствие общепринятого термина для понятия, различные толкования одного и того же понятия и т.п.).

При систематизации понятий выделяют такие наиболее общие понятия, как категорию предметов, категорию процессов и категорию свойств. В результате систематизации выявляется система понятий.

Наиболее показательным, наглядным способом систематизации является классификация понятий по всем возможным основаниям деления, позволяющим характеризовать группы понятий или отдельные понятия в рамках заданной области знания.

В результате сбора и выявления связей в системе понятий составляется *систематизированный словник*.

Третьим этапом в совершенствовании терминосистемы является всесторонний анализ систематизированных терминов и определений исходя из общих предъявляемых к ним требований. При этом необходимо помнить о том, что название (термин) и содержание (определение) должны всегда соответствовать друг другу. Пожалуй, это самый сложный этап работы, требующий определенных знаний и умений от исполнителей.

Завершающим этапом в совершенствовании терминосистемы является выбор из существующих и уточнение или выработка новых терминов и их определений на основе вышеперечисленных требований к ним [121] (2009).

систематизированный словник — основа для анализа, оценки и построения определений и выбора терминов с целью определения границы каждого понятия и, соответственно, места термина в терминосистеме [121] (2009).

требования к терминосистеме — при выборе терминов в совершенствуемой или вновь разрабатываемой терминосистеме предпочтение целесообразно отдавать устоявшимся терминам, длительное время используемым для определения понятий в выбранной предметной области. Заменять существующие термины на новые следует только тогда, когда они входят в явное противоречие с определениями описываемых понятий. Вновь разрабатываемые термины и их аббревиатурные сокращения должны быть благозвучны и хорошо запоминаться.

Вся работа по совершенствованию существующей или созданию новой терминосистемы должна проводиться по принципу «от общего к частному». После систематизации существующих понятий необходимо представить всю систему в целом, определив ее основные элементы и связи между ними. Недопустима разработка частных понятий или новых элементов терминосистемы без учета системных требований, их связи с другими элементами. Также недопустима разработка терминосистемы низшего уровня без разработки основных положений терминосистемы высшего уровня.

Совершенствование существующей или создание новой терминосистемы требует определенных знаний в области построения систем, логики, лингвистики и, естественно, в описываемой предметной области и представляет собой достаточно трудную научно-практическую задачу.

При этом возникает необходимость в проведении экспертизы не только новых терминов и их определений, но терминосистемы в целом. Важной вехой на пути эффективного решения этой задачи может стать создание автоматизированной системы терминологической экспертизы на основе базового электронного словаря военных терминов и определений [121] (2009).

1.3.2.2.2. Энциклопедические словари

Российская Военная Энциклопедия — систематизированный свод военных и военно-исторических знаний.

Являясь универсальным научно-справочным изданием, она дает единое научное толкование научных терминов (понятий), способствует распространению военных знаний и опыта, достижению единства взглядов на основе военной теории, популяризации российской военной истории и боевых традиций, предоставляет необходимую информацию об отечественном и зарубежном вооружении и военной технике.

Энциклопедия содержит объективную научно-справочную информацию об отечественном и зарубежном военном деле с древнейших времен до наших дней. В ней имеются обширные сведения, отражающие многовековой опыт строительства и боевого применения вооруженных сил, историю войн и военного искусства, оружия и военной техники, развития военной науки. Особое место занимают материалы о видах, формах и способах военных действий стратегического, оперативного и тактического масштаба, рассматриваются все составляющие оперативного (боевого), технического и тылового обеспечения, освещаются вопросы управления войсками (силами) и боевыми средствами. В энциклопедии дается информация по военной экономике и политике, военному праву, военной педагогике и психологии, военной медицине, военной географии, военной кибернетике и другим наукам [215] (2000).

военная энциклопедия — единый источник при подготовке боевых уставов, наставлений и руководств, который безусловно, может отставать от практики войск, но в любом случае должен служить лексической основой текстуального оформления указанных документов [103] (2014).

1.3.2.2.3. Словари других типов

тезаурус — в широком смысле — совокупность знаний, накопленных человечеством в той или иной области деятельности; в узком смысле — словарь (толковый или тематический), являющийся лексическим инструментом информационно-поисковых систем.

Любой тезаурус может быть создан только в том случае, если в его основу положены строгие определения тех понятий и терминов, которые составляют его сущность. Интуитивный, экспертный подход к определению понятий и терминов военно-технической области знаний обусловливает понятийную и терминологическую путаницу, суще-

ствующую во многих отечественных и зарубежных классификациях оружия и военной техники конца XX века [131] (2003).

1.3.3. Научно-техническая информация

сайт Министерства обороны Российской Федерации — с несовершенством технологий доступа к информационным ресурсам должностные лица сталкиваются каждодневно. Наглядным примером тому служит сопоставление возможностей сайта Министерства обороны Российской Федерации mil.ru и единого информационного web-портала министерства обороны и сухопутных войск США AKO/DKO.

Сайт Министерства обороны Российской Федерации построен как сайт социальной сети и дает возможность гражданам России иметь информацию о повседневной деятельности Вооруженных Сил в основном социального характера.

Единый информационный web-портал министерства обороны и сухопутных войск США AKO/DKO обеспечивает доступ в интерактивном режиме к информационным ресурсам и сервисам межвидового информационного обслуживания абонентов различных сетей связи, подключенных к вычислительным центрам министерства обороны [120] (2011).

1.3.3.1. Проблемно-ориентированная обработка нормативно-технической информации

нормативно-техническая информация — совокупность норм (правил, требований, показателей, характеристик и регламентов), установленных в нормативных документах по стандартизации (государственных и отраслевых стандартах. руководящих документах по стандартизации, руководящих документах главных конструкторов предприятий, документации на АС, методиках, методических указаниях, инструкциях, положениях и т.д.), применяемых в процессе создания АС ВН на всех этапах ее жизненного цикла [65] (2004).

модель нормативно-технического обеспечения жизненного цикла автоматизированных систем — модель, позволяющая систематизировать содержание нормативной базы и «собрать воедино» все требования, относящиеся к какому-либо этапу жизненного цикла, виду обеспечения или классу (объекту) стандартизации.

Она предполагает следующие этапы обработки нормативно-технической информации: подготовительный, этап накопления информационного фонда и этап применения фонда в практической деятельности пользователей [65] (2004).

смысловые элементы (нормы) нормативно-технического документа — на подготовительном этапе осуществляется формирование (уточнение) признакового пространства модели, предварительная классификация представительной выборки документов, формирование обучающих текстовых массивов для каждого признака. В качестве тематических классов при классификации выступают значения характеристик (признаки) модели нормативно-технического обеспечения жизненного цикла АС. На этом же этапе формируется словарь терминов по текстам представительной выборки документов, производится индексирование документов и создается тематический словарь понятий, отражающий отношения смысловой принадлежности понятий к некоторой группе классификационных признаков и используемый на последующих этапах при классификации текстов. Выполнение этих операций основывается на применении базовых процедур прикладной лингвистики, позволяющих производить семантико-синтаксический анализ текстов: морфологический анализ, нормализацию слов, выделение именных словосочетаний из текстов, нормализацию именных словосочетаний, построение поисковых образов словосочетаний и др. Определяющими показателями при выборе этих процедур может служить универсальность и эффективность алгоритмов для различных предметных областей [65] (2004).

нормативно-технический фонд (НТФ) — на следующем этапе осуществляется наполнение информационного фонда. При этом производится выделение требований в текстах вводимых документов и их автоматизированная классификация при участии специалиста по стандартизации в области автоматизированных систем. В прикладной лингвистике задача классификации текстов на естественном языке состоит в их распределении по тематическим группам (классам) на основе признаков сходства и различия, отражающих наиболее существенные черты смыслового содержания этих текстов. Принадлежность ка-

кого-либо текста к той или иной тематической группе может быть определена путем лексического анализа и последующего сравнения их частотных характеристик (например, количество повторов появления лексических единиц в тексте). При классификации небольших текстов в условиях значительного числа заданных тематических групп анализ текстовой информации целесообразно осуществлять не на уровне отдельных слов, а на уровне наименований понятий, представленных в текстах именными словосочетаниями [65] (2004).

применение нормативно-технического фонда — на заключительном этапе осуществляется проблемно-ориентированный поиск требований по их классификационным признакам и наглядное представление результатов пользователю [65] (2004).

1.3.4. Информация в автоматизированных системах военного назначения

фактографическая база данных (ФБД) — база данных, предназначенная для хранения сведений, подлежащих автоматической обработке при решении информационных и расчетных оперативно-тактических задач.

Разработка всего комплекта боевых документов (как текстовых, так и графических) должна вестись на основе фактографической информации с необходимой степенью ее формализации [153] (2009).

метаданные — структурированные данные, характеризующие информационный ресурс для целей его идентификации, поиска и управления им[7].

Таким образом, преобразование информации в информационный ресурс осуществляется путем формирования метаданных (метаописания) информационного ресурса. Дальнейшая интеграция информационных ресурсов осуществляется с использованием метаданных [17] (2013).

[7] ГОСТ Р 7.0.10—2010 (ИСО 15836:2003).

онтология — система, состоящая из набора понятий и набора утверждений об этих понятиях, на основе которых можно строить классы, объекты, отношения, функции и теории [17] (2013).

1.3.5. Служба информационных ресурсов ВС РФ

служба информационных ресурсов Вооруженных Сил — служба, которая должна обеспечить централизованное руководство процессами создания, ведения и развития единой информационной среды.

До настоящего времени в Вооруженных Силах не создано целостной структуры руководства информационными ресурсами на всех уровнях управления. Так, для обеспечения использования информационных ресурсов в Генеральном штабе имеется Главный вычислительный центр, однако в военных округах и общевойсковых армиях эти задачи решать на повседневных пунктах управления некому, так как центры АСУ ликвидированы. В полевой составляющей все наоборот: в военных округах и общевойсковых армиях в составе бригад управления созданы центры автоматизированных пунктов управления, а в Генеральном штабе в составе полевого узла связи Генерального штаба такое подразделение отсутствует.

Структурными элементами службы информационных ресурсов Вооруженных Сил должны стать информационные органы и подразделения при штабах всех звеньев управления [120] (2011).

служба информационных ресурсов Вооруженных Сил Российской Федерации — основными целями ее[8] создания являются:

обеспечение методологического и организационного единства в области информационной поддержки процессов управления Вооруженными Силами РФ;

создание условий для повышения качества информационного взаимодействия автоматизированных систем военного назначения;

формирование основ единого терминологического, понятийного и кодового аппарата в ВС РФ;

обеспечение основ создания Единого информационного пространства (ЕИП) ВС РФ [31] (2006).

[8] О службе информационных ресурсов Вооруженных Сил Российской Федерации. Введено в действие приказом Министра обороны № 260 от 22.07.2006 г.

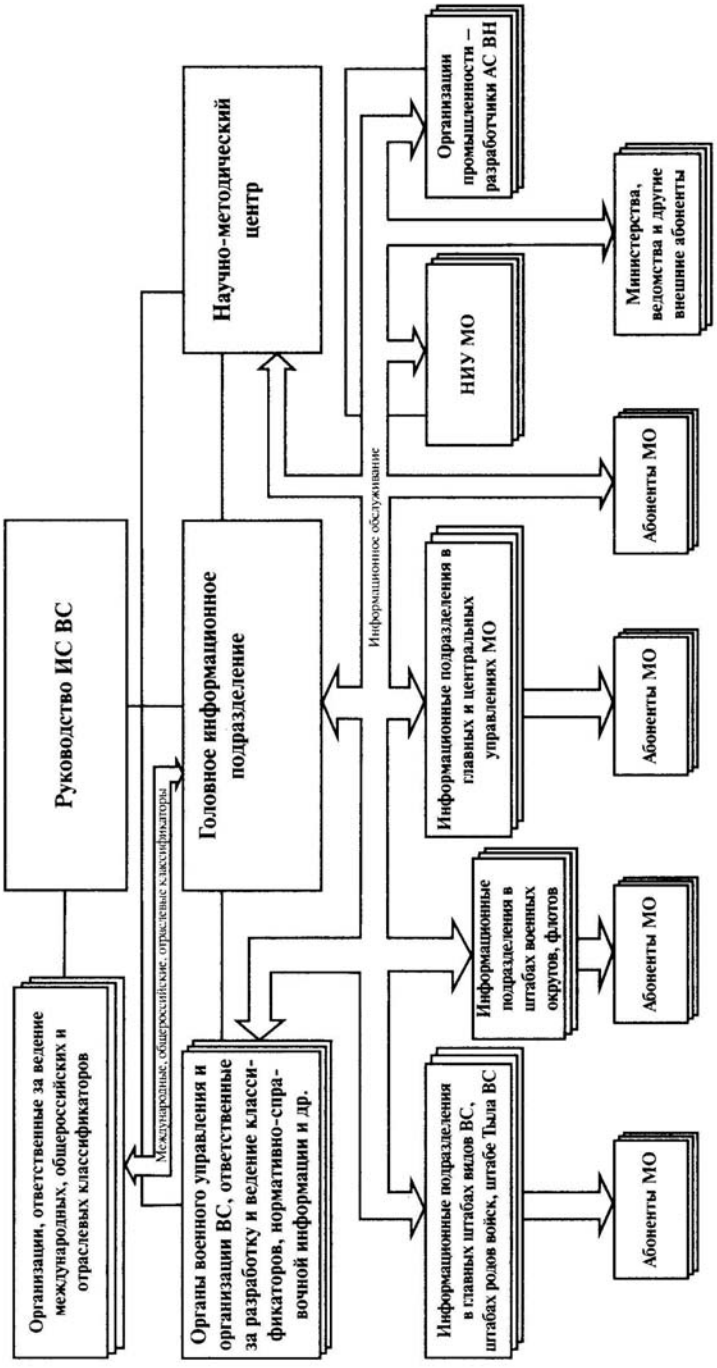
служба информационных ресурсов ВС РФ — ее создание осуществилось в 2006 году. Информационное обеспечение АСУ войсками (силами) включает в свой состав оперативную информацию и условно-постоянную информацию. Целью службы информационных ресурсов ВС РФ являлось создание условий для своевременного централизованного обеспечения органов военного управления, воинских частей ВС РФ и организаций промышленности условно-постоянной информацией из информационного фонда ВС РФ.

В 2011 году приказом министра обороны Российской Федерации выполнение функций организации, осуществляющей ведение информационного фонда ВС РФ, возложено на ФГУП «ЦНИИ ЭИСУ». В настоящее время ряд автоматизированных систем военного назначения поставлены на снабжение из информационного фонда ВС РФ в части получения контрольных экземпляров отдельных категорий информационных ресурсов, изменений к ним, извещений об их изменении, а также соответствующих сопроводительных документов. Исходные данные для актуализации информационного фонда ВС РФ регулярно поступают из соответствующих федеральных органов исполнительной власти и органов военного управления, определенных ответственными за их ведение [17] (2013).

1.3.5.1. Организационные вопросы создания информационной службы ВС РФ

информационная служба ВС РФ — служба, осуществляющая функции общей координации работ в области информационной поддержки процессов управления, а также функции централизованного обеспечения органов военного управления и автоматизированных систем военного назначения отдельными категориями информационных ресурсов ВС РФ [16] (2004).

информационная служба Вооруженных Сил (ИС ВС) — совокупность взаимодействующих органов (подразделений), осуществляющих координацию работ в области информационной поддержки процессов управления, а также функции своевременного и достоверного централизованного обеспечения ОВУ и АС ВН отдельными категориями информационных ресурсов (рис. на с. 57).



Организационная структура информационной службы ВС РФ (вариант)

На начальных этапах создания ИС ВС предлагается отработать порядок ее функционирования на примере ведения классификаторов, НСИ и УФД. Это обусловлено их достаточной стабильностью во времени, сравнительно небольшими объемами и четко упорядоченными потоками распространения, а также их использованием для формализации, систематизации, упорядочения и унификации информационных ресурсов.

Основными целями создания такой системы, по мнению авторов, являются: обеспечение методологического и организационного единства работ в области информационной поддержки процессов управления в ВС; создание условий для обеспечения информационной совместимости АС ВН; формирование основ единого терминологического и кодового аппарата в ВС и единого информационного пространства ВС.

Можно определить следующие главные задачи ИС ВС: координация работ в области информационной поддержки процессов управления; создание и ведение информационного фонда, содержащего классификаторы, НСИ и УФД; централизованное обеспечение ОВУ, организаций и учреждений ВС необходимой информацией; установление единого перечня терминов и понятий, используемых в деятельности ОВУ, а также организаций и учреждений ВС [10] (2003).

головное информационное подразделение — основными его функциями являются поддержание информационного фонда в актуальном состоянии и информационное обслуживание нижестоящих подразделений ИС ВС и своих абонентов. Кроме того, оно взаимодействует с организациями, осуществляющими ведение общероссийских классификаторов, а также с ОВУ, осуществляющими разработку и ведение классификаторов военной информации и НСИ [10] (2003).

информационные подразделения в органах военного управления — группы должностных лиц в рамках существующих подразделений автоматизации. Они получают копии фрагментов информационного фонда, осуществляют ведение этих копий и своевременное обеспечение своих абонентов актуальной информацией из фонда [10] (2003).

научно-методический центр — может быть создан на базе одного из научно-исследовательских учреждений МО. В рамках, возложенных на него функций, он проводит исследования по основным направлениям работ, связанным с совершенствованием информацион-

ной поддержки процессов управления в ВС, в том числе по разработке единой методологии проектирования информационного обеспечения АС ВН, а также осуществляет проведение экспертиз проектов классификаторов военной информации и системных классификаторов, НСИ и УФД для определения возможности их включения в состав информационного фонда [10] (2003).

абоненты информационной службы Вооруженных Сил — органы управления, организации и автоматизированные системы, использующие информацию из фонда.

Они могут быть внутренними и внешними. К внутренним абонентам относятся ОВУ, организации ВС и АС ВН. К внешним — органы управления и учреждения, не входящие в Министерство обороны, а также организации промышленности — разработчики АС ВН и др. Все абоненты регистрируются соответствующими подразделениями ведения информационного фонда, к которым они прикреплены. Информационное обслуживание абонентов осуществляется в соответствии с их информационными потребностями и уровнем полномочий. В этих рамках абонентам предоставляется перечень классификаторов, НСИ и УФД, входящих в фонд, и осуществляется снабжение контрольными экземплярами этих категорий информации в соответствии с установленным регламентом. Кроме того, предусматривается оказание консультативной помощи абонентам по вопросам, связанным с получением и использованием информации из фонда [10] (2003).

информационный фонд — совокупность взаимоувязанных классификаторов различных категорий, а также НСИ и УФД, используемых в деятельности ОВУ, организаций ВС и в АС ВН.

Создание информационного фонда является довольно трудоемким процессом, включающим детальный анализ информационных потребностей ОВУ, объединение всех необходимых классификаторов, НСИ и УФД, их систематизацию, упорядочение и унификацию форматов представления и хранения. Для решения этой проблемы необходимо проведение углубленных исследований и разработка специализированных программных средств.

Ведение информационного фонда заключается в постоянном поддержании в актуальном состоянии входящих в него классификаторов, НСИ и УФД. Данный процесс должен осуществляться централизованно головным информационным подразделением, а также информационными подразделениями в главных штабах видов ВС, штабах

родов войск и специальных войск, штабе Тыла ВС РФ, главных и центральных управлениях МО РФ и штабах военных округов. При этом должен быть четко определен порядок получения копий классификаторов, НСИ и УФД от ОВУ, ответственных за их разработку. При обслуживании нижестоящих подразделений головное подразделение обязано снабжать их фрагментами информационного фонда (в части касающейся), программными средствами ведения этого фонда и нормативно-методическими документами [10] (2003).

1.3.5.2. Служба информационных ресурсов в видах и родах войск

информационная служба (служба информационно-лингвистического обеспечения) — служба, которую необходимо создать в РВиА в целях эффективного проектирования и реализации информационного обмена.

На службу могут быть возложены следующие функции:

— разработка предложений по перечню, формам представления и содержанию документов (сообщений), подлежащих реализации в АСУ РВиА; по составу, структуре и содержанию классификаторов и словарей оперативно-тактической и военно-технической информации; по структуре и содержанию информационного обмена;

— учет протоколов организационной, информационной и технической совместимости между объектами АСУ РВиА и степени их согласования;

— контроль за реализацией информационного обмена в создаваемых КСА и определение возможности их сопряжения с существующими комплексами [114] (2004).

1.4. Единое информационное пространство

пространство — форма сосуществования материальных объектов и процессов (характеризует структурность и протяженность материальных систем)[9].

Также понятие «пространство» трактуется как множество объектов, между которыми установлены отношения, сходные по своей

[9] Большой энциклопедический словарь, Т. 2. С. 212.

структуре с обычными пространственными отношениями. По сути, пространство есть порядок расположения одновременно сосуществующих объектов применительно к какой-либо сфере [8] (2011).

информационное пространство[1] — термин стал привычным в контексте эксплуатации систем обеспечения радиолокационной информацией и расширения телекоммуникационных сетей. Научного же определения упомянутого понятия в рамках информатики до сих пор не появилось. Однако заметные даже на бытовом уровне признаки интеграции программно-аппаратных средств в единый многофункциональный комплекс, опирающийся на глобальную интеллектуализированную информационную систему, дают основание рассматривать информационное пространство как одну из наиболее перспективных и важных для теоретического осмысления категорий эпохи информационной цивилизации [24] (1999).

информационное пространство[2] — сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию[10] [13] (2012).

информационное пространство[3] — пространство (гиперплоскость), в пределах которого обеспечивается сбор, формирование, распространение и использование информации в интересах соответствующих пользователей (логических объектов информационного взаимодействия).

Основными координатами этого пространства (гиперплоскости) являются координаты адресов, сообщений, данных и знаний. Следует подчеркнуть, что информационное пространство принадлежит определенной сфере деятельности и формируется при создании информационной инфраструктуры [53] (2012).

информационное пространство[4] — представление всей информации, циркулирующей в системе управления.

В качестве системы координат этого пространства предлагается использовать набор характеристик в терминах Общероссийского клас-

[10] Приложение № 1 к «Соглашению между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области международной информационной безопасности», Екатеринбург, 2008.

сификатора технико-экономических и социальных показателей, определяющих время, место действия, вид операции и другие параметры. Это позволит создать единую систему классификации и кодирования информации, унифицировать форматы ее хранения и представления, для чего разрабатывается унифицированная система документации [11] (1996).

информационное пространство[5] — некий объем информации (информационных ресурсов, а проще говоря, сведений), одинаково доступный для всех заинтересованных лиц, органов и структур.

В более общем виде — это база данных, т.е. сведений, причем существующих в различных форматах (в мыслительной деятельности человека, на бумажных, электронных и иных носителях) и используемых в своей совокупности при решении определенных задач.

Однако сегодня не вызывает сомнения, что сама база данных при всей ее ценности не способна повысить эффективность управления и в конечном счете поражения противника, а напротив, избыток информации (что уже стало очевидным) может привести к ее существенному снижению.

В этой связи следует обратить внимание на то, что создаваемое информационное пространство должно представлять собой весьма широкое, по сути, явление и включать не только собственно информацию (сведения) об обстановке, но и весь методологический, а главное — программно-математический аппарат, реализованный на новой технологической (компьютерной) базе и позволяющий в реальном масштабе времени осуществлять всю совокупность необходимых информационных процессов, причем не вообще, а в интересах достижения вполне определенных целей. В рассматриваемом контексте такими целями являются максимально быстрое принятие решений и их практическая реализация. Достичь их возможно только при таком управлении, которое обеспечит максимально быстрое определение способов наиболее эффективного поражения противника и успешную реализацию войсками этих способов.

Однако создания на практике такого информационного пространства, очевидно, мало для того, чтобы рассчитывать на качественный скачок в области управления войсками в целях существенного повышения эффективности их действий (прежде всего в интересах максимально эффективного поражения противника), поскольку наличие информации вообще — это один вопрос, а обеспечение ее доступности

для определенного круга должностных лиц, органов и структур — совершенно другой. Обеспечить доступность и реальное единство информационного пространства можно только при наличии соответствующих коммуникаций, способных существенно изменить характер управленческой деятельности.

Поэтому логичнее говорить о едином информационно-коммуникационном пространстве [165] (2012).

информационное пространство[6] — совокупность объектов (систем), осуществляющих разведку, наблюдение, сбор данных и обмен ими, принятие и реализацию решений.

Считается что, будучи достаточно обособленным, оно одновременно является частью наземного, морского, воздушного и космического пространства.

Американские специалисты условно делят информационное пространство на три взаимосвязанных сегмента. В состав первого — **физического** — включены информационные системы, обеспечивающие проведение военных операции на суше, на море, в воздухе и в космосе. К ним относятся системы управления, вооружение и военная техника, объекты инфраструктуры, а также население, находящееся в зоне военных действий. Во второй — **информационный** — входит различная информация, как зафиксированная в форме боевых документов, так и циркулирующая в системах управления в форме сигналов. Третий — **когнитивный** — это органы управления (должностные лица), вырабатывающие и принимающие решения, а также личный состав, выполняющий их. Отмечается, что современные информационные операции проводятся в основном в отношении именно этих объектов. Причем на процесс выработки и принятия решения определяющее влияние оказывают такие информационно-психологические факторы, как моральный дух войск, их сплоченность, уровень подготовки, опыт, личностные мотивации, осведомленность об обстановке органов управления и исполнителей, а также состояние общественного мнения и то, какая информация может его изменять в нужном направлении.

По мнению американских военных специалистов, информационное пространство динамично изменяется во времени под влиянием взаимосвязанных долгосрочных, среднесрочных и краткосрочных факторов.

К **долгосрочным факторам** относятся: особенности общественно-экономического строя государств, входящих в ареал информацион-

ного пространства; система их государственного и военного управления; культурные, общественные, этнические, религиозные устои, а также социально-политическое, экономическое состояние стран и уровень их технологического развития.

Среднесрочные факторы могут включать возможности правящих кругов и конкурирующих политико-формирующих групп по использованию информационной инфраструктуры и информационных ресурсов противоборствующих сторон.

Краткосрочные факторы, оказывающие влияние на формирование информационного пространства, — это возможности сторон по использованию информационных технологий и информационной инфраструктуры непосредственно в зоне проведения информационной операции [113] (2008).

информационное пространство[7] — пространство формализованных знаний, в котором через систему сообщений обеспечивается коммуникация составляющих суть этих знаний сведений между субъектами (индивидуумами и коллективами) предметного (физического) пространства [52] (2014).

интеллектуальное пространство — запечатленная в сознании человека картина окружающей действительности, а также представление о способах и средствах сознательных действий по вектору улучшения качества жизни.

Иначе говоря, интеллектуальное пространство — это пространство мыслей, знаний, вместилищем которых является мозг человека [52] (2014).

физическое пространство — окружающий человека мир, в котором человек устраивает свой быт, активно взаимодействуя с окружающей материальной и социальной средой в целях обеспечения соответствующего качества своей жизни [52] (2014).

информационное пространство ВС РФ — вся совокупность информации, используемой в ВС РФ.

Ее источниками являются: руководящие и нормативно-методические документы; оперативные сводки, донесения, распоряжения; документы первичного учета; результаты решения задач в автоматизированных системах военного назначения; базы данных, базы знаний автоматизированных систем военного назначения; нормативно-справоч-

ная информация, классификаторы; результаты научных исследований; архивы; документы, поступающие из внешних источников, и др. [15] (2003).

единое информационное пространство[1] — упорядоченная и взаимосвязанная совокупность информационных, вычислительных и телекоммуникационных ресурсов, организованных и функционирующих во времени и пространстве в интересах единого информационного обеспечения задач управления подразделениями общевойсковых формирований тактического звена [49] (2014).

единое информационное пространство[2] (ЕИП) — часть информационного пространства, в пределах которого реализованы единые правила доступа к информационным ресурсам пользователей из определенного множества различных инфосфер [53] (2012).

единое информационное пространство[3] — совокупность информации о противнике, своих войсках и условиях ведения боевых действий, получаемой автономными командно-штабными и боевыми модулями и характеризующейся согласованностью по составу, объему и срокам доведения [180] (2005).

единое информационное пространство[4] — взаимосвязанный комплекс средств и способов общения и отображения реальности в видах деятельности в новой технологической среде.

При этом подразумевается использование общепринятых систем формирования и применения информационных ресурсов, языков общения, технологий доступа, обмена и переработки информации, коммуникаций, а также единых структур информационных ресурсов, банков данных и знаний, систем управления ими [24] (1999).

единое информационное пространство[5] [Net-Centric Environment] — инфраструктура для взаимодействия всех военнослужащих и совместного функционирования технических средств, позволяющая всем должностным лицам министерства обороны и других органов управления обмениваться необходимой для них секретной информацией в понимаемой форме, а также обеспечивающая защиту информации от несанкционированного доступа[11].

[11] Net-Centric Environment Joint Functional Concept // DOD, 2005. Appendix B. Glossary.

Оно является основой для ведения сетецентрической войны. Большинство авторов переводят этот термин на русский язык именно как «единое информационное пространство», хотя дословным его переводом является «**среда, центральной частью которой является вычислительная (компьютерная) сеть**» [17] (2013).

Единое информационное пространство Вооруженных Сил Российской Федерации[1] (ЕИП ВС РФ) — совокупность информационных ресурсов ВС РФ, упорядоченная по единым принципам и правилам формирования, формализации, хранения и распространения[12].

ЕИП ВС РФ было призвано не заменить существующие автоматизированные системы военного назначения, а обеспечить интеграцию информационных ресурсов, распределенных по различным автоматизированным системам и комплексам средств автоматизации.

В последние десятилетия информационные ресурсы по своей ценности поставлены в один ряд с другими ресурсами: сырьевыми, людскими, финансовыми. Качество и актуальность информационных ресурсов влияет практически на все области деятельности, являясь ключевыми факторами для принятия решений.

Предназначением ЕИП ВС РФ является наиболее полное удовлетворение информационных потребностей должностных лиц органов военного управления. Это может быть достигнуто путем концентрации и интеграции актуальной, полной, достоверной и сформированной по определенным правилам информации, а также обеспечения возможности ее своевременного предоставления в соответствии с установленным порядком доступа.

Одним из результатов создания ЕИП ВС РФ должна была стать унификация информационного обеспечения и реализуемая в нем часть лингвистического обеспечения разрабатываемых и модернизируемых АСУ войсками и оружием [17] (2013).

Единое информационное пространство ВС РФ[1] (ЕИП ВС РФ) — в широком смысле его можно представить как специальным образом упорядоченную совокупность всей информации, а в узком — как совокупность взаимосвязанных информационных ресурсов ВС РФ с

[12] Концепция Единого информационного пространства Вооруженных Сил Российской Федерации. Утверждена начальником Генерального штаба ВС РФ 16 декабря 2004 г.

общими правилами их формирования, унификации, хранения, распространения и использования.

Основным предназначением ЕИП ВС РФ является наиболее полное удовлетворение информационных потребностей должностных лиц ОВУ в целях повышения оперативности, обоснованности и качества принимаемых решений в различных областях военной деятельности. Это может быть достигнуто путем концентрации актуальной, достоверной, своевременной и всесторонней информации, необходимой ОВУ для решения задач управления.

Сложность создания ЕИП обусловлена наличием большого количества источников информации, их разнородностью и территориальной распределенностью. Кроме того, для системы управления ВС характерны непрерывное расширение и усложнение решаемых задач, увеличение информационных потребностей, постоянное изменение числа источников и потребителей информации, большое количество неформализованной информации и т.д.

Из-за сложности ЕИП его необходимо рассматривать с различных точек зрения: с оперативной — как совокупность информации, используемой в ВС и распределенной по ОВУ, пунктам управления и АС ВН; с технологической — как сочетание хранилищ информации, средств их ведения и использования, телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам и обеспечивающих информационное взаимодействие органов военного управления, а также удовлетворение информационных потребностей должностных лиц этих органов; с организационной — как совокупность структурных подразделений (должностных лиц), осуществляющих наполнение и ведение хранилищ информации, а также администрирование информационных ресурсов; с информационной — как совокупность взаимоувязанных информационных объектов, обеспечивающих реализацию информационных процессов в системе управления ВС РФ, с общими правилами их описания, формализации, унификации, хранения и использования [15] (2003).

Единое информационное пространство ВС РФ[2] (ЕИП ВС РФ) — специальным образом упорядоченная совокупность информационных ресурсов ВС с общими правилами их формирования, формализации, хранения и распространения.

Основной целью создания ЕИП ВС РФ является повышение эффективности управления Вооруженными Силами за счет совершен-

ствования информационной поддержки процессов управления. Основным предназначением единого информационного пространства ВС РФ является наиболее полное удовлетворение в реальном масштабе времени информационных потребностей должностных лиц ОВУ [16] (2004).

Единое информационное пространство Вооруженных Сил Российской Федерации[2] (ЕИП ВС РФ) — главным его предназначением является удовлетворение в реальном масштабе времени информационных потребностей органов военного управления (ОВУ). Эту задачу предполагается решать путем концентрации и интеграции актуальной, полной, достоверной и сформированной по определенным правилам информации, а также обеспечения возможности ее своевременного представления в соответствии с установленным порядком доступа.

Идеологически (методологически) создание ЕИП и внедрение информационной поддержки жизненного цикла изделий являются родственными процессами, вследствие чего должны вестись одновременно с использованием единых принципов:

принцип разделения и закрепления ответственности за развитие тех или иных видов информационных ресурсов между органами и организациями МО РФ;

принцип встраивания новых информационных ресурсов в систему информационного обмена, существующую в Министерстве обороны, либо рациональное изменение элементов и связей этой системы для обеспечения функционирования нового информационного ресурса;

принцип минимизации циркулирующей в ЕИП информации, включение в него только тех информационных ресурсов, которые нужны при принятии решений на разных уровнях военного управления;

принцип унификации и стандартизации информационных ресурсов (т.е. введение единых правил представления данных об информационных объектах, осуществления их обработки) и используемых для этого технических и программных средств [31] (2006).

единое информационное пространство Вооруженных Сил — по нашему мнению — специальным образом упорядоченная и взаимосвязанная совокупность информационных, вычислительных и телекоммуникационных ресурсов, организованных и функционирующих во времени и пространстве (в космосе, воздухе, на море и суше), с це-

лью повышения качества управления войсками (силами) и оружием в мирное и военное время.

Мировой опыт создания сетевых информационных структур показывает, что архитектура единого информационного пространства Вооруженных Сил должна обеспечивать возможность рационального сочетания централизованного и распределенного использования информации на всех уровнях управления. Кроме того, она должна обладать гибкой системой обеспечения, состоящей из организационного, программного и технического компонентов[13].

Введение нового определение обусловлено тем, что в Вооруженных Силах Российской Федерации построение единого информационного пространства регламентируется целым рядом документов, содержание которых предусматривает удовлетворение информационных потребностей органов военного управления за счет совершенствования информационной поддержки принятия решений[14]:

— создание **единого информационного пространства Вооруженных Сил Российской Федерации** как совокупности информационных ресурсов Вооруженных Сил[15];

— создание **единой системы информационно-телекоммуникационной поддержки нужд** системы обеспечения национальной безопасности[16];

— обеспечение гарантированного управления войсками (силами) и оружием в **едином информационном пространстве**[17];

— создание **единого информационного поля** Вооруженных Сил[18].

---

[13] Столь решительное толкование авторами термина единого информационного пространства представляется спорным. Подобная нотация скорее подходит для определения информационной инфраструктуры системы управления войсками (силами). — *Прим. редактора журнала «Военная мысль».*

[14] Понятийная чехарда, заложенная в концептуальных документах недопустима, ибо она заведомо готовит для единого информационного пространства участь библейской Вавилонской башни. Нельзя говорить о едином информационном пространстве, не имея единой вербальной модели инфосферы управления. — *Прим. редактора журнала «Военная мысль».*

[15] Концепция единого информационного пространства Вооруженных Сил, 2004 г.

[16] Стратегия национальной безопасности Российской Федерации до 2020 года, 2009 г.

[17] Концепция развития системы управления Вооруженных Сил до 2025 года, 2009 г.

[18] Военная доктрина Российской Федерации, 2010 г.

В этих документах содержится различное толкование сходных базовых терминов инфосферы управления войсками (силами). Это не позволяет правильно сформировать дерево целей и четко установить этапы и сроки создания единого информационного пространства [120] (2011).

1.4.1. Аспекты создания единого информационного пространства ВС РФ

проблемы создания единого информационное пространство Вооруженных Сил — объективно существующее информационное пространство Вооруженных Сил в настоящее время нельзя считать единым вследствие нерешенности ряда проблем:

1) организационного характера:

— отсутствие в концептуальных и уставных документах, регламентирующих формы и способы ведения военных действий, определения места, роли и порядка использования единого информационного пространства;

— несовершенство нормативной правовой базы, регламентирующей формирование, тиражирование и использование информации;

— отсутствие органов, обеспечивающих координацию работ по созданию, тиражированию и использованию информации (информационных ресурсов);

— недостаток квалифицированных специалистов, владеющих навыками работы с прикладными программами и эксплуатации АСУ;

2) методологического характера:

— отсутствие единства методологии построения технической основы системы управления Вооруженных Сил и ее элементов, особенно автоматизированных систем управления;

— необходимо воссоздание Института главного конструктора АСУ Вооруженных Сил, в разграничении функций и задач между органами военного управления, отвечающими за развитие системы управления Вооруженными Силами Российской Федерации, и информационных и телекоммуникационных технологий Министерства обороны Российской Федерации, научно-исследовательскими организациями, ввузами и предприятиями оборонно-промышленного комплекса (ОПК), а также в разработке и внедрении взаимосвязанной системы стандартов на основе международных и национальных стандартов;

— необходимо постоянное научное сопровождение развития компонентов единого информационного пространства Вооруженных Сил (назрела необходимость объединения НИР и начальных этапов ОКР по разработке (модернизации) элементов технической основы системы управления Вооруженными Силами);

3) технологического характера:

— существующая АСУ Вооруженных Сил имеет ярко выраженную стволовую архитектуру и не обеспечивает взаимодействия на всех уровнях управления, техническую и информационную совместимость автоматизированных систем военного назначения (в настоящее время на обеспечении войск находится почти 300 различных систем связи и АСУ военного назначения, при этом на рабочем месте операторов порой установлено по два-три компьютера из различных комплексов, поскольку системы не увязаны между собой);

— обеспечение адресности и оперативности предоставления необходимой информации;

— многие применяемые средства связи и автоматизации не обеспечивают работу по высокоскоростным цифровым каналам;

— ограниченный набор предоставляемых услуг, отсутствие единой системы защищенных каналов связи и несовершенство средств криптозащиты;

— недостаточность вычислительных ресурсов для создания, ведения и использования баз знаний в интересах поддержки управленческих решений;

— несовершенство технологий доступа к информационным ресурсам;

— АСУ различного уровня и предназначения не согласуются в полном объеме между собой по общему и специальному программному обеспечению, имеют различное информационно-лингвистическое обеспечение с разным интерфейсом, ориентированы на различные технические средства;

4) информационного характера:

— согласование классификаторов и справочников, лежащих в основе информационного обеспечения АСУ военного назначения (в системе управления развитием ВВТ используется более 400 классификаторов и справочников различного уровня, начиная с международных и всероссийских и заканчивая «внутренними» классификаторами конкретных организаций);

— несогласованность понятийно-терминологической базы;

— разная степень актуальности информационных ресурсов в различных звеньях управления не позволяет в полной мере обрабатывать информацию и распределять ее по степени важности;

— многообразие и несвязанность форм документов, циркулирующих в АСУ [120] (2011).

информационные потребности — объект информатизации.

Предметом информатизации являются методы, системы и средства, позволяющие указанные потребности удовлетворить, то есть новые технологии [24] (1999).

информационная потребность — совокупность соответствующих данных, необходимых для достижения намеченных целей каждым компонентом.

Например, на оперативном уровне информационные потребности АСУВ включают сведения, способствующие правильной оценке (прогнозированию) возможностей своих войск и войск противника, оценке (прогнозированию) условий ведения боевых действий и их влияния на выполнение поставленных задач [79] (2012).

информационные потребности органа военного управления — совокупность всех информационных ресурсов, необходимых для решения задач, поставленных перед органом военного управления [16] (2004).

информационные потребности конкретных должностных лиц — объективные нужды последних в специально организованной информации, необходимой для полноценной реализации ими своих функций в определенных условиях деятельности.

В более широком смысле информационные потребности — заявка (заказ) систем различного назначения на необходимые для их функционирования информационные ресурсы, которые могут находиться на разных технологических стадиях готовности к использованию. Применение такого подхода к информационным процессам побуждает выделять в них стадии переработки информации от информационного сырья до продукта высшего качества. Причем критерии качества информации должны быть непосредственно связаны с возможностями по ее использованию для решения конкретных задач в видах деятельности. Поэтому так важен, например, поиск и выбор форм представления пользователям результатов информационных процессов при удовле-

творении их информационных потребностей. Речь идет прежде всего о способах визуализации запрашиваемых пользователями сведений об объектах и процессах [24] (1999).

информационное положение — текущее состояние информированности соответствующих компонентов группировки войск в ходе выполнения ими поставленных (уточненных) задач [79] (2012).

информационная диспропорция — разница между информационной потребностью компонентов группировки войск для выполнения задач и их информационным положением.

Фактически она определяет степень несоответствия на текущий момент необходимых данных для достижения требуемых информационных потребностей [79] (2012).

Концепция Единого информационного пространства ВС РФ — концепция, утвержденная в 2004 году и направленная на формирование условий для построения единого информационного пространства ВС РФ посредством применения базовых информационных защищенных компьютерных технологий, системы классификации и кодирования информации, унифицированной системы документации, единых протоколов информационного взаимодействия.

В последние годы сотрудниками института при активном участии М.В. Букатова, А.В. Ширманова, В.Р. Гриня, В.А. Двойченкова, В.В. Кошкина, С.И. Тимохина, С.А. Столбова, К.Г. Безчастнова проводятся исследования по проблемам создания единого информационного пространства ВС РФ, интеграции информационных ресурсов существующих и создаваемых автоматизированных систем как совокупности информационно-расчетных подсистем автоматизированных систем и средств, обеспечивающих интеграцию их информационных ресурсов, а также унифицированное представление их должностным лицам органов военного управления [99] (2009).

проведенные работы по созданию Единого информационного пространства Вооруженных Сил Российской Федерации — концепцией были предусмотрены основные направления создания ЕИП ВС РФ, а именно: научно-исследовательское; организационное; технологическое. По этим направлениям с 2002 года было выполнено три научно-исследовательских и две опытно-конструкторских работы, в рамках которых были осуществлены следующие мероприятия:

— проведены информационные обследования органов военного управления и обработаны их результаты;

— осуществлена инвентаризация информационных ресурсов, по результатам которой составлен перечень информационных ресурсов, ведущихся службой информационных ресурсов ВС РФ;

— разработаны формальные онтологии уровня ВС РФ в интересах описания информационных ресурсов;

— составлены шаблоны описаний информационных ресурсов с контрольными примерами информационного наполнения;

— разработаны и утверждены первоочередные нормативные документы, регламентирующие разработку, ведение и использование информационных ресурсов;

— осуществлены работы по формированию информационного фонда ВС РФ в части классификаторов и нормативно-справочной информации;

— проведены работы по накоплению терминологии, используемой в ВС РФ и при разработке продукции военного назначения, и на их основе начато составление электронного словаря военных терминов в части основной терминологии;

— разработаны средства формирования, ведения, хранения, интеграции и предоставления информационных ресурсов в интересах службы информационных ресурсов ВС РФ;

— разработаны средства для системы поддержки и управления информационными ресурсами, являющейся основой для создания систем хранения данных перспективных автоматизированных систем военного назначения [17] (2013).

система обеспечения Единого информационного пространства Вооруженных Сил Российской Федерации — организационная и техническая основа для ведения и использования ЕИП ВС РФ, предоставляющая возможность осуществлять наполнение и актуализацию хранилищ информации, поиск необходимой информации, ее гарантированную защиту, доступ к информации независимо от места ее хранения и в соответствии с уровнем полномочий [17] (2013).

1.4.2. Хранилища информации

хранилища информации — автоматизированные информационные системы, позволяющие собирать сведения из распределенных

баз данных (знаний), формировать, хранить и использовать информационные ресурсы как единое целое.

В новой технологической среде информационные ресурсы содержатся в хранилищах информации. Основными компонентами таких хранилищ являются: информационное сырье (первичные сведения об объектах и процессах); правила применения накопленного опыта (нормативная база, критерии эффективности, различные классификаторы и т.п.), вычислительные ресурсы и программные средства. Поэтому если мы хотим получать информационный продукт требуемого качества, то должны выполнить по крайней мере три условия: определить систему описания видов деятельности; сформировать первичную информационно-справочную систему и внедрить ее в технологическую среду, преобразующую информационное сырье в некий продукт [24] (1999).

информационный объект — структурированная совокупность семантически связанной информации. Основой для формирования информационных объектов является информация, циркулирующая в системе управления [15] (2003).

релевантная информация — информация, существенная для решения конкретной задачи, в конкретном месте и в конкретное время [100] (2004).

1.4.3. Военные информационные пространства и поля

информационное пространство ведения военных действий — логическое завершение определенного этапа в процессе осмысления военно-политическим руководством развитых стран того факта, что на рубеже тысячелетий информационное пространство по праву заняло свою нишу наряду с сухопутным, морским, воздушным и космическим пространствами (сферами) ведения военных действий. Материальную основу информационного пространства составляют такие элементы, как информационные инфраструктуры государств, СМИ, связь, космическая навигация, компьютерные сети типа Интернета и другие [35] (2006).

единое военное информационное пространство (ЕВИП) — информационное пространство, необходимое для обеспечения информа-

ционной связности и организации взаимодействия между всеми участниками боевых действий в бою или операции.

В нем должны создаваться и циркулировать информационные потоки, обеспечивающие решение всех боевых задач, задач управления войсками и оружием, обслуживания войск в ходе подготовки и ведения операций, а также осуществляться информационное взаимодействие государственных органов, органов военного управления, командующих, командиров и их штабов, всех вооруженных сил как в мирное время, так и в условиях военных конфликтов. ЕВИП должно являться составной частью единого информационного пространства страны.

При этом важно, чтобы доступ к информационным ресурсам осуществлялся в любой точке этого пространства (при соответствующих полномочиях). Непрерывность ЕВИП может быть достигнута на базе широкого использования разветвленных наземных проводных, радио-, радиорелейных и тропосферных сетей связи, сетей подвижной радиосвязи и систем спутниковой связи в результате системной интеграции локальных и территориальных информационных и телекоммуникационных сетей, охватывающих все объемное военное информационное пространство на земле, воде, под водой, в воздухе и космосе.

Основным компонентом ЕВИП, как и любого информационного пространства, должна, на наш взгляд, являться информационная инфраструктура, которая определяет его размеры и форму, обеспечивает создание и циркуляцию информационных потоков, а также функционирование и развитие ЕВИП, организует сбор, обработку, поиск, хранение, анализ, распределение и распространение всей циркулирующей в информационном пространстве информации [100] (2004).

информационное пространство (поле) — в узком смысле для оперативно-тактического звена — массивы информации, связанной с объектами управления; в широком смысле — совокупность результатов семантической деятельности человечества [130] (2014).

информационное пространство операции — структурированная совокупность сведений по всем свойствам, элементам и объектам оперативного пространства, существенным для успешного проведения операции [89] (2001).

информационное поле[1] — вся информация в таком поле должна отвечать следующим требованиям: полнота и всесторонность, достоверность, своевременность и оперативность. Оптимальное решение

предполагает исчерпывающую информацию обо всех обстоятельствах, влияющих (могущих повлиять) на объекты и ход событий, на которые направлена властно-распорядительная деятельность органов военного управления.

С этим связано наличие целого ряда объективных противоречий в формировании информационного поля.

Во-первых, достоверность информации обеспечивается ее перепроверкой, что требует времени и, следовательно, ведет к запаздыванию информации, снижает ее оперативность. И наоборот, оперативность может стать причиной недостаточной надежности информации.

Во-вторых, полнота информации предполагает наличие всех знаний обо всем, что в принципе невозможно. Между тем очень большое количество сведений с трудом поддается обработке. Поэтому избыток или излишняя детализация информации, как и ее недостаток, затрудняют оценку обстановки.

В-третьих, наличие многих и разных источников информации может стать причиной, с одной стороны, повторяемости информации, а с другой — ее несопоставимости.

И, наконец, в-четвертых, определенные трудности связаны с обострением противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение [176] (2008).

информационное поле[2] — совокупность значений, принимаемых характеристиками объектов в системе классификации и кодирования информации.

Для этого при разработке модели следует выявить базисные информационные структуры, точно определяющие состав объектов, которые должны входить в нее, а также перечни их характеристик [21] (1994).

единое информационное пространство РВиА — совокупность баз и банков данных РВиА, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей РВиА, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие формирований (объектов) и отдельных военнослужащих РВиА, а также удовлетворение их информационных потребностей.

При этом ЕИП РВиА должно состоять из следующих основных компонентов: информационные ресурсы, содержащие данные, сведения и знания, зафиксированные на соответствующих носителях информации; организационные структуры, обеспечивающие функционирование и развитие ЕИП РВиА, в частности сбор, обработку, хранение, распространение, поиск и передачу информации; средства информационного взаимодействия формирований и отдельных военнослужащих РВиА, обеспечивающие доступ к информационным ресурсам.

Единое информационное пространство базируется на применении компьютерных, информационно-коммуникационных и передовых педагогических технологий.

Единое информационное пространство рода войск условно подразделяется на три уровня.

Уровень управления. На данном уровне осуществляется: разработка стратегии применения компьютерной техники; материально-техническое оснащение подразделений, частей и соединений РВиА; подготовка кадров и создание мотивации использования информационно-коммуникационных технологий; создание автоматизированных рабочих мест вышестоящих командиров (начальников) и командиров подразделений, частей, соединений; составление оптимального расписания, позволяющего максимально эффективно задействовать имеющуюся компьютерную технику; развитие информационных ресурсов и их содержательное наполнение; создание условий для повышения возможностей информационных коммуникаций и ресурсов компьютерных сетей в (учебно-воспитательном) процессе подготовки войск; создание нормативно-организационной структуры, обеспечивающей эффективное взаимодействие пользователей в условиях информационной среды; разработка единых универсальных правил анализа, оценки и учета результатов подготовки подразделений, частей и соединений по предметам обучения.

Уровень исполнителей (командиров подразделений, частей и соединений). Функциями этого уровня являются: формирование методического обеспечения, позволяющего эффективно использовать компьютерную технику (тренажеры); разработка и подбор методик использования новых информационных технологий (тренажеров) на занятиях; формирование банка обучающих и контролирующих программ по предметам обучения; создание банка учебных (комплексных) задач, способных расширить возможность выбора; обеспечение условий для

самостоятельной подготовки обучаемых с использованием возможностей информационно-коммуникационных технологий.

Уровень обучаемых. В этой среде происходит доступ к информации, банкам знаний, дистанционным ресурсам, необходимым обучаемым для учебной деятельности и самостоятельной подготовки, получения дополнительного образования [7] (2014).

информационное обеспечение стрельбы и управления огнем зенитных средств группировки войск ПВО СВ — совокупность мероприятий, направленных на сбор, обработку, передачу, хранение, защиту и предоставление должностным лицам органов управления информации, необходимой для выполнения ими своих функциональных обязанностей в процессе планирования и оперативного управления огнем подчиненных сил и средств [66] (2007).

система информационного обеспечения стрельбы и управления огнем — совокупность пунктов и средств сбора, обработки, передачи, хранения, защиты, преобразования и представления потребителям информации, необходимой для реализации ими функций управления огнем [66] (2007).

информационное поле стрельбы и управления огнем зенитных средств группировки войск ПВО СВ — область пространства, в пределах которой обеспечивается формирование, обработка и взаимный обмен информацией о воздушной обстановке, необходимой для эффективного функционирования системы управления огнем зенитных группировки войск ПВО СВ [66] (2007).

способ формирования информационного поля стрельбы и управления огнем — порядок и приемы ведения разведки, которые характеризуются числом и разнообразием типов источников информации, привлекаемых к работе на различных этапах отражения удара воздушного противника, режимами их функционирования, спецификой схемы передачи информации о воздушной обстановке [66] (2007).

единое информационное пространство Военно-воздушных сил — совокупность информации о противнике, своих войсках и условиях ведения боевых действий, получаемой органами и пунктами управления и характеризующейся согласованностью по составу, объему и срокам доведения.

Оно должно обеспечивать своевременное получение информации от источников различной физической природы и видовой принадлежности, формирование и ведение единой информационной базы и своевременное доведение необходимой информации до органов и пунктов управления, а также средств поражения в соответствии с предоставленными правами доступа [193] (2004).

единое информационное поле корабля — его создание потребует: стандартизации и унификации информационных ресурсов, необходимых для реализации типовых функций управления; разработки унифицированной системы боевых текстовых, графических, электронных документов и панелей диалога, словарей и классификаторов, нормативно-справочной информации; унификации документальных и логических структур баз данных; сосредоточения усилий разработчиков на стандартизации протоколов информационного взаимодействия боевых и технических систем; внедрения единой схемы адресования и именования ресурсов [202] (2001).

единое разведывательно-информационное пространство (ЕРИП) — пространство, основу создания которого составляют обеспечивающие автоматизированное управление системы поиска (добывания) информации.

При этом источниками информации являются базы данных разведывательных органов и служб, технических средств получения разведывательной информации различного вида, которые являются компонентами системы поиска (добывания) информации.

Создание единого информационного пространства является необходимым, но не единственным условием успеха боевых действий. ЕРИП позволяет решать всего лишь элементарные фрагменты задач управления в ходе подготовки и ведения военных действий. Решение всего ряда управленческих задач (принятие решения, планирование, доведение задач и др.) требует автоматизации всех информационных процессов [199] (2011).

разведывательно-информационное пространство соединения (РИП) — совокупность знаний и информации о противнике в зоне ответственности соединения, подчиненных и взаимодействующих силах и средствах разведки (в том числе и других министерств и ведомств РФ), решаемых ими задачах, условиях ведения тактических действий, собираемой, накапливаемой и хранимой системой разведки соедине-

ния по единым правилам в виде оформленных документов в определенной информационной среде (базе данных) на текущий момент времени.

В перспективе следует добиться, чтобы РИП соединения стало составной частью единого разведывательно-информационного пространства (ЕРИП) [201] (2013).

информационное образовательное пространство системы военного образования — составная часть единого информационного образовательного пространства (среды) сферы образования Российской Федерации, обеспечивающая оперативный и полный доступ пользователей к потребным информационным ресурсам [149] (2006).

1.5. Телекоммуникации

информационно-телекоммуникационная система (ИТКС) — совокупность согласованных по задачам комплексов технических и программных средств передачи, обработки, хранения и защиты информации (компьютерных и телекоммуникационных сетей), массивов информации различного назначения, создаваемых (развертываемых) для обеспечения автоматизированного управления.

Она обеспечивает своевременное получение данных обстановки и разведывательных сведений от специальных сил и средств, составляющих систем поиска информации различных уровней.

ИТКС является базовым элементом, от которого во многом зависит реализация возможностей других составляющих системы автоматизированного управления подготовкой и ведением военных действий. При этом сама необходимость создания информационно-телекоммуникационной системы диктуется общим эволюционным процессом трансформации системы связи, а на этой основе и других автоматизированных систем [199] (2011).

информационно-телекоммуникационная система Вооруженных Сил — организационно-техническое объединение сил (средств) связи и автоматизации, реализующее информационные процессы с использованием информационных и сетевых технологий в рамках системы управления Вооруженных Сил.

При этом основой информационной составляющей являются фонды, базы данных, информационное, математическое, программное,

техническое (аппаратное), лингвистическое обеспечение, а также информационные технологии как инструментарий по обработке и преобразованию информационного ресурса. Информационная часть по сути отражает основное содержание автоматизированной системы управления.

Телекоммуникационная составляющая включает в себя систему связи, а также сетевые технологии, которые определяют тип, архитектуру, порядок и правила функционирования сетей связи.

Организационная составляющая в свою очередь обеспечивает эффективное функционирование информационно-телекоммуникационной системы с помощью правовых и нормативных механизмов [197] (2008).

процесс интеграции компьютерных и телекоммуникационных сетей — процесс объединения систем связи и автоматизированных систем управления в единую информационно-коммуникационную систему специального назначения, реализуемую на основе сети связи общего назначения, имеющую возможности выхода в международные глобальные сети [217] (2014).

интегрированная система связи и передачи данных (ИССПД) — совокупность унифицированных многофункциональных широкодиапазонных радиостанций и коммутационных устройств, аппаратурно и функционально сопрягаемых, объединенных единой системой управления, обеспечивающих передачу потоков разнородной информации (речевые сигналы, данные, графические и видеоизображения) и «бесшовное» сопряжение по горизонтали и вертикали мобильных и стационарных абонентов АСУ различного функционального назначения.

Под «бесшовностью» понимается исключение ручных операций при соединении абонентов и обмене данными между разнородными системами связи [88] (2014).

единая информационно-коммуникационная сеть — сеть, объединяющая ударные разнородные средства и органы управления ими на основе новых информационных технологий [73] (2012).

единое информационно-коммуникационное пространство[1] — совокупность высокотехнологичных коммуникационных средств и необходимых информационных ресурсов (данных), обеспечивающих

своевременное решение управленческих задач в целях эффективного воздействия на противника в реальном масштабе времени.

По-нашему мнению, понятие «единое информационно-коммуникационное пространство» в более полной мере, чем относительно узкое по смыслу понятие «единое информационное пространство», соответствует реально происходящим изменениям в военной и смежных с ней науках в области управления войсками и оружием. По сути, отражаемое данным понятием явление представляет собой материальный объект в виде высокотехнологичной глобальной информационно-коммуникационной сети, что, кстати, соответствует сущности понятия «сеть» в теории сетецентрической войны.

Вряд ли нужно доказывать, что «единое информационно-коммуникационное пространство» не является пространством как таковым, а представляет собой совокупность современных средств (в самом широком смысле), которая позволяет существенно повысить возможности управления, в частности, войсками и оружием.

Несмотря на условность понятия «Единое информационно-коммуникационное пространство», этой условностью можно пренебречь, так как в конечном счете данное понятие трансформируется в понятие «Универсальная автоматизированная система управления войсками» [165] (2012).

единое информационно-коммуникационное пространство[2] — в его рамках любые источники информации, системы оружия всех видов вооруженных сил и системы управления будут объединены посредством локальных, территориальных и глобальных систем связи наземного, морского, воздушного и космического базирования, обладающих высокой мобильностью, скоростью развертывания и пропускной способностью. С построением единого информационно-коммуникационного пространства ВС США, как ожидается, получат преимущество в возможности нанесения упреждающего глобального информационно-огневого удара, лишающего противника шанса организовать хоть какое-нибудь активное сопротивление [148] (2008).

единое информационно-коммуникационное пространство[3] — его сторонники утверждают, что формирование такого пространства, позволяющего каждому участнику боевых действий иметь точные данные о ситуационной осведомленности, повышает уровень взаимодействия и самосинхронизации, а, в конечном счете, и скорость управления подчиненными силами и средствами, а также боевые возможно-

сти формирований, то «сомневающиеся» отмечают, что сетецентрическая логика военного руководства может задушить разумную критику новых концепций со стороны командиров оперативного и тактического звеньев управления. Они говорят о вероятности того, что, в конечном счете, министерство обороны США может реформировать свои вооруженные силы не для проведения операций, с которыми они, скорее всего, столкнутся, а для таких войн и вооруженных конфликтов, которые они сами хотят вести. Например, если в соответствии с сетецентрическими концепциями продолжительность перспективных боевых действий будет уменьшаться, то более слабый противник постарается втянуть ВС США в продолжительный конфликт, чтобы попытаться выиграть войну единственным для себя способом — избежать быстрого разгрома. В случае затяжной войны политическая воля США будет таять, а военные расходы — неумолимо расти.

Кроме того, принцип «первым увидел и первым начал действовать», который лежит в основе всех сетецентрических концепций, может не сработать в случае, если темп операции будет опережать способности командования ВС США оценивать ситуацию и принимать решение. Более того, многие эксперты отмечают, что «...сетецентризм» — это тезис не только переоценивающий значение информации и информационных технологий, но и одновременно с этим не способный полностью реализовать имеющиеся потенциальные технологические возможности» [117] (2009).

информационно-коммуникационное пространство — объединяет подсистемы, имеющие структуру решетки: сенсорной (разведывательной) и боевой, в свою очередь, интегрирующей средства управления и поражения.

В результате единая сеть средств разведки, связи и органов управления увязывается с сетью средств поражения и сетями боевого и тылового обеспечения [73] (2012).

система связи — подсистема системы управления, представляющая собой организационно-техническое объединение сил и средств связи, создаваемое для обеспечения обмена всеми видами информации в систему управления войсками.

На практике организация связи в операции (бою) обычно осуществляется по направлениям. При этом известно, что **направление связи** — это совокупность узлов и линий связи, образованных различными средствами и обеспечивающих связь между двумя пунктами

управления. Виды связи и их количество на каждом направлении связи определяются потребностями системы управления (объемом и срочностью передаваемых сообщений, а также требуемой оперативностью ведения переговоров) [46] (2008).

система связи Вооруженных Сил — значительную часть задач решает, используя ресурсы Единой сети электросвязи страны, в первую очередь ее магистральные линии и каналы, а также сети специального назначения [167] (2005).

система связи ВС РФ — целью ее развития является создание в кратчайшие сроки взаимоувязанной информационно-телекоммуникационной инфраструктуры и обеспечение ее соответствия требованиям управления ВС РФ в новых условиях военно-политической обстановки в мире. Основополагающим в этом вопросе является переоснащение объектов связи (узлов связи, отдельных центров, аппаратных и др.) современными автоматизированными средствами связи, раработанными на основе передовых нано- и биотехнологий. При этом транспортная сеть должна обеспечить образование цифровых каналов (трактов), коммутацию и маршрутизацию интегрированных цифровых потоков, обеспечение доступа к образованному ресурсу как узлов связи пунктов управления, так и подвижных объектов [194] (2011).

объединенная автоматизированная цифровая система связи общего назначения — система связи, структурно включающая в свой состав интегрированную цифровую территориальную систему связи ВС РФ, цифровые полевые системы связи стратегических, оперативно-стратегических, оперативных объединений и средства связи специализированных систем связи [167] (2005).

объединенная автоматизированная цифровая система связи ВС РФ — система связи, представляющая собой организационно-техническое объединение взаимоувязанных, технологически сопряженных перспективных автоматизированных систем связи звеньев управления (при сохранении их прежней видовой принадлежности и подчиненности), реализованное на базе интегрирования цифровых ресурсов их первичных и вторичных сетей, применения современных телекоммуникационных технологий и протоколов формирования и переноса сообщений в цифровой форме [169] (2008).

1.5.1. Требования к цифровым военным сетям связи

унификация цифрового оборудования и систем управления — весь спектр цифрового телекоммуникационного оборудования для различных сетей связи должен производиться одним разработчиком и иметь единую распределенную систему управления. Это позволит повысить эффективность технического обслуживания и оперативного управления связью, уменьшить расходы на обучение личного состава, закупку ЗИП и т.п.

Однако на практике каждый вид войск Вооруженных Сил имеет свои заказывающие и экспертные учреждения, свою сложившуюся кооперацию разработчиков. В данной ситуации выход состоит в том, чтобы новая техника создавалась на принципах «открытых систем», с применением стандартных алгоритмов и протоколов, обеспечивающих возможность совместной работы и единых принципов управления [4] (2006).

уровень защищенности — конструктивные и эксплуатационные характеристики оборудования должны соответствовать уровню защищенности объектов, на которых оно применяется [4] (2006).

информационная и техническая безопасность — применяемое оборудование должно быть отечественного производства, иметь полный комплект эксплуатационной и конструкторской документации в соответствии с ГОСТ. Программное обеспечение должно иметь полностью открытый код и быть сертифицировано уполномоченными органами [4] (2006).

допуск персонала — разработчик должен иметь персонал с допусками на режимные объекты для осуществления гарантийного и послегарантийного обслуживания поставляемого оборудования [4] (2006).

устойчивость функционирования информационно-телекоммуникационных систем — способность обеспечивать установленные регламенты выполнения технологических циклов управления, определенных требованиями нормативно-технической документации, в условиях информационно-технических воздействий [104] (2016).

1.5.2. Глобальная система связи США

единая глобальная система связи и информационного обеспечения — система, на которую в США возлагаются задачи сопряжения подсистем, и которая объединяет в единое целое инфраструктуру МО США и организационные структуры системы государственного управления [148] (2008).

глобальная информационная сеть — взаимосвязанный четко очерченный круг информационных средств и личного состава, предназначенных для осуществления процессов сбора, обработки, хранения, распространения и управления информацией по требованию политиков, военных и поддерживающего персонала.

Глобальная информационная сеть включает находящиеся в собственности министерства обороны и арендованные информационно-коммуникационные системы, программное обеспечение, информационные ресурсы, средства безопасности, а также другие взаимосвязанные информационные структуры, входящие в систему национальной безопасности США[19] [161] (2011).

глобальная информационно-управленческая сеть — сеть, предназначенная для информационного обеспечения всех элементов системы национальной безопасности страны, в том числе и вооруженных сил.

Она объединяет взаимосвязанные распределенные вычислительные системы коллективного пользования, локальные вычислительные сети, системы связи, базы данных, системы компьютерной и сетевой безопасности, средства обучения пользователей, а также другие элементы, предназначенные для централизованного удовлетворения всех информационно-технических потребностей системы управления войсками и органов административного управления. Работы по созданию сети предусматривают реализацию ряда взаимосвязанных программ различных министерств и ведомств США. На эти цели в ближайшие 10 лет планируется израсходовать порядка 200 млрд. долларов [148] (2008).

[19] The Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 12 April 2001. As Amended Through 17 October 2008.

тактический Интернет — комплекс, который включает в себя локальные сети и автономные компьютеры, находящиеся на пунктах управления, соединенные между собой любыми средствами связи, а также программные средства, обеспечивающие взаимодействие всех этих элементов [173] (2005).

1.5.3. Военный (боевой) Интернет ВС РФ

глобальный боевой Интернет — сеть связи для обмена информацией в режиме on-line, главное в которой управление из единого центра всеми видами и родами войск в их иерархическом построении, вплоть до конкретного бойца, которому отводится роль «электронного солдата».

Военными действиями в любой точке Земли будут управлять непосредственно из Пентагона. Верховный главнокомандующий в реальном масштабе времени может наблюдать картину боя на экране компьютера и при желании связываться со всеми командирами [194] (2011).

военный (боевой) Интернет ВС РФ — информационная сеть закрытого типа (ограниченного доступа), предназначенная для управления Вооруженными Силами Российской Федерации в условиях мирного (в повседневной деятельности войск) и военного времени и обеспечивающуя ее пользователям быстрый доступ к различной информации в режиме on-line.

В отличие от глобальной сети, работающей в операционной системе Windows NT, с централизованной службой WINS и IP-адресами Интернет ВС РФ должен создаваться как автономная сеть со своей операционной системой (МС ВС), специальной службой доменных имен — DNS (Domain Name Service) и IP-адресами.

Достоинство военного (боевого) Интернета ВС РФ заключается в том, что создается единая разветвленная информационная сеть (типа «решетка»), обеспечивающая определенный санкционированный доступ к информации, повышается эффективность боевого управления войсками, их маневренность и взаимодействие в боевых условиях. Создаваемая сеть будет представлять три взаимоувязанные сферы (сегменты): информационную, физическую и когнитивную, что позволит обеспечить синхронизацию боевых действий и систем управления на поле боя, и тем самым повысить уровень боевых возможностей Во-

оруженных Сил. Сеть должна обеспечить непрерывный и единообразный обмен информацией для всех систем и средств, используемых в мирное время и при ведении боевых действий, и объединить в одно целое слагаемые процесса боевых действий путем создания цепочки: обнаружил, принял решение (обработал), нанес удар (поразил) [194] (2011).

локальный боевой Интернет — сеть связи, охватывающая подразделения (боевые расчеты) батальонного уровня, имеющая программно-аппаратные средства, предназначенные для построения телекоммуникационных сетей, функционирующих в постоянно меняющихся условиях обстановки во всех звеньях управления.

Аппаратные должны включать средства спутниковой и радиорелейной связи, радиосвязи, беспроводного доступа, серверы, кросс-маршрутизаторы, терминальные устройства и другое оборудование. Так как подразделения и боевые расчеты, выполняющие боевые задачи самостоятельно или в составе соединения, как правило, на поле боя будут действовать рассредоточено и при частых перемещениях, то для организации связи необходимо использовать средства беспроводного доступа:

— станции беспроводного доступа на основе стандарта IEEE 802.11;

— УКВ и КВ радиостанции типа «Акведук» и последующих разработок;

— станции спутниковой связи;

— станции широкополосного беспроводного доступа 802.16 [194] (2011).

недостатки глобального боевого Интернета — отрицательные факторы, оказывающие влияние на функционирование глобальной сети Интернет:

— вероятность «зависания» компьютеров у должностных лиц или сбоев в работе серверов, какими бы совершенными и технически надежными они ни были;

— возможность ввода ложной информации;

— возможность несанкционированного «скачивания» информации, имеющей определенный гриф секретности;

— увеличивающийся риск подверженности каждого пользователя сети;

— ввод в сеть и в системы управления супервирусов.

Уязвимости могут быть подвержены линии и каналы связи, обеспечивающие доступ управляющих и управляемых объектов к сети Интернета. А если представить картину, когда идет бой, а управляющий им комплект не функционирует, «завис», военный Интернет не реагирует на внешнее радиоэлектронное противодействие и абсолютно беспомощен перед угрозой внутреннего вторжения. То есть сетецентрическую войну в ее нынешнем виде может выиграть один человек, имеющий в своем арсенале специально созданную вирусную программу и доступ во Всемирную сеть [194] (2011).

единое адресное пространство — адресное пространства в масштабе Вооруженных Сил Российской Федерации, необходимое для устойчивой работы военного (боевого) Интернета, обеспечивающее работу пользователей в сети на всех уровнях иерархии.

В ВС РФ должен создаваться специальный орган, ответственный за распределение IP-адресов из таблицы IP-адресов ВС РФ. Управление адресами единого адресного домена организуется на основе формирования иерархии доменов в соответствии с подчиненностью [194] (2011).

полевая составляющая системы связи — развертываемая система связи для применения военного (боевого) Интернета в условиях ведения боевых действий (сетецентрическом действии войск), которая должна представлять единое информационное пространство, взаимоувязанное со стационарной составляющей на основе внедрения новых информационных технологий, современных автоматизированных систем управления, слежения (наблюдения), разведки, сбора данных, с совокупностью ударно-огневых элементов (комплексов) различного назначения. При этом единое информационное пространство должно поддерживаться линиями, трактами и каналами связи различной родовой принадлежности [194] (2011).

1.5.4. Информационные сети

информационная сеть — совокупность источников информации, средств ее хранения и обработки (ЭВМ различных типов) и рабочих (информационных) станций должностных лиц органов управления, связанных между собой каналами связи, с распределенным по ЭВМ хранением и обработкой информации, с возможностью доступа к лю-

бой хранимой информации с любых рабочих (информационных) станций должностных лиц (кроме случаев закрытой информации), с централизованным управлением сетью.

Таким образом, основными технологическими признаками информационной сети, отличающими ее от обычных информационных систем, являются: рабочие (информационные) станции должностных лиц органов управления, локальные вычислительные сети (ЛВС) органов управления, распределенное хранение информации, распределенная обработка информации, единые для всех узлов сети языковые средства общения должностных лиц с системой и языковые средства взаимодействия между узлами сети, совместимые для всех ЭВМ (ПЭВМ) средства общего программного и информационного обеспечения [96] (1997).

локальные вычислительные сети (ЛВС) — техническая основа информационных сетей.

Узлами ЛВС являются рабочие (информационные) станции на основе ПЭВМ, центральная (большая) ЭВМ, используемая чаще всего в качестве так называемого «сервера базы данных», и процессоры для решения специальных и наиболее общих задач органа управления. Важнейшая функция ЛВС заключается в организации распределенного хранения и распределенной обработки информации в узлах сети. Если в каждом из узлов сети это может осуществляться с помощью существующих ныне средств, то для управления работой всех узлов сети требуются специальные средства управления функционированием информационной сети. При этом желательно на всех узлах сети использовать совместимые средства программного и информационного обеспечения, с тем чтобы повысить эффективность функционирования сети и ее эксплуатационные характеристики, а также снизить затраты на ее создание [96] (1997).

рабочие (информационные) станции — создаются на основе ПЭВМ, которые наряду с функцией отображения информации, свойственной автоматизированным рабочим местам (АРМ), обладают функциями хранения информации, ее обработки и взаимодействия с любыми узлами (ЭВМ) и другими рабочими станциями сети. Причем взаимодействие между ними осуществляется не только за счет возможности организации физической связи между ними, но прежде всего на основе использования средств программного управления ЛВС. Клиенты рабочих (информационных) станций могут работать как со свои-

ми локальными информационными ресурсами (локальной базой данных) и программами, размещенными на станции, так и с общими ресурсами, распределенными в ЛВС. Рабочие (информационные) станции могут одновременно являться источниками информации. При этом обработка информации в интересах рабочей станции может выполняться на самой рабочей станции на основе собственной и получаемой из других узлов (ЭВМ) сети информации, а также в других узлах (ЭВМ) сети с последующей передачей на эту рабочую станцию конечных результатов [96] (1997).

интегрированная база данных — база данных, находящаяся в центральной ЭВМ сети, где будет храниться общая для всех узлов сети информация, информация для решения на центральной ЭВМ сети общих для всех рабочих станций задач и индивидуальная информация центральной ЭВМ [96] (1997).

индивидуальные базы данных — базы данных, находящиеся на рабочих станциях, где будет храниться собственная информация, используемая только на этой рабочей станции, и часть информации интегрированной базы данных, для которой эта станция является источником поступления информации [96] (1997).

1.5.5. Нетрадиционный способ передачи информации в тактическом звене

артиллерийский информационный снаряд (АИС) — один из новых нетрадиционных способов передачи больших объемов информации на расстояния, ограниченные тактической зоной боевых действий.

Для этого должны быть выделены специальные артиллерийские орудия, стреляющие информационными снарядами, подготовлены площадки (районы) приема АИС. Их следует оборудовать вблизи (до нескольких сот метров) от узла связи пункта управления (ПУ) желательно на открытой местности с твердым грунтом на площади, ограниченной прямоугольником со сторонами 150—200 м или окружностью с радиусом 100—150 м.

В свою очередь артиллерийский информационный снаряд вместо взрывчатого вещества будет оснащаться специальными контейнерами

с носителями информации различного типа (устройства флэш-памяти, компакт-диски и др.) [154] (2006).

2. Информационная война

информационная война[1] — противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, 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[20] [13, 141] (2012, 2014).

информационная война[2] — использование современных технологий, позволяющих создавать заведомо ложную информацию или фальсифицировать (искажать) существующую информацию. Данный термин имеет два значения.

Первое. Воздействие на гражданское население и военнослужащих другого государства путем распространения определенной информации. Термин «информационно-психологическая война» был заимствован из словаря военных кругов США. Перевод этого термина с английского языка может означать информационное противоборство, информационную и психологическую войну, которая оказывает психологическое воздействие на гражданское население и военнослужащих другого государства с целью достижения политических или чисто военных целей.

Второе. Целенаправленные действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информационным процессам и системам противника при одновременной защите собственной информации, информационных процессов и систем [177] (2015).

информационная война[3] — совокупность мер и мероприятий, предназначенных для обеспечения информационного преимущества по отношению к потенциальному или реальному противнику.

---

[20] Приложение № 1 к «Соглашению между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области международной информационной безопасности», Екатеринбург, 2008.

Информационную войну, на наш взгляд, целесообразно рассматривать в двух основных аспектах: в широком понимании — как новую форму геополитического соперничества сторон (в этом случае имеет смысл использовать термин «информационное противоборство») и в более узком значении — применительно к области вооруженной борьбы (здесь целесообразно использовать термин «информационная борьба») [171] (1997).

информационная война[4] — комплексное воздействие (совокупность информационных операций) на систему государственного, военного управления и военно-политическое руководство противостоящей стороны, которое уже в мирное время может привести к принятию благоприятных для стороны — инициатора решений, а в ходе конфликта позволяет полностью парализовать функционирование инфраструктуры управления противника.

Одна из целей ведения информационной войны, по мнению военных экспертов США, является достижение информационного превосходства над противником [203] (2012).

информационная война[5] — комплексное воздействие на систему государственного и военного управления противостоящей стороны, ее политическое и военное руководство, которое уже в мирное время приводит к принятию благоприятных для США решений, а в ходе военных действий полностью парализует всю систему управления противника.

Одновременно предусматриваются меры по защите своих систем управления от несанкционированного использования, изменения и физического разрушения.

Соответственно выделяются два основных уровня реализации концепции: государственный и военный. На государственном — организуется целенаправленное информационное (информационно-психологическое) воздействие на недружественные страны (на потенциальных противников) в интересах влияния на процессы принятия решений высшим военно-политическим руководством этих стран, всестороннего воздействия на их политическую и культурную жизнь с задачей подрыва национально-государственных устоев общества, проникновения на все уровни системы государственного управления. На военном уровне министерством обороны, штабами видов вооруженных сил и объединенных командований проводится комплекс информационно-технических и других мероприятий, направленных на достижение ин-

формационного господства над противником и защиту своих систем управления от его аналогичных действий.

Следует подчеркнуть, что принятая в США концепция «информационной войны» предусматривает разграничение задач и характера действий на мирное и военное время. Это означает одно — «информационная война» рассматривается ими как самостоятельное явление (существующее и без вооруженной борьбы, в мирное время). В мирное время она имеет целью подрыв основ безопасности личности, общества и государства противоположной стороны и защиту национальных интересов своей страны, в военное — достижение полного информационного господства над противником [93] (2002).

информационная война[6] — действия, предпринимаемые для достижения информационного превосходства в интересах национальной военной стратегии и осуществляемые путем влияния на информацию и информационные системы противника при одновременной защите собственной информации и своих информационных систем.

Основные усилия в ней сосредоточиваются не на поражении личного состава и боевой техники противника, а на выведении из строя его компьютерных сетей и сетей связи главных штабов [223] (2017).

информационная война[7] (ИВ) — кроме военного включает еще и финансовые, торговые, психологические, юридические и другие аспекты.

При этом в ИВ главная цель наступательных информационных воздействий смещается с активного воздействия на автоматические системы и средства вооружения — на человека, т.е. на лицо, принимающее решение.

В качестве базовых категорий ИВ в США приняты: оборонительная ИВ; наступательная ИВ; ИВ в локальных случаях угроз и конфликтов; ИВ в периоды напряженности и перехода к конфликту. Оборонительная ИВ ведется в целях обеспечения информационной безопасности, т.е. для защиты собственной информационной системы от проникновения в нее вражеских или криминальных элементов. Наступательная ИВ включает практически весь спектр действий, используемый системой борьбы за управление и контроль C2W. Объектами воздействия при ИВ являются: военная информационная инфраструктура, решающая задачи управления войсками; информационные и управляющие структуры банков и других предприятий; средства массовой информации [133] (2003).

информационная война[8] — Пентагон отказался от использования категории «информационная война», под которой ранее понимались «информационные операции», проводимые во время конфликта или кризиса для достижения или продвижения специальных целей в отношении определенного противника или противников.

Скорее всего, этот шаг обусловлен не столько научными, сколько политическими соображениями. Предпринимая его, американский истеблишмент, видимо, стремится ликвидировать повод к обвинению Вашингтона в разжигании вооруженных конфликтов путем проведения подрывных или иных эскалационных и агрессивных действий в мировом информационном пространстве, ассоциируемых в общественном сознании с понятием «война» [113] (2008).

информационная война[9] — термин может рассматриваться только как качественная характеристика обеспечения современных боевых действий, что не дает никаких оснований считать информацию чуть ли не поражающим фактором и придавать ей решающее значение в деле достижения победы на поле боя.

Позицию американских военных в этом вопросе можно счесть даже в какой-то мере скептической. Как указывает Joint vision 2020, поскольку «конечной целью информационных операций является лицо, принимающее решение, командиру Объединенных сил будет трудно точно оценить последствия этих операций».

Отмечается также, что размер боевого ущерба от информационных операций крайне трудно оценить и что сделать это возможно только на основе опытных данных и строго спланированного и проведенного эксперимента.

Доктрина весьма прагматично замечает, что в войнах будущего американцы не гарантированы от того, что им придется столкнуться с противником, который окажется способным адаптироваться, использовать асимметричные варианты нанесения ущерба и возможности относительно недорогих информационных технологий: коммерческих спутников, цифровой связи, интернет-коммуникации и прочих [123] (2014).

методы информационной войны — подача дезинформации или представление информации на то или иное событие в выгодном для себя свете.

Данные методы позволяют изменять реальную оценку происходящего события в сознании населения противника, развивать поражен-

ческие настроения и в перспективе обеспечить переход на свою сторону [177] (2015).

информационная агрессия (киберагрессия) — агрессия в информационном пространстве.

Речь идет о целесообразности адаптации и развития существующего Определения агрессии на основе включения в его ст. 3 возможных актов агрессии в информационном пространстве. В частности, к их числу предлагается отнести:

— применение вооруженными силами государства информационного оружия против информационных ресурсов критически важных объектов другого государства;

— пропаганда государством войны и применения силы, распространение подстрекательской информации, способствующие дестабилизации внутригосударственной и международной обстановки, развязыванию и эскалации вооруженных конфликтов [83] (2013).

2.1. Информационное противоборство

информационное противоборство[1] — целенаправленное использование информации для достижения политических, экономических, военных и других целей.

Главной целью информационного противоборства в военной сфере, по нашему мнению, является завоевание и удержание информационного превосходства над вооруженными силами противника и создание благоприятных условий для подготовки и применения своих Вооруженных Сил.

Информационное противоборство должно вестись постоянно в мирное время, в угрожаемый период и в военное время всеми имеющимися силами и средствами путем воздействия на информационные объекты противоборствующей стороны и защиты собственных от подобного воздействия.

Главным принципом достижения цели является комплексное воздействие сил и средств информационного противоборства по объектам противника в тесном сочетании и взаимодействии с действиями войск (сил) [188] (2014).

информационное противоборство[2] — открытое и (или) скрытое целенаправленное информационное воздействие противоборствующих

сторон друг на друга в целях получения определенного выигрыша в материальной сфере.

Официально термин был впервые применен в директиве МО США от 21 декабря 1992 года.

В соответствии с основополагающим документом комитета начальников штабов[21] основной составляющей кардинального повышения боевых возможностей ВС США в перспективе до 2010 года является достижение информационного и технологического превосходства. Причем это превосходство должно носить характер «всеохватывающего (всеобъемлющего, глобального) господства».

Некоторые зарубежные специалисты считают, что информационное противоборство (борьба) является частью информационной войны [133] (2003).

информационное противоборство[3] — одна из форм управления, в том числе противником и защиты от его аналогичного воздействия на деятельность соответствующих органов наших войск [185] (2008).

информационное противоборство[4] — направлено на достижение целей государственной политики в мирное и военное время. Оно является закономерным объективным процессом, который всегда имел и будет иметь место в отношениях между государствами независимо от развития сотрудничества между ними [171] (1997).

информационное противоборство[5] — конфликтное взаимодействие в информационной сфере субъектов политики, действующих в соответствии с нормами национального права (легитимных), и субъектов политики, действующих вне национального правового поля (нелегитимных) [204] (2011).

информационное противоборство[6] (ИП) — комплексное воздействие на системы управления противостоящей стороны, ее политическое и военное руководство, которое еще в мирное время призвано обеспечить выгодную для воздействующей стороны направленность процессов управления и принятия решений противостоящей стороной[22] [217] (2014).

---

[21] Joint Vision 2010 года.

[22] Доктрина «Информационные операции» (JP 3—13), утвержденная Комитетом начальников штабов США 13 февраля 2006 г.

информационное противоборство[7] [Information Warfare, IW] — комплексное воздействие на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство [212] (2012).

информационное противоборство[8] — необходимость четкого отлаживания информационных процессов в своей системе управления должна сочетаться с активными действиями в целях срыва информационного обеспечения противника.

Для этого прежде всего требуется, надежно перекрывая возможные каналы утечки особо важной информации, активно препятствовать добыванию, сбору, передаче, обработке информации противником, всячески дезинформировать его [33] (1990).

информационное противоборство[9] — принципами его ведения являются: скрытность, изощренность, систематичность, активность, многообразие приемов, правдоподобие, избирательность, знание психологии противника, рефлективное управление его поведением; упреждение противника. Составными элементами такой борьбы могут быть: информационная блокада, противоразведывательная деятельность, электронное подавление систем боевого управления противника; проведение электронно-огневой информационно-ударной операции; сочетание огневого, радиоэлектронного и массированного информационно-психологического воздействия на противника.

В США информационное противоборство рассматривается как один из способов ведения так называемой «управляемой войны» (Р. Канн), когда сильнейшая сторона путем информационного воздействия диктует свою волю противнику без применения оружия. Силовые акции в таком противоборстве предусматриваются на завершающей фазе действий, в случае если будут исчерпаны политические, дипломатические и иные возможности «бескровного сокрушения» вражеского государства. Новым при проведении комплексной информационно-ударной операции, по опыту локальных войн, является то, что массированное применение новейших радиоэлектронных средств, постановка радиозавес, радиопомех, создание ложной радиоэлектронной обстановки, имитация ложных радиосетей, радиоблокада каналов сбора и обработки информации противника сочетаются с проведением воздушно-наземной операции [39] (2008).

система информационного противоборства — основная система в перспективном облике Вооруженных Сил, обеспечивающая проведение мероприятий по информационной безопасности своих и подавлению (поражению) информационных объектов противника.

Ее структура может включать ряд подсистем:

— информационно-технического воздействия и защиты;

— программно-аппаратного воздействия и защиты;

— разведки, в том числе радиоэлектронной разведки;

— радиоэлектронной борьбы;

— психологической борьбы и морально-психологического обеспечения [188] (2014).

управление информационным противоборством — управление при подготовке и ведении стратегических действий (операций) Вооруженными Силами Российской Федерации, осуществляемое органами военного управления с учетом информационных мероприятий общегосударственного (невоенного) характера и информационных мер, проводимых органами управления, силами и средствами различных министерств и ведомств.

При подготовке и проведении операций (боевых действий) все информационные мероприятия, направленные на воздействие по информационным объектам противника и на защиту своих войск (сил) и оружия, населения в районах военных действий (военных конфликтов), должны централизованно координироваться [188] (2014).

2.1.1. Информационное противоборство в государственной политике

субъект политики — социально активная сила общества (политический лидер, политическая партия, общественное объединение, государство), участвующая в борьбе за право использования ресурсов публичной власти для реализации своих представлений о наиболее острых проблемах общественного развития и путях их решения [204] (2011).

политическое информационное противоборство — нейтрализация или снижение опасности распространения вредоносных идеологий и религиозных учений, а также дезинформации национальной и

международной общественности по вопросам реализации государственной политики [204] (2011).

техническое информационное противоборство — принуждение противостоящего субъекта политики, обладающего публичной властью, посредством реализации потенциала «силового» использования информационных технологий как средства демонстрации и (или) нанесения ущерба его интересам, вынуждения к согласию с ущемлением его политической независимости и суверенитета. Выполнение этой задачи предполагает одновременную нейтрализацию потенциала противостоящей стороны по осуществлению аналогичных действий [204] (2011).

информационное обеспечение государственной политики — достижение поддержки со стороны национального общества и международного сообщества мероприятий этой политики и содействие их успешной реализации [204] (2011).

политический имидж государства — эмоциональное представление (восприятие) государства в политическом сознании национального общества и международного сообщества в качестве позитивного, нейтрального или негативного фактора их существования и развития [204] (2011).

политический имидж руководителей государства — неэмоциональное восприятие в политическом сознании в качестве позитивного, нейтрального или негативного фактора развития национального общества и международного сообщества [204] (2011).

2.1.2. Стратегическая коммуникация США

стратегическая коммуникация — совокупность используемых способов, сил и средств оказания информационно-психологического воздействия при решении задач информационного противоборства на государственном уровне.

Стратегическая коммуникация США использует следующие основные инструменты: публичная дипломатия, связь с общественностью, международное вещание, психологические операции, проводимые с использованием средств массовой информации [148] (2008).

угрозы для информационной инфраструктуры — военно-политическое руководство США выделяет четыре типа угроз.

Первый — умышленное нарушение нормального функционирования информационных процессов и вывод из строя объектов информационной инфраструктуры. К примерам такой деятельности американские специалисты относят разного рода нарушения сеансов информационного обмена или проведения каких-либо электронных финансовых операций, срыв проведения электронных конференций и переговоров, провоцирование сбоев в работе различных объектов национальной информационной инфраструктуры, в том числе обеспечивающих управление сложными техническими системами, отнесенными к категории критически важных.

Второй — незаконное получение и использование информации и данных. К этой группе угроз относят разноплановую криминальную деятельность, начиная от незаконного получения паролей доступа до проникновения в федеральные информационные сети и системы. При этом основная сложность в расследовании преступлений такого рода связана с идентификацией источника враждебного информационного воздействия, в качестве которого может выступать как отдельный хакер, так и хорошо организованная команда профессионалов, работающая в интересах государства — вероятного противника.

Третий — манипуляция информацией с целью достижения политических, экономических, военных преимуществ или удовлетворения собственных амбиций правонарушителей. Такого рода информационные атаки могут проводиться комбинированно, совместно с атаками, отнесенными к первой и (или) второй группе. Особенность угроз данного типа заключается в том, что нельзя однозначно оценить ущерб от их реализации. Если в некоторых случаях это может быть основанием для какого-либо официального заявления и негативные последствия оперативно устраняются, то иногда ущерб бывает гораздо более значительным, особенно когда такого рода атаки остаются не обнаруженными и связаны с манипулированием финансовой, экономической или военной информацией.

Четвертый — разрушение или уничтожение объектов критически важной инфраструктуры государства и его ВС путем воздействия на них через информационно-управляющие сети. Реализация угроз этой группы может иметь значительные негативные последствия как для экономики страны, так и для ее безопасности [148] (2008).

публичная дипломатия — целенаправленное информирование международной общественности, а также установление и поддержание контактов в сфере образования и культуры, нацеленное на формирование привлекательного образа страны [148] (2008).

связь с общественностью — деятельность, осуществляемая службами по связям с общественностью, входящими в организационную структуру Белого дома, Совета национальной безопасности, а также министерств, ведомств и военных командований ВС США с целью информирования и оказания воздействия на население и средства массовой информации США [148] (2008).

международное вещание — деятельность служб, финансируемых правительством США, направленная на распространение новостных сообщений, информации, программ публичной дипломатии, а также развлекательных программ посредством радиовещания, спутникового телевидения и глобальной сети Интернет [148] (2008).

психологические операции, проводимые с использованием средств массовой информации — осуществление заранее спланированных мероприятий, предусматривающих доведение специально подготовленной информации и психологических установок объекту воздействия с целью принятия им благоприятных для США решений [148] (2008).

операции по оказанию информационного воздействия — операции, которые включают психологические операции, военную дезинформацию, обеспечение безопасности действий войск (сил), контрразведывательные операции, операции по противодействию пропаганде противника, связь с общественностью [148] (2008).

2.1.3. Фальсификация истории

фальсификация истории — целенаправленное искажение (частичное нарушение) целостной картины исторического развития человеческого общества (или выбранной его части) в определенный временной промежуток [3] (2006).

ложное основание — способ, когда совокупность аргументов оказывается неполной, скрыты или искажены неугодные факты [3] (2006).

эклектика — разновидность предметной фальсификации, когда в качестве аргументов приведены такие, которые никак не связаны с доказываемым тезисом [3] (2006).

ложный тезис — разновидность предметной фальсификации, когда искажен (сужен или расширен) или подменен сам доказываемый тезис [3] (2006).

уход от предмета — способ, при котором среди многочисленных уловок в споре может применяться уход или отклонение от темы или попытка запутать основную мысль в деталях и частностях.

Главное при этом навязать оппоненту выгодную для себя тематику. Однако следует учитывать, что применение подобного способа может решать задачу доказательства иного тезиса, является составной частью информационной борьбы в другой области [3] (2006).

демагогия (апелляция к аудитории) — способ, при котором преследуется цель увеличения количества сторонников своей позиции в споре за счет использования группового эгоизма, национальных или расовых предрассудков слушателей и др. [3] (2006).

переход на личность оппонента — способ фальсификации, который преследует те же цели, что и способы предыдущей группы, но объект воздействия при этом иной. Примером может служить ссылка на порочащую действия оппонента мотивацию (трусость, жажда наживы и т.д.) или на какие-либо его (или его сторонников) проступки или неэтичные действия [3] (2006).

2.1.4. Информационное оружие

информационное оружие[1] — информационные технологии, средства и методы, применяемые в целях ведения информационной войны[23] [13, 141] (2012, 2014).

[23] Приложение № 1 к «Соглашению между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области международной информационной безопасности», Екатеринбург, 2008.

информационное оружие[2] — разделяют на технические (кибернетические и др.) средства информационного воздействия и «собственно информационные средства, связанные с восприятием и воздействием информации на личность и общество». Нетрудно заметить, что в данном случае речь идет об информационном оружии, которое лишь отчасти соотносится с традиционными информационными войнами, поскольку в них, как известно, технические средства информационного воздействия не применялись.

Теперь же, говоря об информационном оружии, часто имеют в виду не только и не столько информацию, сколько технические, кибернетические и другие средства, позволяющие воздействовать на саму информацию — «передаваемую, обрабатываемую, создаваемую, уничтожаемую, воспринимаемую и хранящуюся».

В этой связи следует подчеркнуть принципиальный момент, заключающийся в том, что информация непосредственно не может являться объектом воздействия, поскольку воздействовать на нее можно только опосредованно, через ее носитель. Это обусловлено тем, что информация — идеальный объект, не существующий в материальном виде. Она может быть изъята с носителя или вместе с носителем, уничтожена («стерта») на носителе, например, магнитном, или вместе с носителем.

Применение технических и кибернетических средств в информационной борьбе в целях физического воздействия на информацию (т.е. на ее носители) по сути превращает эту борьбу в вооруженную, но ведущуюся оружием, отличным от традиционного и создаваемым на основе новейших технологий.

Физическое воздействие на носитель информации следует относить к содержанию не информационной, а вооруженной борьбы. Сами же средства такого воздействия — к перспективным видам оружия.

Поэтому, неприемлемо отнесение технических средств и кибернетического оружия к области информационной борьбы [163] (2008).

информационное оружие[3] — устройства и средства, предназначенные для нанесения противоборствующей стороне максимального урона в ходе информационной борьбы (путем опасных информационных воздействий).

Объектами таких воздействий являются информационно-технические системы; информационно-аналитические системы; информационно-технические системы, включающие человека; информационно-

аналитические системы, включающие человека; информационные ресурсы; системы формирования общественного сознания и мнения, базирующиеся на средствах массовой информации и пропаганды; психика человека [144] (2008).

информационное оружие[4] (ИО) — средства, позволяющие достигнуть цели информационного противодействия.

Такие средства можно классифицировать по характеру воздействия на следующие группы: социальные средства воздействия (на психику и сознание людей); средства воздействия на сети информационного обмена; средства воздействия на массивы хранящейся информации; средства воздействия на комплексы обработки информации.

Такая классификация позволяет определить информационное оружие как совокупность средств воздействия на психику, сознание людей, информационно-техническую структуру системы.

В зависимости от предназначения информационное оружие может быть обеспечивающим и атакующим. Обеспечивающее оружие применяется для снятия системы защиты атакуемой стороны — системы компьютерной разведки и системы преодоления. Атакующее информационное оружие оказывает непосредственное воздействие на атакуемую компьютерную систему и включает средства нарушения конфиденциальности информации, целостности информации, доступности информации, психологического воздействия на абонентов информационной системы.

Информационное оружие атак на компьютерные сети может быть программным и аппаратным [206] (2007).

информационно-психологическое оружие — специальное оружие, основанное на применении разрушающего информационно-психологического и информационно-управляющего воздействия на психику человека для управления его поведением и деятельностью или для его уничтожения.

К числу таких видов оружия относятся: средства массовой информации (MASS-MEDIA оружие), энерго-информационно-психологическое, психотропно-информационное, биоэнерго-информационное, информационно-энергетическое, виртуальное информационно-психологическое, соматропно-психо-информационное, а также компьютерные телекоммуникационные сети и др. [44] (2006).

информационное оружие[5] — совокупность средств, предназначенных для нарушения (копирования, искажения или уничтожения) информационных ресурсов на стадии их создания, обработки, распространения и хранения.

В структуре инфосферы можно выделить следующие основные объекты его воздействия: программное и собственно информационное обеспечение; программно-аппаратные и телекоммуникационные средства; каналы связи, обеспечивающие циркуляцию информационных потоков и интеграцию систем управления; интеллект человека и массовое сознание [6] (1999).

оружие массового воздействия [weapons of mass effect] — новый военно-политический термин, впервые примененный в национальной военной стратегии США. Принципиально важным в предложенной дефиниции является, во-первых, то, что данный вид оружия поставлен в один ряд с традиционными видами оружия массового поражения (weapons of mass destruction): химическим, биологическим и ядерным. Во-вторых, в качестве разновидностей «оружия массового воздействия» определены такие виды оружия, как оружие электромагнитных импульсов (electromagnetic pulse), оружие микроволн большой мощности (nigh powered microwave), а также другое «асимметричное» оружие. В качестве иллюстрации такой асимметричности приведен пример о том, что кибератаки на американские коммерческие информационные системы или на национальные транспортные сети могут иметь более серьезный экономический или психологический эффект, чем при применении по ним какого-либо иного традиционного вида оружия. Основными объектами поражения будут информационная инфраструктура и психика личного состава войск противника [35] (2006).

информационное противодействие (ИПД) — в широком смысле — создание системы научно обоснованных и официально принятых мер по обеспечению информационной безопасности своих эргасистем и информационному воздействию на эргасистемы противостоящей стороны [206] (2007).

военно-политическая угроза в области международной информационной безопасности — использование информационно-коммуникационных технологий в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направлен-

ных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности [36] (2015).

международный режим нераспространения информационного оружия — система закономерностей, принципов, норм, правил и процедур предотвращения распространения информационного оружия, закрепленных в международных договоренностях и национальных законодательствах, а также международных и национальных органов с участием всех членов мирового сообщества и негосударственных структур, чьей конечной целью является полное запрещение информационного оружия [36, 141] (2014, 2015).

2.1.5. Международная информационная безопасность

система информационной безопасности — система, обеспечивающая стабильное состояние защищенности информационных ресурсов от воздействия информационного оружия.

При этом все необходимые силы и средства поддерживаются в постоянной готовности к отражению возможной агрессии как в самом информационном пространстве, так и с его широкомасштабным использованием, а также принимаются все возможные меры по раннему выявлению и нейтрализации потенциальных военных конфликтов в информационном пространстве [13] (2012).

государственная политика обеспечения информационной безопасности в условиях военных конфликтов — деятельность федеральных органов исполнительной власти по подготовке и реализации в информационной сфере системы мер, направленных на отражение деструктивных информационных воздействий, реализуемых конфликтующей стороной в отношении Российской Федерации [184] (2005).

информационная безопасность вооруженных сил — состояние защищенности информационных ресурсов вооруженных сил от воздействия информационного оружия[24] [13] (2012).

[24] Приложение № 1 к «Соглашению между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области международной информационной безопасности», Екатеринбург, 2008.

международная информационная безопасность — состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве[24] [13] (2012).

система деятельности в информационном пространстве — система, опирающаяся на концептуальную систему принципов и правил, а также меры доверия между Вооруженными Силами Российской Федерации и их зарубежными партнерами.

Совокупная целенаправленная реализация принципов, правил и мер доверия призвана обеспечить эффективное сдерживание, предотвращение и разрешение межгосударственных или внутригосударственных противоречий с применением информационного оружия.

При этом совокупность взаимосвязанных принципов определяет ориентиры, в наибольшей степени способствующих достижению целей эффективного использования информационного пространства в интересах решения поставленных задач. Правила раскрывают практический механизм реализации действия данных принципов в интересах сдерживания, предотвращения и разрешения военных конфликтов в информационном пространстве. Реализация мер доверия в свою очередь способствует повышению открытости межгосударственных отношений, а также стабильности и предсказуемости военной деятельности в информационном пространстве.

Подробно сущность принципов, правил и мер доверия изложена в **Концептуальных взглядах на деятельность Вооруженных Сил Российской Федерации в информационном пространстве**, размещенных на сайте Министерства обороны Российской Федерации. Остановимся на наиболее принципиальных положениях этого документа.

1) Деятельность Вооруженных Сил Российской Федерации в информационном пространстве главным образом нацелена на сдерживание и предотвращение военных конфликтов в информационном пространстве.

2) В случае развязывания военного конфликта в информационном пространстве его разрешение будет осуществляться в первую очередь путем переговоров, примирения, обращения к Совету Безопасности ООН, региональным органам или иными мирными средствами.

3) Решение глобальной проблемы противодействия угрозе развязывания информационных войн, распространения и применения ин-

формационного оружия должно осуществляться на основе широкого международного сотрудничества.

4) Вооруженные Силы Российской Федерации в целях повышения прозрачности и предсказуемости военной деятельности в информационном пространстве будут стремиться к установлению следующих мер доверия:

— обмен национальными концепциями обеспечения безопасности в информационном пространстве;

— оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации;

— консультации по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность сторон, и сотрудничество в отношении урегулирования конфликтных ситуаций военного характера.

В заключение следует отметить, что главной целью деятельности Вооруженных Сил Российской Федерации в информационном пространстве является стремление к укреплению обороноспособности государства, сдерживанию и предотвращению военных конфликтов, развитию военного сотрудничества, а также к формированию системы международной информационной безопасности в интересах всего мирового сообщества [13] (2012).

2.1.6. Китайская стратегия ведения информационной войны

концепция информационной войны — термин был впервые введен в Китае в 1985 году ведущим китайским теоретиком Шэнь Вэйгуаном.

Китайская система взглядов на ведение информационной войны включает уникальные представления о войне вообще, основанные на современной концепции «народной войны», 36-ти стратегемах великого Сунь-Цзы, а также местных взглядах о том, как воевать на стратегическом, оперативном и тактическом уровне. Многое из этого подхода имеет отношение к акценту на обман противника, войну знаний и поиск асимметричных преимуществ над противником.

В основе теоретических подходов китайских специалистов в области информационного противоборства лежат взгляды древнекитайского военачальника и философа Сунь-Цзы, который первым обобщил

опыт информационного воздействия на противника. В своем трактате «Искусство войны» он писал: «Во всякой войне, как правило, наилучшая политика сводится к захвату государства целостным; разрушить его значительно легче. Взять в плен армию противника лучше, чем ее уничтожить... Одержать сотню побед в сражениях — это не предел искусства. Покорить противника без сражения — вот венец искусства». Сунь-цзы объясняет важность владения информацией и приемами дезинформации противника для манипулирования его состоянием и действиями: «Если я покажу противнику какую-либо форму, а сам этой формы не буду иметь, я сохраню цельность, а противник разделится на части».

Современная концепция ведения информационной войны начала разрабатываться в Китае в конце 80-х годов XX столетия. Под информационной войной понимались действия (политические, экономические, культурные, технологические и др.) по захвату глобального информационного пространства и созданию защитной информационной границы Китая. К основным ее элементам китайские теоретики относили теоретическое устрашение; противостояние информационных потенциалов; конкуренцию информационных стратегий; повышение информатизации войск (искусственный интеллект); экономическую информационную агрессию; культурную информационную агрессию; информационную войну умов, где главный метод — мирное устрашение, а главный объект — психология.

Неизбежность будущего геополитического столкновения с США требует от китайского руководства необходимости тщательно подготовиться к информационным операциям в современных условиях. И китайцы взяли на вооружение информационную концепцию начальника Генерального штаба Вооруженных Сил СССР маршала Н.В. Огаркова (она не была воспринята в СССР), а также древние китайские национальные технологии.

Основной вывод американских военных экспертов сводится к тому, что существующая сегодня в Китае концепция информационной войны это не 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.

Если Китай намеревается победить, не вступая в открытое противоборство, то он в ближайшие годы будет тщательно придерживаться выбранной линии подкупа, запугивания, заимствования и кражи каждого возможного преимущества, но не противопоставляя при этом себя Западу и не идя на открытую конфронтацию.

Анализ открытой китайской литературы позволяет выделить ряд базовых положений китайской концепции информационной войны: атаки на компьютерные сети; информационные операции; экономические операции; высокоточные удары и направленные акции. К наиболее часто описываемым целям возможной войны относятся: преимущество национальной безопасности; экономическое преимущество; финансовая выгода; политическое влияние; изменение политики. В перспективе можно ожидать тесного переплетения всех четырех инструментов национальной мощи: вооруженных сил (преимущество национальной безопасности), экономики (финансовая выгода), дипломатии/политики (изменение политики) и информации (политическое влияние). Таким образом, любые средства, которые увеличивают национальную мощь, рассматриваются китайскими стратегами в качестве средств противоборства [144] (2008).

информационная война[10] — несмотря на отсутствие общепринятого, официального определения понятия «информационная война», китайские военные эксперты уже давно оперируют им. В данном вопросе они широко используют наработки иностранных, в частности американских, военных специалистов и выделяют шесть аспектов в содержании этого понятия: разведка военного, экономического, политического и культурного потенциала противника и блокировка аналогичных действий с его стороны; разрушение (подавление) информационной составляющей его систем боевого управления и связи и защита своей; обеспечение беспрепятственного доступа к глобальным информационным системам и недопущение к ним противника; широкое использование АСУ как средства информационного обеспечения любых видов боевой деятельности; создание гибкой и мобильной базы данных; компьютерное воспроизводство реального поля боя. Считается, что информационная война включает также боевые действия с участием современных информационно насыщенных средств ведения боя.

Предполагается создание специальных боевых формирований, предназначенных для захвата и контроля информации, применения всех видов информационного оружия, подавления (нейтрализации) информационных систем противника, введения его в заблуждение и противодействия ему.

Военные аналитики КНР, формулируя понятие «информационная война», трактуют его в узком и широком смысле. В узком смысле информационная война — это полевая информационная война, т.е. боевые действия в сфере управления войсками. Сюда входят активное использование средств разведки, мероприятия по введению противника в заблуждение и оперативной маскировке, психологические операции, последовательное поражение его информационных систем, систем боевого управления и связи, а также действия по защите своих аналогичных систем.

В широком смысле информационная война — это крупномасштабные боевые действия с преобладанием информационной составляющей, характеризующиеся применением специально предназначенных для ее ведения воинских формирований и высокоточного оружия. Если основным средством достижения успеха на поле боя в XX веке были танки, то в будущем им станет компьютер. Это, в свою очередь, подразумевает применение компьютерных вирусов, способных разрушать программное обеспечение технических средств органов боевого управления и связи, инициировать сбои в системах управления и наведения высокоточного оружия и тем самым значительно снижать боевой потенциал противника. Война с широким использованием высокоточного оружия потребует существенного увеличения скорости добывания разведданных, времени предупреждения об ударах противника, улучшения взаимодействия командиров всех степеней, повышения маневренности войск, а значит, и эффективности всех видов информационного обеспечения. Самолеты, танки, корабли и ракеты, изготовленные с применением технологии «стелс», станут основной боевой техникой войск. Боевые действия с их участием, скорее всего, будут напоминать соревнование в быстроте обнаружения и уничтожения и характеризоваться высокой интенсивностью и скоротечностью.

Китайские военные эксперты пристальное внимание уделяют зарубежным разработкам в области ведения информационной войны. Как и западные военные специалисты, они полагают, что информационная война не есть в прямом смысле война на поле боя, подготовкой к которой служат многочисленные учения и маневры войск. Вооружен-

ные конфликты последнего времени побудили их выделить несколько характерных черт, присущих информационной войне.

Во-первых, «прозрачность» поля боя. Привычная «горячка боя» уступает место «хирургическим» методам работы подразделений информационной войны. Оператор компьютера может осуществлять непрерывный контроль за ситуацией, наблюдать отображаемое на дисплее расположение своих войск и войск противника, его объекты, концентрацию и перемещение его сил.

Во-вторых, общая координация действий войск посредством создания единого канала управления для всех боевых подразделений и подразделений тылового обеспечения. Все оперативные функции указанных формирований (разведка, управление, связь) в этом случае сводятся в единую систему. Например, оператор информационного центра, имея данные о количестве, составе и координатах выявленных целей противника, производит расчеты для распределения их по средствам поражения, определяет количество необходимых боеприпасов и т.д.

В-третьих, ведение боевых действий в реальном масштабе времени, т.е. немедленное реагирование на изменение боевой обстановки.

В-четвертых, точность ударов, отличающихся своеобразной чистотой и аккуратностью, подобной работе скальпеля хирурга.

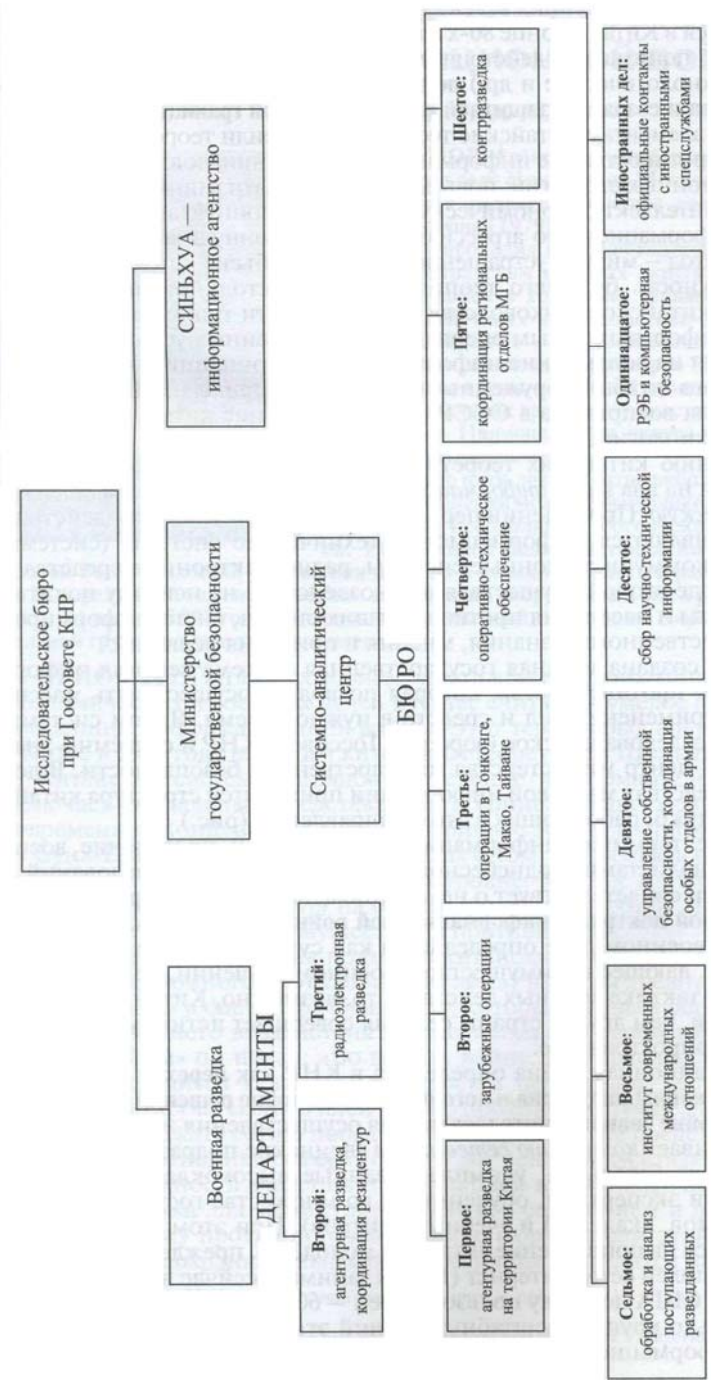
Для победы в информационной войне необходимо оснащение вооруженных сил передовыми информационными технологиями [69] (1999).

система ведения информационного противоборства — государственная система в Китае, которая позволяет осуществлять массированное применение сил и средств в нужное время.

Ядром системы являются исследовательское бюро при Госсовете КНР и системно-аналитический центр министерства государственной безопасности. В доступных средствах массовой информации приводится структура китайских спецслужб, работающих в этом направлении (рис. на с. 115) [144] (2008).

информационная война в КНР — переход от механизированной войны индустриального общества к войне решений и стиля управления, войне знаний и интеллекта.

Для осуществления этого перехода Китай развивает концепцию сетевых сил [144] (2008).



Структура спецслужб Китая, работающих в системе ведения информационного противоборства

информатизированная война — война, ведущаяся на «информационном» театре военных действий, «информатизированными» воинскими формированиями (как основная военная сила), «информатизированными вооружениями и военной техникой», в том числе информационным оружием как основным средством вооруженной борьбы [144] (2008).

сетевые силы — воинские подразделения численностью до батальона, укомплектованные высококлассными компьютерными экспертами, обученными во множестве государственных университетов, академий и учебных центров [144] (2008).

2.2. Информационная борьба

информация в вооруженной борьбе — абсолютизация роли информации в современных военных конфликтах ведет к искажению их сущности и основного содержания вооруженной борьбы.

Вооруженная, информационная и другие виды борьбы являются существенно отличающимися друг от друга структурными элементами военного конфликта, имеют свои цели, сущность и содержание, ведутся собственными силами и средствами. Поэтому утверждение о том, что в будущем «вооруженная борьба будет пронизана разветвленным информационным противоборством», представляется не соответствующим не только положениям Военной доктрины страны, но и объективной реальности.

Информация всегда играла обеспечивающую роль и могла иметь решающее значение только при прочих равных или сопоставимых условиях, к которым в вооруженной борьбе, прежде всего, относили наличие у противоборствующих сторон оружия и войск, способных его применять.

Информация пока не стала средством, способным воздействовать на человека так же эффективно, как современные виды оружия.

Информация может оказывать определенное воздействие на отдельного человека и на массы людей, результативность которого сегодня оценивается относительно невысоко.

Так, по мнению ученых Академии военных наук России, «ведение победоносной информационной войны представляется пока трудно-разрешимой задачей... В настоящее время мы наблюдаем лишь попытки внедрения средств гарантированного воздействия на индивиду-

альное и массовое сознание». Следует уточнить, что в данном случае авторы имеют в виду именно те информационные войны, которые ведутся в обществе на протяжении тысячелетий и в которых в качестве основного воздействующего фактора, влияющего на ход и исход событий, служит не что иное, как информация [163] (2008).

информационная борьба[1] — 1) в классическом понимании — использование каждой из противоборствующих сторон как ложной, так и правдивой, но интерпретированной в выгодном для себя свете информации в целях навязывания другой стороне объективно невыгодных ей решений.

Ее содержание включает: распространение правдивой информации, характеризующей обстановку в невыгодном для другой стороны свете; распространение заведомо ложной информации, не соответствующей реально складывающейся обстановке; демонстративные действия, способствующие введению противостоящей стороны в заблуждение относительно своих истинных намерений или же создающие у нее определенное представление о степени реальной угрозы, возможном неблагоприятном для нее варианте развития событий; имитацию, направленную на достижение целей дезинформации; комплексное противодействие противостоящей стороне в получении достоверной информации.

Именно такая информационная борьба ведется на протяжении всего существования человечества. Сущность и цели этой борьбы остаются неизменными, совершенствуются лишь средства, содержание, формы и способы ее ведения в различных сферах общественной жизни. В области военного искусства сущность подобной борьбы конкретно выражается во введении в заблуждение (обмане) противника, в результате чего достигаются внезапность действий своих войск и снижение эффективности действий противника. Обман противника — не отдельный вид борьбы, а внутренняя составляющая вооруженного противоборства. Он является составной частью оперативной маскировки (в современной ее трактовке), непосредственно связан с процессом комплексного поражения противника, осуществлением маневра, другими действиями войск (сил). Обманные действия (мероприятия) должны быть оригинальными и проводиться непрерывно при подготовке операции (боя) и ее ведении.

Из-за некорректной трактовки роли информационной борьбы вместо развития теории вооруженной борьбы делаются попытки все

свести к совершенствованию форм и способов информационной борьбы. При этом на нее возлагается решение задач, которые традиционно относятся к тем или иным видам оперативного (боевого) обеспечения, что вносит сумятицу в военную теорию.

Например, попытка планировать в рамках информационной борьбы комплексное поражение противника, мероприятия по его обману, а также по защите своих войск (сил) значительно усложняет этот процесс. Во-первых, происходит неизбежное дублирование мероприятий, содержащихся в различных планах, что ведет к нерациональному использованию сил и времени. Во-вторых, качество подобного плана не может быть достаточно высоким, так как он разрабатывается небольшой группой лиц, которые, естественно, не являются универсалами, специалистами в области применения самых различных средств борьбы. В-третьих, целевая направленность плана такой информационной борьбы настолько широка, а силы и средства, как и способы их применения, настолько разнообразны, что раскрыть их с требуемой степенью детализации и обеспечить тем самым согласованность в действиях не представляется возможным. Вследствие же его прямой зависимости от других планирующих документов он обречен быть постоянно «отстающим». В условиях, когда требуется быстрая реакция на изменения обстановки, своевременная корректировка задач и способов их выполнения, на основе такого плана нельзя обеспечить надежное управление войсками (силами) в операции (бою).

2) в настоящее время — проведение мероприятий по захвату и удержанию информационного превосходства над противником (или снижению его информационного превосходства) при подготовке и в ходе военных действий.

Предполагается, что информационного превосходства можно достичь, снизив до необходимого уровня информационный ресурс противника. При такой трактовке под информационным ресурсом следовало бы подразумевать нечто материальное, ибо снижение какого-либо ресурса предполагает нанесение ущерба тем или иным материальным средствам. Однако в этом отношении единства во взглядах на сегодняшний день нет [162] (2002).

информационная борьба[2] — по мнению китайских теоретиков, подразделяется на два вида: информационно-техническую и информационно-психологическую. При ведении первой главными объектами воздействия и защиты являются информационно-технические системы

(системы связи, телекоммуникационные системы, радиоэлектронные средства и т.п.), а в ходе второй осуществляется воздействие на психику политической элиты и населения противостоящих сторон, системы формирования общественного сознания, мнения и принятия решений [144] (2008).

информационная борьба[3] — часть отношений и форма борьбы сторон, каждая из которых стремится нанести противнику поражение (ущерб) посредством информационных воздействий на его информационную сферу, парируя или снижая такое воздействие с его стороны.

Информационная борьба может вестись по двум направлениям: разрушение информационных (радиоэлектронных, компьютерных) сетей и несанкционированный доступ к информационным ресурсам противника, а также информационно-психологическое воздействие на население и личный состав вооруженных сил противоборствующих сторон [82] (2016).

информационная борьба[4] — использование специальных способов и средств для воздействия на информационную среду противостоящей стороны, а также защиты собственной в интересах достижения поставленных целей.

Ввиду специфичности информационная борьба является и самостоятельным видом, и составным элементом любой другой разновидности борьбы (вооруженной, идеологической, экономической и т.п.). Она ведется постоянно, как в мирное, так и в военное время. Масштабы информационной борьбы настолько грандиозны, что ее подготовка не может быть спонтанной. Она должна носить плановый, систематический характер, основанный на глубоком знании законов и закономерностей информационной борьбы [124] (1997).

информационная борьба[5] — имеет целью завоевание и удержание информационного превосходства над противником при подготовке и в ходе ведения операций (боевых действий). Это предполагает обеспеченность более полной, точной, достоверной и своевременной информацией об обстановке, чем органы управления войсками и оружием противника, и возможность системы управления реализовать это преимущество в боевых действиях войск (сил) [171] (1997).

информационная борьба[6] — основной ее целью является завоевание информационного превосходства в процессе вооруженного противоборства [183] (1998).

информационная борьба[7] — комплекс мероприятий информационного обеспечения, информационного противодействия и информационной защиты, проводимых по единому замыслу и плану в целях захвата и удержания информационного превосходства над противником при подготовке и в ходе военных (боевых) действий.

Конечная цель информационной борьбы состоит в достижении информационного превосходства над противником, т.е. такого положения в информированности своих органов управления войсками и оружием, при котором они обеспечены более полной, точной, достоверной и своевременной информацией об обстановке, чем соответствующие органы управления противника [110] (1996).

информационная борьба[8] — система, включающая три составляющих элемента: информационное обеспечение функционирования своих боевых систем, информационное противодействие функционированию боевых систем противника и информационную защиту своих боевых систем от информационного противодействия возможного противника [185] (2008).

информационное воздействие[1] — воздействие с помощью информации, но не воздействие на информацию.

Воздействие с помощью информации может оказываться только на человека, так как она в виде сведений может восприниматься только человеком (не будем принимать во внимание животный мир). Отсюда следует, что информационная борьба (при соответствии понятия сущности данного явления) не может включать в себя какого бы то ни было технического (силового) аспекта. В этой борьбе информация используется как фактор воздействия на индивидуальное и общественное сознание и одновременно как средство защиты от такого воздействия [163] (2008).

информационное воздействие[2] — организованное применение сил и средств информационной борьбы для решения задач по завоеванию (поддержанию) информационного превосходства над противником [112] (1997).

информационное превосходство[1] — полная осведомленность о противнике и его действиях, способность эффективно управлять своими войсками (силами), системами вооружения и военной техникой, возможность обеспечить их результативное применение, в полной мере используя современные информационно-коммуникационные технологии [153] (2009).

информационное превосходство[2] — способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя действиям противника в том же направлении.

Оно может быть также определено и как способность назначить и поддерживать такой темп проведения операции, который превосходит темп противника, позволяя доминировать во все время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях [212] (2012).

информационное превосходство[3] — абсолютно обязательный инструмент опережения противника в быстроте нашего реагирования на складывающуюся в условиях боя (операции) боевую обстановку [12] (2011).

информационное превосходство[4] — способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, не давая противнику делать то же самое [105] (2011).

информационное превосходство[5] — не поступление информации в большом количестве, а более высокая степень осознания, более глубокое, соответствующее обстановке понимание ситуации на поле боя и более точное уяснение своих преимуществ и недостатков в системе управления противника.

Такое информационное превосходство в технологическом плане достигается внедрением новых систем управления, слежения, разведки, контроля, компьютерного моделирования и информационной войны (борьбы с системами боевого управления противника) [57] (2006).

информационное превосходство[6] — завоевание и поддержание наиболее благоприятной обстановки в информационной сфере для активных действий своих сил и средств, привлекаемых для решения задач информационного противоборства, без эффективного противодействия со стороны противника. Указанная трактовка «информационного превосходства», на наш взгляд, имеет слишком абстрактный ха-

рактер, не раскрывает физическую сущность этого явления, а, следовательно, не выводит на слагаемые превосходства и пути его достижения в операциях (боях).

Информационное противоборство ведется в информационной сфере, охватывающей все процессы, связанные с добыванием, сбором информации, ее обработкой, хранением и представлением в требуемом виде потребителям.

Сущность информационного превосходства заключается в наличии явного преимущества у одной из противоборствующих сторон в оперативности (быстроте) и качестве (объеме, точности, достоверности и рациональности формата представления данных) информационного обеспечения как принимаемых решений, так и выполнения задач подчиненными.

Под термином «информационное превосходство» в армии США понимается такое состояние, когда одна из противоборствующих сторон обладает более полной и точной информацией. Американские военные специалисты планируют достичь информационного превосходства за счет оснащения войск эффективными системами разведки и средствами передачи информации центрам управления и огневого поражения [78] (2003).

информационное превосходство[7] — оперативное преимущество, получаемое от способности сбора, обработки и распространения непрерывного потока информации в процессе эксплуатации или от лишения противника возможности сделать то же самое[25].

При этом разработчики Joint vision 2020 полагают, что информационное превосходство достигается или в **небоевых ситуациях**, или при отсутствии четко определенных противников, когда дружественные силы имеют сведения, необходимые для выполнения оперативных задач [123] (2014).

информационное превосходство[8] — главной целью проведения «информационных операций» ставится завоевание информационного превосходства американскими вооруженными силами над противником, которое имеет не обеспечивающее, а оперативное значение.

Предполагается, что информационное превосходство будет достигнуто за счет способности собирать, обрабатывать и распространять

[25] The Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 2008.

непрерывный поток информации, одновременно лишая противника возможности делать то же самое или используя его информацию в своих интересах. В ходе «информационных операций» планируется активно влиять в нужном направлении на принятие и реализацию решений противником, а также защищать процесс принятия и реализации решений американским военным руководством в различных условиях обстановки. Подчеркивается, что при наличии информационного превосходства объем и содержание информации, которой располагают органы управления, позволит им правильно оценивать обстановку, предвидеть развитие событий и своевременно принимать и реализовывать более эффективные решения, чем противник [113] (2008).

информационное превосходство ВС РФ — осуществляется в рамках комплексных программ, которые направлены на решение следующих основных задач:

1) Качественное улучшение способности к организации взаимодействия систем, органов военного управления, войск (сил), боевых платформ и отдельных военнослужащих в **едином информационном пространстве** за счет совместного использования единых сведений, данных и информации для решения стоящих задач.

2) Обеспечение информационного превосходства и возможности в мирное и военное время проведения своевременных информационных операций (действий, акций) [212] (2012).

системы информационного обеспечения боевых действий (СИО БД) — системы, создаваемые для получения изначального информационного превосходства над противником.

В их основу положено сложное сочетание четырех главных процессов: добывание (получение) информации, ее автоматизированная оперативная обработка, передача по каналам связи и использование потребителями (органами управления и исполнительными элементами) для эффективного управления войсками и применения оружия в бою (операции) [128] (2013).

2.2.1. Информационная борьба в военных конфликтах

информационная борьба в мирное время — носит скрытный характер. Ее основным содержанием является ведение разведыватель-

ных и политико-психологических действий по отношению к противнику, а также осуществление мероприятий по обеспечению собственной информационной безопасности. Все возрастающую роль на этом этапе играют средства специального программно-математического воздействия на информационный ресурс технических систем противника. В данный период могут также решаться задачи по созданию, развитию, поддержанию в требуемых степенях боевой готовности и отработке планов эффективного боевого использования информационных ресурсов своих войск (сил), а также по своевременному и достоверному вскрытию и нейтрализации информационных воздействий противника [171] (1997).

информационная борьба в угрожаемый период — добавляет задачи, решаемые в интересах обеспечения требуемой эффективности планируемых операций (боевых действий). В полном объеме развертывается инфраструктура системы управления планируемой для боевых действий группировки войск (сил) с учетом обеспечения ее максимальной скрытности.

К основным особенностям ведения информационной борьбы в этот период можно отнести: предельную ограниченность в использовании сил, средств и способов информационного воздействия на противника; соблюдение существующих норм международного права (например, на запрет радиоэлектронного подавления определенных частот и систем, предусмотренных Уставом Международного союза электросвязи и Регламентом радиосвязи); тесное взаимодействие различных силовых ведомств и федеральных структур при проведении мероприятий информационной борьбы [171] (1997).

информационная борьба с началом военных действий — решает следующие основные задачи: массированное воздействие на информационный ресурс группировки противника и предотвращение снижения боевых возможностей своих войск (сил), эффективности применения ими вооружения и военной техники из-за использования противником аналогичных средств; проведение мероприятий по снижению уровня морально-психологической устойчивости войск противника и обеспечению нейтрализации информации, воздействующей на морально-психологическое состояние своего личного состава; ведение информационно-разведывательной деятельности и обеспечение скрытности важнейших мероприятий своих войск в ходе подготовки и проведения операций (боевых действий). При проведении мероприя-

тий информационной борьбы в данный период чрезвычайно важно не допустить случайного воздействия своих средств на объекты собственной информационной инфраструктуры [171] (1997).

2.2.2. Теория информационной борьбы

цель информационной борьбы — обеспечение необходимой степени собственной информационной безопасности и максимальное снижение уровня информационной безопасности противостоящей стороны [124] (1997).

теория информационной борьбы — система знаний о характере, законах, закономерностях, принципах, формах, способах ее подготовки и ведения.

Изучение всех аспектов информационной борьбы и решение на этой основе конкретных вопросов не может осуществить какая-либо одна наука. Для исследования проблем в рассматриваемой области требуются объединенные усилия многих наук, особенно военной, которая занимает ведущее место в системе знаний об информационной борьбе.

Таким образом, у различных отраслей знаний, изучающих информационную борьбу, один объект познания — информационная борьба. Предметы же изучения различные. Они определяются спецификой каждой науки и ее способностью исследовать лишь какую-то одну сторону или часть объекта познания. В целом же предметом теории информационной борьбы следует считать систему законов, закономерностей, принципов, форм, способов ее подготовки и ведения [124] (1997).

структура теории информационной борьбы — должна включать общие основы, теорию поражения информации и теорию защиты информации [124] (1997).

основные задачи информационной борьбы — поражение объектов информационной среды противостоящей стороны и защита собственной информации [124] (1997).

категории теории информационной борьбы — фундаментальные понятия, отражающие наиболее общие, существенные предметы, процессы и свойства информационной борьбы.

Следует различать общие и частные категории. Общие имеют отношение ко всем отраслям теории. Главные из них «информация» и «информационная борьба». Частные формируются в составных частях теории информационной борьбы. Так, теория защиты информации имеет свои категории, например, «защита информации» и «информационная безопасность», теория поражения информации — свои, например, «поражение информации».

Система категорий теории информационной борьбы чрезвычайно важна. Она отражает глубинные характеристики наиболее существенных явлений информационной борьбы. Объективность содержания и высокий уровень обобщения превращают категории в одну из основ логического построения теории информационной борьбы. Категории выполняют важные познавательные функции. Выступая в качестве своеобразных инструментов исследования, они помогают систематизировать, углублять и развивать наши знания, а будучи взаимосвязанными, взаимообусловленными и целенаправленными, образуют логический каркас военно-теоретической мысли. Они отражают различные стороны информационного противоборства, но, взятые в совокупности, дают целостную характеристику таких сложных явлений, как война, информационная борьба, информационная безопасность и т.п. Категории и выражающие их термины обеспечивают процессы обучения и обмена научной информацией, единство понимания тех или иных явлений, что особенно важно для практики. Значение категорий тем больше, чем объективнее, глубже и точнее они отражают процессы информационной борьбы [124] (1997).

закон информационной борьбы — существенное, необходимое, устойчиво повторяющееся отношение, характеризующее упорядоченность строения и функционирования, тенденции изменения и развития тех или иных явлений информационной борьбы.

Законы информационной борьбы представляют собой более или менее точное отражение в сознании людей тех объективных связей и отношений, которые существуют и действуют в информационном пространстве. Их выявление и познание только начинается. Будучи познаны, отражены в нашем сознании, описаны, они становятся основой для практической деятельности по подготовке и ведению информационной борьбы [124] (1997).

принципы информационной борьбы — общие научно обоснованные положения, правила, рекомендации по подготовке и ведению информационной борьбы, руководству ее силами и средствами.

Понятие «принцип» близко по содержанию к понятиям «закон» и «закономерность». Их общность состоит в том, что все они отражают существенные, необходимые, повторяющиеся связи, отношения действительности. Однако принцип не только отражает объективную связь, но и предписывает, как следует действовать в конкретных условиях для достижения той или иной цели. В нем выражается единство объективного и субъективного.

Содержание и масштабы задач информационной борьбы предполагают наличие множества принципов информационной борьбы. Военная наука, учитывая характер законов войны и информационной борьбы, руководствуется прежде всего принципами, вытекающими из законов материалистической диалектики, из общих законов и закономерностей социального развития. Вместе с тем она вырабатывает свои специфические принципы, отражающие главным образом закономерности информационной борьбы [124] (1997).

закономерность информационной борьбы — подчиненность закону или указание на то, что в основе познания какого-либо явления информационной борьбы лежит один или несколько законов.

Понятие «закономерность» более предпочтительно в тех случаях, когда связи, повторяющиеся отношения информационной борьбы недостаточно выражены количественно. Информационные отношения нередко связаны с подобными явлениями [124] (1997).

2.2.3. Составные части информационной борьбы

информационное обеспечение управления войсками и оружием — комплекс мероприятий по добыванию информации о противнике и условиях противоборства (радиоэлектронной, метеорологической, инженерной обстановке и т.д.); сбору информации о своих войсках; обработке информации и обмену ею между органами (пунктами) управления в целях организации и ведения боевых действий.

Информация должна быть достоверной, точной и полной, а информирование — избирательным и своевременным.

Информационное обеспечение включает мероприятия по разведке, сбору информации, организации и осуществлению связи и инфор-

мационную работу штабов. В задачи разведки входит добывание информации о противнике и занимаемой им местности, элементах оперативного оборудования районов боевых действий и т.д. Сведения о подчиненных и взаимодействующих войсках поступают в результате сбора информации. Регистрация, анализ, обобщение, систематизация и другая обработка поступающих сведений осуществляются в ходе информационной работы штабов. Связь обеспечивает оперативный обмен информацией между органами управления войсками и оружием [110] (1996).

противодействие информационному обеспечению управления войсками и оружием противника (информационное противодействие) — включает мероприятия по блокированию добывания, обработки и обмена информацией и внедрению дезинформации на всех этапах информационного обеспечения управления противника.

Задачи информационного противодействия решаются путем проведения комплекса мероприятий, включающих маскировку, контрразведку, радиоэлектронное и огневое подавление информационных систем противника. Маскировка как вид оперативного (боевого) обеспечения нацелена на скрытие истинной и внедрение в сети данных противника ложной информации о своих войсках и планах действий. Контрразведка противодействует агентурной разведке противостоящей стороны. Огневое и радиоэлектронное подавление или захват элементов информационных систем ведет к нарушению управления войсками и оружием противника [110] (1996).

защита от информационного противодействия противника (информационная защита) — мероприятия, включающие действия по деблокированию информации, необходимой для решения задач управления, и блокированию дезинформации, распространяемой и внедряемой в систему управления.

Информационная защита повышает эффективность информационного обеспечения в условиях информационного противодействия противника.

Информационная защита включает мероприятия по контрольной разведке (доразведке), проверке информации, защите от огневого поражения (захвата) элементов информационных систем, а также по радиоэлектронной защите. Контрольная разведка (доразведка) осуществляется для подтверждения и уточнения ранее добытых сведений. При этом объединяются данные различных видов разведки. В отдельных

случаях возможна разведка боем, а также провоцирование противника на действия, которые раскрыли бы его возможности и намерения. Сведения о своих войсках подтверждаются или уточняются в ходе проверки информации, поступающей от подчиненных и взаимодействующих формирований [110] (1996).

2.2.4. Способы информационной борьбы

способы информационной борьбы — порядок и приемы применения сил и средств объединения (соединения, части, подразделения) для захвата и удержания информационного превосходства над противником при подготовке и в ходе боевых действий.

Способы информационной борьбы включают: вид и последовательность информационных воздействий на противника; объекты воздействий; состав сил и средств, выделяемых для ведения информационной борьбы, их оперативное построение (боевой порядок). Содержание способов отличается большим разнообразием. Последнее связано с тем, что одна и та же информация может быть сформирована и доведена до органов управления с помощью различных сил и средств.

Все способы информационной борьбы, на наш взгляд, делятся на три основные категории: силовые, интеллектуальные и комбинированные.

К категории **силовых** относятся способы, основанные на поражении объектов информационной борьбы различными видами оружия (обычного, радиоэлектронного, информационного). Применение силовых способов позволяет достичь информационного превосходства в количестве информации, необходимой для решения задач управления войсками (силами). **Интеллектуальные** способы нацелены на реализацию рефлексивного управления противником. Их применение позволяет достичь информационного превосходства в качестве информации, используемой для управления войсками (силами). К **комбинированным** относятся способы, обеспечивающие достижение информационного превосходства как в количестве, так и в качестве информации об обстановке.

Кроме того, в информационной борьбе (по аналогии с вооруженной) можно выделить две основные группы способов: наступательные и оборонительные.

К группе наступательных отнесем следующие способы: блокирование, отвлечение, сковывание, изматывание, инсценировку, дезинтег-

рацию, умиротворение, устрашение, провоцирование, перегрузку, внушение и давление.

К группе оборонительных можно отнести способы деблокирования и отождествления [112] (1997).

2.2.4.1. Наступательные способы информационной борьбы

способ блокирования информации — силовой способ информационной борьбы, сущность которого состоит в том, что на этапе подготовки и в ходе боевых действий путем проведения комплекса мероприятий информационного противодействия полностью или частично воспрещается добывание (сбор) информации об обстановке и обмен информацией в системах управления войсками и оружием противника.

Для реализации этого способа активно применяется огневое, радиоэлектронное и информационное поражение (подавление) элементов систем управления войсками (силами) и оружием противника [112] (1997).

способ отвлечения внимания — способ информационной борьбы, заключающийся в том, что на этапе подготовки боевых действий путем проведения комплекса мероприятий информационного противодействия стремятся создать реальную или мнимую угрозу для одного из уязвимых мест противника (на флангах, в тылу и т.д.) и тем самым убедить его в своем намерении действовать на одном из возможных направлений с целью отвлечь главные силы противника на решение второстепенных задач [112] (1997).

способ сковывания сил противника — разновидность способа отвлечения внимания, при применении которого у противника создается убеждение в наличии угрозы для одного из его уязвимых мест, предотвращение которой требует выделения части сил и средств [112] (1997).

способ изматывания — способ информационной борьбы, заключающийся в проведении комплекса мероприятий информационного противодействия с целью вынудить противника предпринять невыгодные или бесполезные действия и, как следствие, вступить в бой с растраченными ресурсами и пониженной боеспособностью. При этом

могут проводиться ограниченные боевые или отвлекающие действия [112] (1997).

способ инсценировки — способ информационной борьбы, состоящий в том, что на этапе подготовки боевых действий путем проведения комплекса мероприятий информационного противодействия противнику навязывается представление о наличии ложной угрозы для одного из его уязвимых мест (в тылу, на флангах и т.д.), предотвращение которой не требует выделения сил и средств. Это делается с той целью, чтобы противник заметил обман и его бдительность была бы усыплена. При возникновении настоящей угрозы он также примет ее за ложную и не сможет действовать в соответствии с реальной обстановкой [112] (1997).

способ дезинтеграции (раскола) — комплекс мероприятий информационного противодействия, позволяющих навязать противнику представление о необходимости действовать вопреки коалиционным интересам.

В этих целях может использоваться дезинформирование общественного мнения, а также формирование ложных представлений о военно-политической обстановке у глав государств, участвующих в конфликте. Кроме того, могут проводиться мероприятия, способствующие обострению реально существующих или искусственно формируемых противоречий в стане врага с целью снизить его военную и экономическую мощь.

Этот способ чаще применяется в дипломатии, чем в военном деле. Между тем в современных условиях вооруженные силы нередко используются в качестве аргумента, необходимого для решения политических задач в межгосударственных конфликтах [112] (1997).

способ умиротворения — навязывание противнику представления о нейтральной или союзнической позиции противостоящей стороны.

Сущность способа заключается в проведении комплекса мероприятий информационного противодействия, основной целью которых является создание у противника впечатления о том, что осуществляется не подготовка к боевым действиям, а плановая оперативная (боевая) подготовка или какие-либо иные мероприятия. Противник должен увериться в дружеских или мирных намерениях противостоящей стороны

и потерять бдительность. Втайне же планируется и готовится нападение на него при первом удобном случае [112] (1997).

способ устрашения противника — доведение до противника информации, создающей представление о превосходстве в чем-либо противоборствующей стороны, которого на самом деле может и не быть [112] (1997).

способ провоцирования противника — способ информационной борьбы, имеющий целью побудить противника к осуществлению каких-либо действий, выгодных противоположной стороне [112] (1997).

способ перегрузки — способ информационной борьбы, заключающийся в том, чтобы на этапе подготовки и в ходе боевых действий довести до противника такое количество противоречивой информации, которое перегружает его систему управления и вынуждает принимать и реализовывать решения в условиях повышенной неопределенности обстановки [112] (1997).

способ внушения — формирование и последующее использование информационного стереотипа поведения противостоящей стороны.

Для этого на этапе подготовки и в ходе боевых действий путем проведения комплекса мероприятий информационного противодействия до сведения противника доводится информация, обладающая юридической, нравственной, идеологической или иной силой, побуждающей его к осуществлению каких-либо действий, выгодных противостоящей стороне [112] (1997).

способ давления — доведение до общественного мнения порочащих противника сведений, вынуждающих государственные, межгосударственные, общественные и иные организации предпринимать действия, затрудняющие реализацию его замыслов [112] (1997).

2.2.4.2. Оборонительные способы информационной борьбы

способ деблокирования информации — проведение комплекса мероприятий информационной защиты в целях получения скрываемой или модифицированной противником информации. При этом могут

применяться все возможные методы, силы и средства, вплоть до проведения широкомасштабных боевых действий [112] (1997).

способ отождествления — проведение комплекса мероприятий информационной защиты, обеспечивающего сбор и сопоставление информации об одном и том же факте (явлении) от различных источников, что позволяет выявить и блокировать дезинформацию, распространяемую противником [112] (1997).

2.2.5. Формы ведения информационной борьбы

информационная операция[1] — совокупность согласованных по цели, задачам, месту и времени информационных воздействий, атак и сражений, проводимых по единому замыслу и плану для решения задач информационной борьбы на театре военных действий, стратегическом или операционном направлении [112] (1997).

информационная операция[2] — совокупность согласованных и взаимосвязанных по цели, задачам, месту и времени информационных воздействий на объект или группу объектов государственного или военного уровня противника, проводимых по единому замыслу и плану в мирное и военное время.

Информационные операции подразделяются на наступательные, оборонительные и специальные, проводимые как последовательно, так и одновременно.

Зарубежными экспертами выделяются следующие виды информационных операций: радиоэлектронная борьба; операции в компьютерных сетях; операции по оказанию информационного воздействия [148] (2008).

информационно-электронная операция — совокупность взаимосвязанных и согласованных по цели, задачам, месту, времени и способам ведения информационно-ударных сражений, информационно-огневых и информационных ударов, проводимых в целях дезорганизации системы управления войсками и оружием противника, нанесения поражения его информационным ресурсам.

В ходе операции «Буря в пустыне» наносились следующие виды ударов:

информационно-психологический — в целях дезинформации и введения противника в заблуждение;

психотропный — воздействие специальными средствами на психику людей;

радиоэлектронный — воздействие средствами радиоэлектронного подавления;

программно-компьютерный — воздействие на ЭВМ систем управления специальными разрушающими или искажающими программными средствами [41] (2014).

информационная операция[3] — совокупность согласованных и взаимосвязанных по целям, задачам, месту и времени информационных сражений, действий (акций) и ударов, проводимых для завоевания и удержания информационного превосходства над противником (или снижения его информационного превосходства) на театре военных действий или стратегическом (операционном) направлении.

Информационные операции могут быть наступательными и оборонительными.

Цели информационных операций достигаются решением следующих задач: информационным воздействием на противника, информационной защитой и эффективным использованием информационных ресурсов собственной группировки войск (сил). Информационная операция обычно проводится в рамках соответствующей общевойсковой, самостоятельной, совместной или специальной операции.

По масштабам информационные операции можно классифицировать как стратегические, оперативно-стратегические, оперативные и оперативно-тактические.

В некоторых условиях обстановки нельзя исключить возможности проведения в рамках информационной операции информационного сражения, в ходе которого решается одна из ее важнейших оперативных задач [183] (1998).

информационная операция[4] (ИО) — комплекс действий, проводимых в целях оказания деструктивного влияния на информацию и информационную систему противника при одновременной защите своей информации и информационной системы.

В прежних войнах информационные операции применялись эпизодически [9] (2005).

информационная операция[5] — воздействие на информацию противника, информационные системы и процедуру принятия им ре-

шения, а также действия при защите собственной информации, информационных систем и процедур принятия решения.

Исключены из обращения оказавшиеся сугубо теоретическими термины «наступательная информационная операция» и «оборонительная информационная операция». При этом сохранены как наступательная, так и оборонительная цели «информационной операции».

По мнению экспертов Пентагона, общим результатом успешного проведения любой «информационной операции» является повышение качества своей информации, используемой для управления войсками (силами) и снижение качества аналогичной информации противника, так как тем самым для своих органов управления создается возможность быстро принять более верное решение. При этом качество информации оценивается по семи основным критериям: точность, адекватность, своевременность, возможность использования, полнота, краткость и защищенность. Основные механизмы, используемые для воздействий на противника в рамках информационных операций, включают: оказание влияния, разрушение (дезорганизация), искажение (разложение) или захват (использование в своих целях).

В рамках «информационных операций» может выполняться в большем или меньшем объеме следующий комплекс задач:

уничтожить — причинить такой ущерб объекту воздействия, в результате которого он не сможет выполнить ни одну из своих функций и не будет подлежать восстановлению;

нарушить — прервать обмен информацией между соответствующими объектами воздействия;

подавить — снизить эффективность или работоспособность объекта воздействия;

воспретить — лишить противника возможности доступа к элементам информационного пространства;

обмануть — ввести в заблуждение должностных лиц противника, принимающих решения, путем манипулирования их восприятием реальной обстановки;

использовать (в своих целях) — обеспечить доступ к объектам противника в целях добывания информации или внедрения ложной или дезориентирующей информации;

повлиять — принудить противника к определенным действиям;

защитить — принять меры по противодействию разведке противника или захвату им важного объекта;

обнаружить — установить факт вторжения в информационные системы;

восстановить — возвратить элементы информационного пространства в их первоначальное состояние;

реагировать — ответить на информационную или физическую атаку противника или других субъектов.

В новой доктрине содержание «информационных операций» сужено до пяти основных составных элементов: радиоэлектронная борьба, психологические операции, безопасность операций, военный обман и компьютерные сетевые операции. Остальные элементы, ранее входившие в содержание «информационных операций», отнесены к обеспечивающим и сопутствующим действиям [113] (2008).

информационная операция[6] — комплексное применение информационных (не кинетических) и других средств в соответствии с замыслом операции с целью нарушения, искажения, срыва процессов принятия противником решений и защиты аналогичных процессов своих органов управления[26].

Тогда же были введены и новые категории операций в киберпространстве, включая и «стратегическую коммуникацию». Этот термин расширял возможности информационных операций и направлял их воздействие не только на противника, но также на союзников [5] (2014).

информационная операция[7] (ИО) — комплекс мероприятий по воздействию на людские и материальные ресурсы противоборствующей стороны с целью затруднить или сделать невозможным принятие ею верных решений с одновременной защитой своих информационных систем[27] [217] (2014).

специальная информационная операция — совокупность согласованных и взаимосвязанных по цели, задачам, месту и времени мероприятий, действий и акций войск (сил и средств), заключающихся в целенаправленном воздействии на объекты системы информационного обеспечения боевых действий группировки войск противника для

[26] Меморандум министра обороны США № 12401-10 от 25 января 2011 года.

[27] Доктрина «Информационные операции» (JP 3—13), утвержденная Комитетом начальников штабов США 13 февраля 2006 г.

завоевания информационного превосходства в определенный период, на отдельном направлении или во всей полосе операции [76] (2005).

наступательная информационная операция — имеет целью завоевание и удержание информационного превосходства над противником. В этой операции главные усилия направляются на дезорганизацию его систем управления войсками и оружием, а часть сил и средств обеспечивают устойчивость собственного управления. При этом все мероприятия, проводимые в рамках информационной борьбы, должны обеспечивать благоприятные условия для боевых действий своих войск (сил) [183] (1998).

оборонительная информационная операция — проводится в условиях подавляющего информационного превосходства противника и имеет цель снижение этого превосходства. В такой операции главные усилия сил и средств направляются на обеспечение информационной безопасности органов управления объединений и соединений, на защиту информации в системах управления. Часть сил и средств направляются на дезорганизацию управления войсками и оружием противника [183] (1998).

информационно-ударная операция (ИУО) — совокупность взаимосвязанных и согласованных по цели, задачам, месту, времени и способам ведения информационно-ударных сражений, информационно-огневых боев и информационных ударов, проводимых с целью дезорганизовать систему управления войсками и оружием противника, нанести поражение его информационным ресурсам.

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 [37] (2007).

информационное сражение[1] — совокупность различных информационных воздействий и атак, объединенных общим замыслом, проводимых специально выделенными силами и средствами и направленных на решение одной оперативной задачи информационной борьбы [112] (1997).

информационное сражение[2] — совокупность согласованных и взаимосвязанных по цели, задачам, месту и времени информационных действий и ударов.

В зависимости от масштаба и вида проводимой информационной операции в ней может быть одно или несколько информационных сражений, осуществляемых одновременно или последовательно.

В современной войне в ходе информационного сражения оперативная задача, на наш взгляд, может решаться без вторжения сухопутных войск на территорию противника. Успех при этом обеспечивается информационными действиями и ударами, которые вынуждают противника отказаться от запланированных им боевых действий [183] (1998).

информационные действия (акции) — совокупность согласованных по цели, задачам, месту и времени мероприятий, проводимых привлекаемыми для ведения информационной борьбы силами и средствами в течение определенного времени в заданном районе (направлении). В рамках информационных действий могут проводиться информационные удары.

Информационные действия (акции) можно классифицировать по видам (наступательные и оборонительные), масштабам (стратегические, оперативно-стратегические, оперативные, оперативно-тактические и тактические) и объектам воздействия (информационно-технические системы, морально-психологическое состояние личного состава и их комбинация).

К наступательным информационным действиям (акциям) относятся информационное воздействие (акция) и информационная блокада, к оборонительным — действия (акции) по информационной защите [183] (1998).

наступательное информационное воздействие (акция) — активное, целенаправленное, согласованное по задачам, месту и времени воздействие привлекаемых к ведению информационной борьбы сил и средств в течение определенного времени в заданном районе по отдельным информационным объектам системы управления противника или его информационного ресурса в целом.

При этом могут проводиться различные информационные удары. Информационные акции (например, манипулирование средствами массовой информации, культуры, искусства и др.) будут осуществляться в рамках информационного противоборства [183] (1998).

действия (акции) по информационной защите — согласованные по задачам, месту и времени применению привлекаемых для веде-

ния информационной борьбы сил и средств действия (акции) в целях обеспечения устойчивости функционирования системы управления войсками (силами) в условиях информационного воздействия противника [183] (1998).

информационная атака — совокупность активных информационных воздействий сил и средств отдельных подразделений на элемент или группу элементов информационных систем противника в целях решения частных тактических задач информационной борьбы [112] (1997).

информационный удар[1] — кратковременное мощное согласованное информационное воздействие сил и средств на наиболее важный элемент (элементы) системы управления противника для достижения решительных целей по завоеванию информационного превосходства (снижению информационного превосходства противника).

Информационные удары можно классифицировать по масштабам (стратегические, оперативно-стратегические, оперативные, оперативно-тактические, тактические), типам (радиоэлектронные, радиоэлектронно-огневые, компьютерные, специальные и комбинированные) и степени массирования сил и средств (избирательные, сосредоточенно-массированные и массированные) [183] (1998).

информационный удар[2] — кратковременное и мощное воздействие информационным оружием на информационный ресурс противника.

Такое воздействие может быть избирательным или специализированным на какой-либо вид информационного ресурса, а также массированным или комбинированным (по всему информационному ресурсу всеми видами информационного оружия).

Возможны следующие виды информационных ударов: информационно-психологический — с целью дезинформировать и ввести противника в заблуждение; психотропный — воздействие специальными средствами на психику людей; радиоэлектронный — воздействие средствами радиоэлектронного подавления; программно-компьютерный — воздействие на ПЭВМ системы управления противника специальными разрушающими или искажающими программными средствами [37] (2007).

2.2.5.1. Американская доктрина информационных операций

теория информационных операций — включена в основы современного американского военного искусства. В перспективе предполагается, что данная теория разовьется в самостоятельную отрасль военного искусства, базирующуюся на специальных органах, силах, средствах и обученных специалистах.

Вместе с тем руководство министерства обороны США признало, что действовавшая до сих пор теоретическая парадигма «информационных операций» оказалась эклектичной и практически плохо реализуемой, так как базировалась на идее объединения в содержании «информационных операций» 13 различных и слабо взаимосвязанных между собой областей деятельности. Отмечается, что эти области сближает между собой лишь то, что все они каким-либо образом связаны с военной информацией [113] (2008).

обеспечивающие действия информационных операций — защита от физического воздействия, контрразведка, физическое воздействие, информационная гарантия и «боевая камера».

Обеспечивающие действия прямо или косвенно влияют на эффективность задач, решаемых в ходе проведения информационных операций. Поэтому, по мнению американского военного руководства, они должны осуществляться комплексно и быть взаимосогласованы с основными составными элементами информационных операций [113] (2008).

физическое воздействие — огневое поражение информационных объектов или их захват, применяемые в качестве средства поддержки «информационных операций» [113] (2008).

информационная гарантия — меры защиты информационных систем, обеспечивающие их боеготовность и отказоустойчивость, а также целостность, подлинность и конфиденциальность информации [113] (2008).

боевая камера — относительно новый элемент обеспечения «информационных операций» видеоматериалами для их последующего распространения или иного использования при решении задач психологического воздействия [113] (2008).

сопутствующие действия информационных операций — связь с общественностью и гражданско-военные операции (совместные действия гражданских и военных органов), а также военная поддержка общественной дипломатии.

Считается, что они также вносят существенный вклад в «информационные операции» и должны интегрироваться и согласовываться с основными и обеспечивающими действиями. Вместе с тем в качестве важного требования выдвигается недопущение компрометации их главного назначения и правил проведения со стороны «информационных операций», что требует особой осторожности при планировании и проведении последних. Для этого специалисты по связям с общественностью и по совместным действиям гражданских и военных органов должны особенно тесно сотрудничать с органами планирования «информационных операций» [113] (2008).

органы разведки — основными их задачами являются добывание разведывательной информации о состоянии и характеристиках элементов информационного пространства, а также оценка хода информационных операций.

Появление этих относительно новых задач вкупе с ограниченностью имеющихся сил и средств вынуждает командующего, оперативные и разведывательные органы штаба работать совместно для того, чтобы четко определить разведывательные потребности подготовки и проведения «информационных операций» и обеспечить приоритетность их удовлетворения. В интересах добывания необходимой информации предусматривается тесное взаимодействие с правоохранительными и другими органами государственной власти [113] (2008).

информационные операции с психологическими целями — Вашингтон планирует в перспективе использовать следующие мероприятия в ходе ведения информационных операций:

официальные выступления в средствах массовой информации (СМИ) и международных организациях представителей американского истеблишмента с осуждением «нарушений прав человека» (abuses of human rights) за рубежом;

публичная поддержка оппозиции «репрессивных наций» (repressive nations), включая встречи с представителями оппозиции на высшем уровне в Белом доме, госдепартаменте и американских посольствах;

информационная поддержка «свободных и справедливых выборов» (free and fair elections), становления «гражданского общества» (civil society), а также свободы СМИ и свободы вероисповедания;

дискредитация представителей власти «репрессивных режимов» (oppressive regimes) путем публичного предъявления к ним претензий и объявления персональных санкций;

призывы в СМИ к членам международного сообщества не поддерживать «репрессивные режимы»;

объявление о создании коалиций с другими «демократическими нациями» (democratic nations) в целях «продвижения свободы, демократии и прав человека» (to promote freedom, democracy, and human rights) в определенных странах и регионах;

создание и укрепление неправительственных и других организаций, воздействующих на существующие международные организации, с тем чтобы использовать их потенциал для установления «демократии в регионах, которые испытывают в ней недостаток» (democracy charters in regions that lack them);

активная пропаганда американских ценностей через СМИ, расширение образовательных программ для иностранных студентов и ученых, поддержка частного сектора, увеличение каналов диалога и контрпропаганды, «чтобы пустить корни в сердцах и умах людей во всем мире» (to take root in the hearts and minds of people across the world).

Приведенный перечень мероприятий детализирует новое положение о ведении «информационных операций» в любых регионах мира в поддержку «общественной дипломатии» для продвижения американских внешнеполитических инициатив путем оказания влияния на иностранную аудиторию и систему формирования общественного мнения.

Отсюда со всей очевидностью следует, что в ходе проведения стратегического курса Вашингтона на дальнейшую «демократизацию» России (democratic progress in Russia) можно ожидать от него активизации применения всего рассмотренного выше арсенала средств современных «информационных операций» уже в мирное время. Тем более что проведение подобных «информационных операций» никак не регулируется действующими нормами международного права [113] (2008).

компьютерные сетевые операции — применяются для уничтожения, нарушения, подавления, обмана, воспрещения, использования и защиты информации и информационной инфраструктуры.

Компьютерные сетевые операции включают: компьютерные сетевые атаки, защиту компьютерных сетей и компьютерную разведку [113] (2008).

операции в компьютерных сетях — операции, к которым относятся, во-первых, операции по воздействию на компьютерные сети противника с целью дезорганизации, снижения эффективности их работы и невозможности использования или полного уничтожения, во-вторых, операции по защите компьютерных сетей своих ВС от воздействия на них противника, от взаимных помех работающих радиоэлектронных систем своих ВС и обеспечению безопасности и устойчивости работы сетей, и, в-третьих, операции по использованию компьютерных сетей противника с целью несанкционированного доступа к информационным ресурсам, извлечения из них и использования в своих интересах секретной информации, преднамеренного искажения и подмены контента для дезинформации [148] (2008).

компьютерная сетевая атака[1] — действия с использованием компьютерных сетей, предпринимаемые для нарушения, воспрещения, подавления и уничтожения компьютерной информации или самих компьютеров или компьютерных сетей [113] (2008).

компьютерная сетевая атака[2] [Computer Network Attack] — действия по нарушению, подавлению, уничтожению информации или воспрещению пользоваться информацией, находящейся в компьютерах и компьютерных сетях, или против самих компьютеров и компьютерных сетей[28].

Этот термин не синонимичен термину «кибератака», так как означает действия именно в сети, а не в киберпространстве и скорее всего является ее слагаемым [8] (2011).

защита компьютерных сетей — обнаружение несанкционированных действий противника в сетях, их анализ и реагирование на эти действия.

---

[28] Директива МО США № 0-3600.01.

Так как защита компьютерных систем обеспечивает безопасность не только от воздействия внешнего противника, но и от внутреннего несанкционированного использования, она является необходимым атрибутом проведения всех видов военных операций [113] (2008).

компьютерная разведка — добывание интересующих сведений из автоматизированных информационных систем или сетей противника.

Отмечается, что благодаря продолжающемуся расширению беспроводных сетей связи и внедрению в системы радиосвязи компьютерных технологий создаются предпосылки для последующей интеграции компьютерных сетевых операций и осуществления мероприятий радиоэлектронной борьбы [113] (2008).

2.2.5.2. Другие формы ведения информационной борьбы

информационная блокада — согласованное по задачам, месту и времени применение сил и средств в целях наиболее полного снижения возможностей противника по получению и использованию информации, необходимой для эффективного ведения операций (боевых действий). В рамках информационной блокады также могут проводиться информационные удары различного вида и масштаба.

Одним из основных способов достижения цели информационной блокады является радиоэлектронное блокирование [183] (1998).

компьютерный (программный) удар — согласованное по задачам, месту и времени внезапное массированное комплексное воздействие атакующих сил и средств специального программно-математического воздействия по объектам АСУ противника в целях срыва управления на отдельных направлениях (или с отдельных пунктов) на определенное время [183] (1998).

специальный удар — согласованное по задачам, месту и времени массированное комплексное морально-психологическое воздействие привлекаемых к ведению информационной борьбы сил и средств на личный состав (прежде всего на персонал органов управления) группировки противника в целях срыва (затруднения) управления на отдельных направлениях на определенное время [183] (1998).

2.3. Война в киберпространстве

кибернетика[1] — 1) наука об общих законах получения, хранения, передачи и переработки информации[29];

2) наука о системах и методах управления, т.е. об организации и реализации целенаправленных действий в машинах, живых организмах и обществе. Кибернетика занимается общими законами преобразования информации в сложных управленческих системах[30] [40, 41] (2012, 2014).

кибернетика[2] — наука об управлении, связи и переработке информации. Основной объект исследования — так называемые «кибернетические системы», рассматриваемые абстрактно, вне зависимости от их материальной природы. Кибернетика разрабатывает общие принципы создания систем управления и систем для автоматизации умственного труда[31].

Таким образом, ключевым элементом кибернетических систем является именно *информация*.

Очевидно, что границы области применения терминов с использованием части слова «кибер» лежат именно в информационной и управленческой сферах. Можно сказать, что объектом кибернетики являются все управляемые информационные системы. Видимо, следует также разделять «информационное» и «кибернетическое» пространства и уточнить их иерархию.

Кибернетическая сфера включает информационные и управленческие процессы. По этой причине можно, с одной стороны, понимать кибернетическое пространство как часть информационного пространства, ограниченную областью, связанной с информационными управленческими технологиями, а с учетом вышесказанного — в первую очередь с компьютерными информационными технологиями. С другой стороны, процессы приема, передачи и обработки информации (информационные процессы) являются составной частью процессов управления, по сути, кибернетических процессов. С этой позиции можно сказать, что информационное пространство является частью кибернетического [8] (2011).

---

[29] Советский Энциклопедический словарь. М.: Советская энциклопедия, 1980. С. 578.

[30] Ожегов С.И. Словарь русского языка. М.: Русский язык, 1986. С. 235.

[31] Большой энциклопедический словарь, Т. 1. С. 572.

военная кибернетика — одно из направлений кибернетики, изучающее общие закономерности управления войсками и оружием на основе единых для кибернетики понятий.

Это составило теоретическую базу для развития автоматизированных систем управления в Вооруженных Силах.

Отечественные ученые рассматривали военную кибернетику как науку, синтезирующую ряд следующих научных дисциплин: теорию исследования операции, теорию алгоритмов, теорию систем, теорию программирования для цифровых вычислительных машин, теорию автоматического регулирования, теорию связи и алгоритмов, теорию вероятностей, теорию программирования и математической логики [40] (2012).

киберпространство[1] — виртуальная обстановка, в которой цифровая информация обращается в компьютерных сетях[32].

Также существует определение, согласно которому киберпространство — своеобразная метафорическая абстракция, философская категория в компьютерной сфере, виртуальная реальность, которая представляет мир, как «внутри компьютеров», так и «внутри компьютерных сетей». При этом не следует отождествлять киберпространство и Интернет, хотя применительно к объектам (программам, сайтам и др. ресурсам) компьютерных сетей можно сказать, что они «расположены в киберпространстве». По аналогии все сетевые события происходят не в конкретной стране, городе или организации, а именно в киберпространстве. Термин также используется и в продуктах массовой культуры. Тем не менее киберпространство в настоящее время — объективная реальность и важный элемент современного общественного устройства, воспринимаемое как среда функционирования компьютеров и всего, что с ними связано.

Как и в традиционном пространстве, в киберпространстве можно воздействовать на кибернетические системы и объекты противника и поддерживать (защищать) свои аналогичные системы и объекты.

К примеру, США выводят защиту своей виртуальной территории в отдельную задачу. В середине 2009 года Сенат США официально признал кибернетическое пространство новой средой (domain) ведения боевых действий и определил целесообразность его объединения с космическим пространством в рамках выполнения задач на новом,

[32] JP 3-13 2006 г. и JP 1-02 2001 г.

«геоцентрическом театре военных действий» (Spherical Area of Operation) (возможные переводы — «сферическая область операций», «сферическое операционное пространство») [8] (2011).

киберпространство[2] [cyberspace] — глобальный домен в пределах информационного пространства, состоящий из взаимозависимой сети информационных технологических инфраструктур, включая Интернет, телекоммуникационные сети, компьютерные системы, а также встроенные в них процессоры и контроллеры[33].

Во второй половине первого десятилетия XXI века в американском военно-политическом лексиконе появились два взаимосвязанных понятия: «киберпространство» и «операции в киберпространстве». Они относительно быстро составили понятийный аппарат нового раздела американской теории военного искусства, который условно можно назвать «организация и ведение операций в киберпространстве».

Благодаря наличию киберпространства обеспечивается высокая маневренность войск (сил), которая зависит от качества информации, используемой при выработке решений, и скорости ее передачи, приближающейся к скорости света. С одной стороны, киберпространство создает благоприятные условия ВС США для эффективного ведения военных действий на суше, море, в воздухе и в космосе. С другой — оно дает возможность различного рода субъектам, в том числе и геополитическим противникам США, относительно легко получать доступ к американским информационным ресурсам и системам. Характерными особенностями киберпространства, отличающими его от традиционных геофизических видов пространств ведения военных действий, являются его искусственное происхождение, инновационность и изменчивость [161] (2011).

киберпространство[3] — составная часть и материальная основа другого, более общего, информационного пространства, представляющая собой совокупность информации и информационной инфраструктуры.

При этом каждый из этих элементов боевого пространства (в широком смысле) обладает своими уникальными особенностями. Так, в

[33] Joint Operations, Joint Publication 3-0, 17 September 2006, Incorporating Change 2, 22 March 2010; The U.S. Army's Cyberspace Operation Concept Capability Plan 2016-2028, Training and Doctrine Command (TRADOC) Pamphlet (Pam) 525-7-8, 22 February 2010; Cyberspace Operations, Air Force Doctrine Document (AFDD) 3-12, 15 July 2010.

киберпространстве основными объектами воздействия являются информационно-технические средства информационной инфраструктуры противника и своих войск. Таковыми являются радиоэлектронные средства, средства вычислительной техники, средства электронной автоматики, электротехнические средства. К таким объектам также следует отнести информацию, которая находится в соответствующих хранилищах, в распределенных базах данных, циркулирует по каналам связи и передачи данных. Именно к этим объектам информационных инфраструктур применимы понятия «кибербой», «киберакция», «кибератака», «воздействие (поражение) специальными программными средствами», «защита от несанкционированного доступа», «разграничение доступа к информации» [129] (2014).

киберпространство[4] — совокупность информации и информационной инфраструктуры, предназначенной для формирования, создания, преобразования, передачи, использования и хранения этой информации на основе применения компьютеров и компьютерных сетей.

При этом термин компьютерная сеть определяется как совокупность связанных между собой функциональных блоков, предоставляющая услугу передачи данных между станциями, подключенными к сети, а компьютером, по определению (compute — от англ. вычислять), является любое средство вычислительной техники [14] (2013).

киберпространство[5] — является такой же «равноправной» сферой ведения боевых действий наряду с традиционными: землей, морем и воздушно-космическим пространством [41] (2014).

виртуальное пространство — синоним кибернетическому пространству (*киберпространству*).

Для информационного и кибернетического пространств достаточно сложно применимы пространственные взаимосвязи в обычном понимании, выстраивать их принято умозрительно, в воображении, т.е. виртуально [8] (2011).

кибернетическая война — систематическая борьба в кибернетическом пространстве между государствами (группами государств), политическими группами, экстремистскими и террористическими и т.п. группировками, проводимая в форме атакующих и защитных действий.

Основными целями как нападения, так и защиты в кибервойне являются информационные ресурсы, свойства которых с точки зрения безопасности (целостность, доступность и конфиденциальность) могут быть нарушены. Даже в ходе локальных конфликтов объектами кибератак могут стать любые информационные ресурсы, в том числе и сугубо гражданские, как всей страны, так и за ее пределами.

Хотелось бы подчеркнуть важные признаки, характеризующие состояние войны и отделяющие его от полярного состояния «мир». Во время войны коренным образом меняется жизненный уклад всего населения страны, все ресурсы направляются на обеспечение действий вооруженных сил, деятельность всех органов государственной власти подчинена достижению победы над врагом. Очевидно, что в полной мере этих признаков кибервойна не имеет. С этой точки зрения более корректным видится употребление термина «кибернетические боевые действия» или «кибернетическое противоборство» [8] (2011).

кибервойна — см. *сетевая война* [57] (2006).

война в киберпространстве [cyberspace war] — компонента кибероперациий, расширяющая зону их проведения за границы глобальной информационной сети с тем, чтобы на просторах мирового киберпространства обнаруживать и сдерживать противника от агрессивных действий, отражать его возможное нападение и нанести решительное поражение.

Объектами кибервойны являются компьютеры, телекоммуникационные сети, встроенные процессоры и контроллеры в оборудовании, системах и информационной инфраструктуре. Кибервойна, по взглядам американского армейского руководства, основана на киберразведке, кибератаках и кибероборонe. При этом обеспечивающими действиями определены киберподдержка и эксплуатация киберсетей [161] (2011).

сетевая война[1] — составная часть информационных операций, проводимых в целях атаки и защиты компьютерных сетей (Computer Network Attack, CNA; Computer Network Defense, CND).

Сетевая война также иногда назвается еще кибервойной.

При ее ведении могут использоваться различные средства радиоэлектронной войны (в том числе средства излучения направленной энергии, средства поражения и др.), информационное оружие и раз-

личные средства радиоэлектронной и компьютерной защиты [57] (2006).

военная политика в области международной информационной безопасности — должна быть направлена на введение международно-правовых механизмов, которые позволят сдержать потенциальных агрессоров от бесконтрольного и скрытого применения кибернетического оружия против Российской Федерации и ее геополитических союзников.

Для этой цели необходимы:

— защита критической информационной инфраструктуры общества и государства;

— защита информационно-психологической сферы общества от негативного контента;

— обеспечение безопасности трансграничного обмена информацией с ограниченным доступом;

— демонополизация управления Интернетом [34] (2007).

2.3.1. Сущность кибернетической войны

киберуязвимость — слабость (недостаток) кибернетической системы, по отношению к которому существует одна или несколько киберугроз и использованием которого может быть реализована кибератака [8] (2011).

киберугроза — совокупность условий и факторов, реализация которых в отношении киберуязвимости повышает риск нанесения ущерба кибернетической системе или ее владельцу [8] (2011).

кибероружие — специальные программно-аппаратные средства, применяющиеся для реализации угроз в отношении уязвимостей и для защиты от этих угроз [8] (2011).

программное оружие — См. *средства программного воздействия на информатизированные ВВСТ* [81] (2011).

средства программного воздействия на информатизированные ВВСТ — оружие, в основе поражения которым лежит использование специфически представленной информации, воспринимаемой техническими устройствами.

Программное поражение может наноситься только с помощью технических средств (специфических магнитных носителей информации), которые в совокупности со специфической информацией и представляют собой данный вид оружия.

Программное оружие способно путем внедрения в информатизированные системы и средства вредоносных программ (компьютерных вирусов) оказывать непосредственное воздействие на электронные носители информации, изменяя их состояние и возможности по осуществлению функционально важных информационных процессов в информатизированных ВВТ. Результатом такого воздействия может быть вывод из строя средств и систем управления, элементов высокоточного оружия и целых соединений и частей, элементов оперативного построения войск [81] (2011).

2.3.2. Операции в киберпространстве

наступательные информационные военные действия — направлены на снижение возможностей информационных систем противника путем создания условий, ухудшающих сбор и использование информации противником или позволяющих использовать информацию противника в своих интересах.

К наступательным информационным действиям относятся программно-информационные атаки на информационные системы, радиоэлектронное или огневое подавление их, воздействие на них электромагнитными импульсами, вхождение в информационные сети для ввода в них дезинформации, искажения информации и данных или получения необходимой информации о противнике [100] (2004).

оборонительные информационные военные действия — заключаются в защите своих информационных систем от всех видов воздействия, предпринимаемых противоборствующей стороной, которые включают в себя физические методы обеспечения безопасности, криптографическую защиту и все методы и способы борьбы с программно-информационными атаками [100] (2004).

операции в киберпространстве [cyberspace operations] — применение кибернетических средств и систем для решения главных задач ВС США, как в самом киберпространстве, так и с его использованием.

Такие операции основываются на компьютерных сетевых операциях, а также обороне и использовании глобальной информационной сети [161] (2011).

кибероперации — См. *операции в киберпространстве* [161].

киберразведка — действия, объединяющие компьютерную разведку с радио- и радиотехнической разведкой и другими видами разведки [161] (2011).

кибератака[1] — действия, объединяющие компьютерные сетевые атаки с электронными атаками, физическими атаками и другими видами действий для уничтожения информации и/или инфраструктуры или управления ими [161] (2011).

кибератака[2] — форма враждебных (противоправных) действий в киберпространстве; действия, направленные против кибернетических систем, информационных ресурсов или информационной инфраструктуры для достижения какой-либо цели и осуществляемые при помощи специальных программно-аппаратных средств и приемов (способов) воздействия [8] (2011).

кибероборона — действия, объединяющие информационную гарантию, защиту компьютерной сети, защиту критической инфраструктуры с радиоэлектронной защитой, поддержкой критической инфраструктуры и другими действиями для обнаружения и предотвращения действий противника, направленных на уничтожение или управление информацией и/или инфраструктурой глобальной информационной сети [161] (2011).

киберзащита — действия в кибернетическом пространстве, направленные на предотвращение возможных последствий влияния негативных факторов, сопутствующих проявлению киберугроз в отношении кибернетической системы [8] (2011).

киберподдержка — действия, которые поддерживают эксплуатацию киберсетей и войну в киберпространстве.

Они включают оценку уязвимости и безопасности силовых операций, а также возможности восстановления, вскрытия вредоносных кодов, кибераспектов эксплуатации сайтов, контрразведки, законода-

тельных и судебных вопросов, исследования, развития, проверки, оценки, боевого развертывания и обеспечения [161] (2011).

эксплуатация киберсетей — компонент кибероперации, который устанавливает, использует, управляет, защищает, обороняет и обеспечивает командование и управление армейской информационной сетью, ключевыми ресурсами критических инфраструктур и другими специфическими элементами киберпространства [161] (2011).

программно-техническое поражение — использование специфически представленной информации, воспринимаемой техническими устройствами.

Однако отнесение его к информационной, а не вооруженной борьбе представляется ошибочным.

Во-первых, программно-техническое поражение может наноситься только с помощью технических средств (определенных носителей информации), которые являются новым видом оружия. Без него, самостоятельно, информация воздействовать ни на что не может. Поэтому более точно это оружие нужно называть не информационным, а компьютерным или программно-техническим (в соответствии с видом поражения).

Во-вторых, новое оружие способно оказывать непосредственное воздействие не на информацию, а на ее носители, изменяя их состояние и функциональные возможности, в результате чего может выводиться из строя боевая техника противоборствующих группировок войск (сил), нарушаться управление ими и в конечном счете снижаться эффективность решения боевых задач. А это область не некой информационной, а вполне определенной — вооруженной борьбы.

В-третьих, средства и способы применения данного вида поражения еще недостаточно глубоко теоретически проработаны и не получили апробации на практике. Только решив эти задачи, можно будет более определенно говорить о их роли в вооруженной борьбе и эффективности применения [162] (2002).

информационно-техническое воздействие[1] — воздействие на техническую и программную основу информационно-телекоммуникационного пространства, или, как его еще называют, киберпространства, противника с целью нанесения ущерба и защиты своих систем управления от подобного воздействии [221] (2012).

информационно-техническое воздействие[2] (ИТВ) — целенаправленное программно-аппаратное (компьютерная атака) или программное воздействие, а также их комбинация на информационно-телекоммуникационные системы, приводящие к нарушению или снижению эффективности управления [104] (2016).

2.3.3. Киберпространство в современных боевых действиях

триада «боевое пространство — киберпространство — информационное пространство» — система, между компонентами которой существует взаимосвязь «часть — целое».

При этом каждому из перечисленных сфер противоборств присущи свои уникальные особенности [129] (2014).

боевое пространство[1] — в узком смысле — традиционное материальное пространство, описываемое трехмерным евклидовым континуумом, задаваемым тремя взаимоортогональными осями координат, в котором в соответствии с определенными временными параметрами ведутся боевые действия.

Так, для мотострелковой (танковой) роты при ведении ею оборонительного боя с мотопехотным батальоном боевое пространство (зона боевой ответственности) находится в пределах визуальной видимости и составляет площадь до 6 км^2. На таком участке может находится до 30 основных объектов противника.

В широком смысле — в настоящее время и в будущем границы традиционного боевого пространства для воинских формирований будут расширяться за счет появления новых сфер противоборства, которые в свою очередь образуют качественно другую боевую форму, характеризующую протяженность и объем зональной ответственности — боевое пространство. Особенным и наиболее приоритетным его элементом является *киберпространство* (боевое пространство в узком смысле, по мнению авторов, входит как элемент в киберпространство — *прим. сост.*) [129] (2014).

управление тактическими воинскими формированиями в киберпространстве — в тактическом звене управления можно выделить следующие шесть уровней иерархии: командование и штабы бригад, батальонов (дивизионов), командиров рот и их заместителей, команди-

ров взводов, отделений (боевых расчетов), а также отдельных солдат. Каждому из них будут соответствовать свои состав, структура и содержание киберпространства. При этом в соответствии с временными параметрами и ограничениями на каждом уровне иерархии вырабатываются свои решения на уточнение боевых задач подчиненным силам и средствам в ходе боевых действий.

Как показывает боевой опыт, солдат или младший командир принимает новое решение через несколько минут после предыдущего, а его реализация осуществляется одним или несколькими исполнителями практически мгновенно в пределах визуальной видимости. Поэтому их киберпространство будет весьма локальным, а количество применяемых компьютеров и каналов доступа к ним будет небольшим. Как следствие, из-за таких ограничений сложно проводить даже выборочные (точечные) кибератаки.

Но если взять цикл управления командира бригады, который в среднем составляет 30—40 минут, то современные показатели его боевого пространства (зоны боевой ответственности) составляют сотни квадратных километров. В принятии и реализации его решения участвуют многочисленные исполнительные элементы, большое количество серверов, компьютеров и компьютерных сетей на площади, значительно превышающей традиционное боевое пространство. Такой содержательный и пространственный масштаб киберпространства на уровне командира бригады позволяет как проводить в нем кибербои, так и осуществлять выборочные точечные кибератаки, приводящие в условиях тотальной информатизации боевых действий к срыву выполнения поставленных боевых задач (принятия решений).

Естественно, что для успешного ведения бригадой боя необходимо согласование и взаимообеспечение на каждом его этапе решений на всех шести уровнях иерархии. Если раньше такое согласование достигалось за счет опыта и умения командира, то в условиях киберпространства необходимы системы, не только собирающие, передающие обобщенный объем информации, но и помогающие командиру принимать решения, адекватные складывающейся обстановке. Таковыми являются системы поддержки и принятия решений. Они должны вырабатывать примерно три-четыре варианта решения, например, рациональное, достаточное, допустимое, из которых лицо, принимающее решение, должно выбрать одно и при необходимости скорректировать его [129] (2014).

2.3.4. Техносферная война

техносферная война (ТСфВ) — система согласованных по цели, месту и времени информационных действий, направленных на захват управления (частичный, полный) выбранными системами автоматизированного управления противника, либо перевод их в деструктивный режим функционирования.

Техносферная война, по сути, представляет собой форму конфликта, в котором объекты нападения (защиты) и средства нападения (защиты) — информация, существующая в рамках общемирового единого телекоммуникационного пространства (ОМЕТП). Под информацией в данном случае понимаются не только данные, передаваемые (хранимые) через ОМЕТП, но также информация о состоянии ОМЕТП (или его части) и состояниях АСУ атакуемой системы и алгоритмах их функционирования. При этом воздействия (разведка) осуществляются за счет использования искусственно созданных цифровых кодов, переданных по средствам искусственной среды (ОМЕТП) и воздействующих на коды (программы, аппаратуру) атакуемой (разведываемой) АСУ.

Техносферная воина будет иметь следующие основные отличительные особенности:

— война ведется в искусственной среде, при этом защищаемый ресурс, средства воздействия и защиты и пространство реализации желаемых эффектов также искусственны;

— воздействия могут осуществляться без прямого участия вооруженных сил и даже при их отсутствии;

— возможность ведения войны любого масштаба при отсутствии юридического факта ее объявления;

— высокая степень скрытности расположения средств воздействия и большая неопределенность в определении их возможностей;

— в отличие от классических войн (информационной и сетецентрической), в которых превалируют случайные процессы (погодные условия, морально-психологическое состояние войск и др.), в ТСфВ при известных законах функционирования техносферы присутствует только неопределенность результатов воздействий;

— чем выше уровень автоматизации объектов (процессов), тем больших результатов можно добиться в ТСфВ (самые уязвимые — наиболее развитые системы);

— возможность проведения отдельных операций, которые противник не сможет даже зафиксировать;

— темпы разработки и совершенствования средств воздействия превышают темпы развития средств защиты;

— планы проведения операций могут разрабатываться специалистами, не имеющими классической военной подготовки;

— стирание традиционных представлений о войне, в частности неактуальность понятий госграница и линия фронта, поскольку полем боя становится общемировое единое телекоммуникационное пространство;

— высокая оперативность проводимых операций при отсутствии ограничений на масштаб операции и удаленность объектов поражения;

— размывание границ между военной и гражданской сферами при ведении ТСфВ;

— несмотря на искусственность (виртуальность) всех элементов ТСфВ, результаты атак имеют физически регистрируемый результат;

— принципиальное переориентирование систем разведки: объектами разведки становятся не только и не столько государственные (военные) объекты, но и коммерческие автоматизированные системы технологического управления; необходимость ведения постоянной (быстрое изменение состояния объекта) и максимально широкой (максимально возможный охват различных по принадлежности объектов) разведки; большой объем развединформации требует внедрения соответствующих эффективных способов и алгоритмов ее обработки и анализа в автоматическом режиме и реальном времени;

— в связи с необходимостью оперативного реконфигурирования (разработки) средств и методов воздействия под конкретный объект на разведку возлагается функция не только определения объекта (системы) для поражения, но и нахождения его уязвимых мест на данный момент времени;

— принципы техносферных воздействий (оружия) основаны на использовании уязвимых мест автоматизированных систем противника, имеющихся в защите и возникших при проектировании и создании, что позволяет переводить систему в режимы, не соответствующие целевому функционированию;

— степень воздействий на системы противника может находиться в диапазоне от ухудшения эффективности функционирования (в том числе и путем изменения цели функционирования) до полного выхода из строя (с возможными техногенными катастрофами);

— точное прогнозирование последствий техносферной атаки пока затруднено вследствие большой сложности атакуемых систем и их множественных взаимосвязей [203] (2012).

принципы ведения техносферной войны — можно сформулировать следующие основные принципы:

массирование (интеграция) результатов;

максимальная синхронизация с процессами атакуемой стороны;

предельная степень приближения финальной (запланированной) ситуации;

приоритетные вклады АСУ в создание и распределение используемого ресурса;

учет характеристик (свойств) ИТКС;

учет уровня технологий и квалификации персонала;

сочетание различных способов и видов компьютерных воздействий;

неразличимость состояний мирного и военного времени [203] (2012).

информационное превосходство над противником — способность своевременно собирать, обрабатывать и распределять непрерывный поток информации об обстановке, препятствуя аналогичным действиям противоборствующей стороны.

В конечном итоге информационное превосходство позволяет поддерживать в ходе операции такой темп ведения боевых действий, который дает возможность доминировать на поле боя и, оставаясь непредсказуемым, постоянно опережать противника. Однако такой подход, на наш взгляд, не нов, он широко известен и многократно использовался в классических операциях [203] (2012).

терминологические конструкции информационной и сетецентрической войн — известные такие конструкции характеризуются следующими основными чертами:

принципиальное (прямое или косвенное) применение вооруженных сил при ведении данных типов войн;

наличие только политических и даже чисто военных целей;

позиционирование информационного превосходства как самостоятельной цели;

использование комбинаторных понятий, в частности «информационно-психологическое воздействие»;

традиционное разграничение на условия мирного и военного времени;

преимущественный упор в определении войн на межгосударственные отношения;

злоупотребление понятием «реальный масштаб времени»;

СЦВ в структурно-понятийном плане отражена в виде типовой системы управления войсками (СУВ), поданной в усеченной децентрализованной форме, но с гипертрофированным представлением вспомогательно-технологических элементов;

роль и место глобальной информационной решетки в рамках СЦВ позиционируется эквивалентно типовой (традиционной) системе связи.

Таким образом, используемые в настоящее время термины «информационная война» и «сетецентрическая война» не сопровождаются соответствующим содержательным наполнением. Более того, неоднозначность данных понятий затрудняет, а в большинстве случаев исключает возможность конструктивных вариантов их методологического и технического наполнения.

Все это свидетельствует о необходимости введения в теорию военного искусства понятия о принципиально новом типе войны — войны в искусственной сфере, где защищаемый ресурс, среда существования этого ресурса, средства разведки и воздействия, а также среда, в которой эти воздействия осуществляются, являются искусственными [203] (2012).

доля автоматизации в управлении войсками — по данным из различных источников, уровень автоматизации систем управления в Вооруженных Силах РФ составляет порядка 20%, а в США — около 80% [203] (2012).

3. Сетецентрическая война

сетецентричная война[1] [Network Centric Warfare[34], NCW] — ориентированная на достижение информационного превосходства

[34] *Прим. сост.:* Другим наиболее распространенным вариантом перевода является термин «сетецентрическая война».

концепция проведения военных операций, предусматривающая увеличение боевой мощи группировки объединенных сил за счет создания информационно-коммутационной сети, связывающей датчики (источники данных), лиц, принимающих решения, и исполнителей, что обеспечивает доведение до участников операций информации об обстановке, ускорение процесса управления силами и средствами, а также повышение темпа операций, эффективности поражения сил противника, живучести войск и уровня самосинхронизации боевых действий[35] [17, 95, 140] (2007, 2010, 2013).

3.1. Теория сетецентрической войны

сетецентризм[1] — понятие впервые появилось в американской компьютерной индустрии и стало результатом прорыва в информационных технологиях, позволяющих организовать взаимодействие между компьютерами, даже несмотря на использование в них разных операционных систем.

В приложении к военному делу сетецентризм означает информатизацию вооруженной борьбы, предусматривающую целенаправленный процесс интеграции компьютерных средств, информационных и коммуникационных технологий в войска для более эффективного планирования, организации, управления и ведения операций (боевых действий).

Вместе с тем нельзя не отметить, что сетецентризм не становится панацеей, т.е. средством для решения всех проблем. Подтверждением этому служит состояние сообщества военных экспертов в США, которое поделилось на сторонников, серьезно сомневающихся и противников подобной концепции. Последние считают, что технологии занимают слишком много места в американской военной стратегии. Более того, надежды Пентагона на то, что инновации принесут победу на поле боя так же, как они делают прибыль в бизнесе, несостоятельны.

Засилье технократизма в виде концепции сетецентрической войны ведет к целому ряду ошибок. Среди них: переоценка способности человека адекватно перерабатывать большой объем противоречивой информации; упрощенное видение противника через сведение его стратегии к асимметричным действиям; неоправданная бюрократиза-

[35] Net-Centric Environment Joint Functional Concept // DOD, 2005. — Appendix B. Glossary.

ция процесса управления и недостаточный учет изменчивой природы боя; наконец, явный или неявный аргумент, что военная победа есть самодостаточная цель всей кампании [27] (2014).

сетецентризм[2] — информатизация вооруженных сил, предусматривающая целенаправленный процесс системной интеграции компьютерных средств, информационных и коммуникационных технологий с целью получения новых общесистемных свойств, позволяющих более эффективно планировать, организовывать и вести операции (боевые действия).

Особенность революции в военном деле, связанной с появлением сетецентризма, состоит в том, что, в отличие от предыдущих, она связана не с новыми образцами вооружения и военной техники, а с их программным обеспечением, т.е. с информационными технологиями.

Часто смешиваются понятия сетецентрической войны (операции) и информационной войны (операции). Тем не менее эти явления различаются целями и задачами. Если первое — это способ повышения боевых возможностей воинских формирований, то второе — способ и инструмент проведения операций в киберпространстве [5] (2014).

аспекты сетецентрической войны — в основе концепции сетецентрической войны лежат военные, технологические и психологические аспекты.

Военные. Началу боевых действий должно предшествовать достижение информационного превосходства, следствием чего будет являться «информационная прозрачность» противника и своих войск. Это достигается соответствующим обстановке пониманием ситуации на поле боя, определением своих преимуществ и слабых мест противника. По сути информационное превосходство — это постоянное опережение противника: опережение в разведке (добывании информации о противнике), в принятии решения на оптимальное применение сил и средств, в нанесении удара, в маневре, т.е. во всем том, что составляет суть вооруженной борьбы.

Технологические. Концепция сетецентрической войны может быть реализована путем внедрения в практику военного дела принципиально новых систем разведки, управления, целеуказания и компьютерного моделирования. Системообразующим элементом здесь выступают космические информационные системы и комплексы.

Психологические. Формирование структур поведения всех участников вооруженного конфликта в сетецентрической войне происходит при помощи рефлексивного подхода [179] (2012).

3.2. Концепция сетецентрической войны

платформо-центрическая война[1] [Platform-Centric Warfare] — принципы ведения военных действий, строительства вооруженных сил и управления подчиненными боевыми формированиями в XX веке в эпоху «индустриальной эры».

В то время успех будущих операций и сражений зависел в основном от индивидуальных возможностей боевых средств, а объединение сетями, хотя и предусматривалось, но не позволяло добиться того эффекта, который дают новые информационные технологии [116] (2008).

концепция «Сетецентрическая война» [Network-Centric Warfare, NCW] — также известная как концепция «Ведение боевых действий в едином информационном пространстве» — система взглядов на способы управления вооруженными силами в операциях XXI века с использованием единого интегрированного информационного пространства, формируемого в масштабе времени, близком к реальному, базирующаяся на трех интегрированных сетях: глобальной информационно-управляющей сети, сети разведки и наблюдения, сети средств поражения и подсистемы высокоточного навигационно-временного обеспечения. Определяется как концепция информационного превосходства над противником в операциях [75] (2017).

концепция сетецентрической войны — отнесена к функциональным концепциям. Ее использование направлено прежде всего на достижение информационного превосходства при ведении боевых действий. Но и информационное превосходство не самоцель. Конечная цель — скачкообразное повышение оперативности управления и принципиальное изменение качества взаимодействия между разнородными группировками войск, что в конечном итоге приводит к достижению подавляющего превосходства в вооруженной борьбе.

По нашему мнению, речь идет не о каком-то новом типе войны, а о сетецентрическом подходе к управлению войсками (силами) при ведении военных действий [179] (2012).

концепция сетецентричной войны — система взглядов на основные цели, задачи, условия ведения сетецентричной войны с противником, обладающим аналогичным военно-техническим потенциалом, теорией применения, уровнем подготовки войск; свойства и способы применения вооружения, военной техники в сетецентричной войне.

Для реализации концепции необходимо уточнить ряд положений оперативного искусства, требования к квалификации и уровню подготовки командно-штабного состава, указать уровни использования сетецентричной системы в операциях, функции органов управления по их созданию, режимы формирования и функционирования, общую структуру, состав привлекаемых сил и средств, основы управления и обеспечения. Цели и задачи ведения сетецентричной войны следует рассмотреть поэлементно в соотношении с оперативными, тактическими и другими задачами группировок войск и сил.

Концепция необходима для организации работ по приданию сетецентричных свойств системам управления, разведки, обеспечения, навигации, наведения боевых комплексов [95] (2010).

новая философия войны — это концепция сетецентричной войны, как утверждают философы и специалисты по информатике.

Но для подготовки и ведения военных действий одних только философских взглядов на войну недостаточно: нужны знания законов, закономерностей и принципов ведения вооруженной борьбы. А это уже предмет изучения военной науки.

Поэтому в новых условиях сетецентричность станет новой особенностью работы командиров и штабов по организации применения войск (сил) в операциях. Но акценты на ней в их глазах не превысят значимости организации управления, взаимодействия и обеспечения военных действий в целом. Словосочетание «сетецентричные операции» прозвучит так же нелепо, как «телефонизация войны». А умения в организации военных действий, характеризующихся свойствами сетецентричности, обретут все органы управления [95] (2010).

новое содержание характера вооруженной борьбы — определено сетецентрическими условиями военных действий, которые ведутся в едином боевом пространстве, объединяющем все сферы вооруженной борьбы, синхронно, взаимосвязано и непрерывно под единым командованием и в единой информационно-коммуникационной среде.

При этом разделенные элементы сети своими действиями во всей глубине боевого пространства способствуют достижению главной цели операции за счет горизонтальных связей, обеспечивающих устойчивое управление и постоянное взаимодействие [74] (2011).

сетецентрическая война[1] [Network-Centric Warfare] — понятие, отражающее суть проводимых мероприятий и определяющее новые принципы управления войсками и силами в будущих операциях, успех в которых будет зависеть в первую очередь от объединения всех участников боевых действий в рамках единого информационно-коммуникационного пространства.

Авторами этого понятия считаются вице-адмирал ВМС США Артур Цебровски и эксперт министерства обороны Джон Гарстка. В едином уставе КНШ ВС США Joint Publication 1-02 «Словарь военных терминов...» данный термин отсутствует.

В эпоху «информационной эры» на первое место выходят новые информационные технологии, которые, по мнению ряда зарубежных экспертов, позволят осуществить революцию в военном деле. Их внедрение в военную сферу также направлено на повышение боевых возможностей формирований, но уже не только за счет повышения огневых, маневренных и других характеристик индивидуальных платформ, но и в первую очередь за счет сокращения цикла боевого управления в операции (бою).

Другой особенностью является то, что объединение сетью охватывает не только системы боевого управления, связи, вычислительной техники, разведки и наблюдения, но и боевые платформы, и в первую очередь такие, как носители средств огневого поражения. Это и определило в текущем десятилетии формирование новой системы взглядов на формы и способы ведения вооруженной борьбы.

Понятие «сетецентрическая война» рассматривает вооруженные силы как устройства, подключенные к сети. В зависимости от выбора сетевой архитектуры и ее типа средствами сети могут быть корабли, самолеты, средства поражения, управления, связи, разведки и наблюдения, группа военнослужащих или отдельные солдаты, а также комбинация и тех, и других. Возможности таких боевых формирований определяются не столько индивидуальными характеристиками, сколько возможностями всей группы подключенных к сети средств как единого целого.

Таким образом, вопрос изучения развертываемых сетей, их архитектур построения является важным и неотъемлемым условием изучения возможностей армий ведущих зарубежных стран в эпоху «информационной эры» [116] (2008).

сетецентрическая война[2] — война, в которой увеличение боевой мощи группировки войск (сил) достигается за счет создания информационно-коммуникативной сети, связывающей источники информации (разведки), органы управления и средства поражения (подавления). Это обеспечивается доведением до участников операций достоверной и полной информации об обстановке практически в реальном масштабе времени.

Образно парадигму сетецентрической войны можно охарактеризовать следующим образом: вместо нескольких «птиц» или «акул» (в зависимости от среды боевых действий) со «сверхдальнозоркими» органами чувств, развитым интеллектом и большой физической силой предполагается иметь «рой насекомых» или «стаю пираний». Каждое из этих «насекомых» существенно уступает «птице» по любому из сенсорных и силовых параметров и в прямом сопоставлении ей безнадежно проигрывает. Однако противостоять хорошо организованному «рою» неизмеримо сложнее, чем «птице», хотя бы потому, что обнаруживать отдельных «насекомых», а значит, и уничтожить их гораздо труднее.

Основными особенностями сетевой войны по сравнению с традиционной в нынешнем ее понимании являются следующие.

1) Широкая возможность использования пространственно распределенной силы. При этом информационная система собирает и распределяет данные, поступающие о всех источников разведывательной информации: спутников, самолетов, вертолетов, танков, БМП и даже отдельного пехотинца.

2) Силы, участвующие в сетевой войне, высокоинтеллектуальны в целом как единая система.

3) Наличие эффективных и защищенных коммуникаций между объектами в боевом пространстве.

4) Виртуальной основой для ведения сетецентрической войны является информационно-коммуникативное пространство, сформировать которое планируется за счет оснащения общевойсковых формирований тактического звена соответствующими средствами, например разведывательно-сигнализационными датчиками, беспилотными лета-

тельными аппаратами от взводного до бригадного уровня, дистанционно управляемыми машинами различного типа и образцами ВВСТ с экипажами, поставляющими информацию в единую систему сбора, обработки и распределения информации. При этом физической основой создания информационно-коммуникативного пространства является электромагнитное поле различных частотных диапазонов [81] (2011).

сетецентричная война[2] — ведение военных действий, предусматривающее увеличение боевой мощи группировки объединенных сил за счет создания информационно-коммутационной сети, связывающей источники информации (разведки), органы управления и средства поражения (подавления), что обеспечивает доведение до участников операций достоверной и полной информации об обстановке практически в реальном масштабе времени.

За счет этого достигается ускорение процесса управления силами и средствами, повышение темпа операций, эффективности поражения сил противника, живучести своих войск и уровня самосинхронизации боевых действий.

Суть таких войн состоит в максимальном расширении форм производства информации, доступа к ней, ее распределении и полном контроле выполнения решений, принятых по этой информации. При этом создаваемая «сеть» представляет собой новое пространство — информационное. Именно в этом пространстве и развертываются основные стратегические операции — как разведывательного, так и военного характера, а также их медийное, дипломатическое, экономическое и техническое обеспечение.

Военные действия в этой сети являются лишь разновидностью сетевых процессов. Регулярная армия, все виды разведок, технические открытия и высокие технологии, журналистика и дипломатия, экономические процессы и социальные трансформации, гражданское население и кадровые военные, регулярные части и отдельные слабо оформленные группы — все это интегрируется в единую сеть, по которой циркулирует информация. Создание такой сети и составляет основную сущность военной реформы ВС США на ближайшие десятилетия [224] (2008).

сетецентрическая война[3] [Network Centric Warfare, NCW] — концепция управления, отражающая новый способ руководства вооруженными силами в операциях XXI века.

На наш взгляд, концепция сетецентрической войны по своей сути не является системой взглядов на ведение войны в целом.

По мнению ее авторов, реализация на практике теории сетецентрической войны позволит перейти от войны на истощение к более скоротечной и более эффективной форме ведения боевых действий, для которой характерны быстрота управления и принцип самосинхронизации структуры войск и их систем управления.

Сетецентрическую войну ведет разветвленная сеть хорошо информированных, но географически рассеянных сил. Главными характеристиками этих сил являются: высокоэффективная «информационная решетка», обеспечивающая санкционированный доступ к информации; применение высокоточного оружия высокой дальности действия; маневренность войск; высокоэффективная система боевого управления; интегрированная «сенсорная решетка», объединенная с подсистемой отдельных тактических подразделений и подсистемой боевого управления.

Войска могут вести сетецентрическую войну на любом уровне (тактическом, оперативном, стратегическом) вне зависимости от географического региона, боевых задач, состава и структуры вооруженных сил.

В чем же различие существующих концепций и новой с точки зрения организации и осуществления управления войсками и оружием? Прежде всего, необходимо отметить, что эта область военного дела в наибольшей степени испытывает воздействие информационно-технологического прорыва, поскольку современная революция в военном деле тесно связана с качественным преобразованием информационных технологий, изменяющим как военную технику, так и принципы управления войсками и оружием. Соответственно, коренным образом изменяются не только сами системы оружия и боевая техника (появление информационного оружия тому свидетельство), но и системы управления, а вместе с ними все военное дело и боевая мощь вооруженных сил. Это, в свою очередь, приводит к появлению новых форм и способов боевых действий. Так, в ВС США и ОВС НАТО появились такие новые формы ведения военных действий, как информационные операции (наступательные, оборонительные, специальные) и такой способ вооруженной борьбы, как борьба с системами боевого управления (Command Control Warfare, C2W).

Анализируя суть изложенной американской концепции сетецентрической войны, нельзя не заметить, что ее авторы, с одной стороны,

смешивают различные понятия, относящиеся к содержанию войны, ее формам, видам и способам ведения, с понятиями управления войсками (силами), а с другой — в завуалированном виде провозглашают новые тенденции в развитии системы управления войсками (силами). Поэтому зачастую трудно понять — идет ли речь о новых принципах, формах, видах и способах ведения военных действий (примеры о гипотетическом начале войны, исчезновении последовательности боевых действий и оперативных пауз, переходе от войны на истощение к более эффективной «форме» ее ведения и др.) или об изменении способов организации управления войсками (примеры о быстроте управления, о самоорганизации структуры военного управления снизу и об отмене централизованной системы управления, изменении доступа к информации, объединении системы управления с системой отдельных тактических подразделений и «сенсорной решеткой» и др.). В то же время, рассматривая суть концепции сетецентрической войны, ее авторы хотя и говорят об обеспечении информационного превосходства, но совершенно не упоминают об информационной войне (в нашей терминологии — информационное противоборство), формах ее ведения (наступательной, оборонительной, специальной информационных операциях и способах их ведения), а также о силах и средствах борьбы с системами боевого управления. Все это дает нам основание утверждать, что главное содержание концепции сетецентрической войны заключается не в новых формах и видах ведения военных действий, а в изменении способа управления войсками (силами).

Необходимо отметить также, что в руководящих документах ВС США, других развитых государств и ОВС НАТО не предусмотрена самоорганизация и самосинхронизация военной структуры снизу, а формы, виды и способы ведения боевых действий и управления ими не могут сами собой видоизменяться, как заявляют авторы концепции сетецентрической войны. Все уставы ВС США и ОВС НАТО определяют **централизованный, иерархический принцип организации ВС** и управления ими, принятия политических и военных решений, допуская лишь разумную инициативу и возможность децентрализованного действия воинских формирований в рамках общего замысла операции и принятого вышестоящим командованием решения. При нарушении этого основного принципа невозможно проведение эффективных психологических операций и дезинформации, обеспечение необходимой оперативной безопасности, своевременное выявление «центров тяжести» в ВС противника, своевременное обнаружение, поражение и по-

давление его наиболее важных объектов. Все это, на наш взгляд, может привести к срыву замысла операции и поражению. Кроме того, самосинхронизация систем управления, осуществляемая снизу, не всегда обеспечит достижение внезапности и информационного превосходства над противником, не исключит иногда весьма необходимые для восстановления боеспособности войск оперативные паузы и не сделает боевые действия более динамичными и результативными. По нашему мнению, она может лишь повысить вероятность преждевременного раскрытия противником замысла кампании (операции, боя) и дать ему возможность завоевать информационное превосходство, а следовательно — упредить в принятии и реализации оперативных решений [57] (2006).

сетецентрическая война[4] — война, для которой характерны быстрота управления и принцип самосинхронизации. Причем главной задачей при реализации данной формы является не достижение быстроты управления, как считают многие приверженцы концепции сетецентрической войны, а наиболее оптимальное использование преимуществ во времени, которые дает применение этой модели [223] (2017).

сетецентрическая война[5] — это не совокупность форм и способов ведения военных действий, а информационно-управленческая технология управления войсками (силами), которая оказывает решающее влияние на характер и исход вооруженной борьбы.

Концепция сетецентрической войны воплощает в себе уход от традиционного способа управления войсками, когда командиры получают информацию через централизованный информационный пункт по иерархической системе управления, и переход к такой системе управления, когда командиры получают информацию напрямую от разведывательных источников во времени, близком к реальному. В конечном итоге оперативность и достоверность получаемой командиром информации выше, чем у противника. Именно за счет этого пытаются довести уровень взаимодействия между разнородными силами и средствами до требуемого уровня и гарантированного поражения противника [179] (2012).

сетецентрическая война[6] [Network Centric Warfare, NCW] — по нашему мнению, концепция сетецентрической войны по своей сути не является системой взглядов на ведение современной войны (вооруженных конфликтов) в целом, а представляет собой концепцию управ-

ления, отражающую новый способ руководства вооруженными силами в операциях XXI века [74] (2011).

сетецентрическая война[7] (СЦВ) — по нашему мнению, употребление этого понятия применительно к содержанию военных действий не совсем корректно, так как данное понятие характеризует не специфические черты войны, а методы обработки данных и используется среди специалистов информационных технологий в контексте «сетецентрическая модель вычислений».

В соответствии с этой моделью пользователю не нужно приобретать все программное обеспечение для решения прикладных задач, а достаточно иметь лишь дешевое оборудование (сетевой компьютер) для обращения к удаленной центральной базе, которая производит все необходимые вычисления и обеспечивает потребителя требуемой информацией. Смысл сетевого принципа в том, что главным элементом всей модели является обмен информацией.

Вызывает сомнение обоснованность утверждения некоторых авторов, что ведение сетевой войны предполагает отказ от классической иерархической системы управления войсками. Если допустить существование такого принципа, то возникает закономерный вопрос: кто и как будет обеспечивать боевые действия войск, имеющих сильные горизонтальные связи и слабые вертикальные?

Некорректным, на наш взгляд, представляется и утверждение о том, что организационная структура частей (подразделений), формы и методы выполнения ими боевых задач в сетецентрической войне, будут видоизменяться в соответствии с принципом самосинхронизации снизу вверх по усмотрению непосредственных исполнителей и в соответствии с потребностями вышестоящего командования. В данном случае необходимо рассматривать не новый специфический принцип из теории сложных систем, а реализацию старого принципа «централизованное управление — децентрализованное исполнение» боевых задач [216] (2006).

сетецентрическая война (операция, бой) — условное понятие иностранного происхождения, адаптация которого применительно к отечественному понятийному аппарату позволяет понимать его как войну (операцию, бой) с применением высокотехнологичных информационно-коммуникационных, ударных, огневых, электромагнитных, программных и других средств, обеспечивающих применение на практике новых путей реализации принципов военного искусства, а в ко-

нечном счете как максимально эффективное поражение противника в реальном масштабе времени [165] (2012).

сетецентрические условия военных действий — модель, представляющая собой систему, интегрирующую возможности средств разведки, поражения и управления в единую сеть [73] (2012).

особенности сетецентрической войны — отличительными ее особенностями по сравнению с традиционной войной, являются:

возможность согласованного использования географически распределенных сил и средств;

самосинхронизация сил, участвующих в сетецентрической войне;

высокая динамичность, активность и результативность всех процессов управления и самих боевых действий;

изменение формы военных действий, которая от последовательных боев и операций с соответствующими промежутками (паузами) между ними, приобретает форму непрерывных высокоскоростных действий (операций, акций) с решительными целями;

наличие эффективных коммуникаций между системами и средствами управления войсками и оружием, что дает возможность на обширном географическом пространстве проводить совместные действия, а также динамически наилучшим образом распределять ответственность и объем задач между различными подразделениями применительно к текущей обстановке.

Превосходство над противником достигается в первую очередь за счет существенного повышения качества управления.

Следует отметить, что для вывода из строя или хотя бы временного снижения эффективности функционирования сетецентрических систем противника требуется согласованное по времени, пространству и целям массированное воздействие на многочисленные взаимоувязанные средства сете- и каналообразования, приводящие к системоразрушению. Это и есть тот единственно возможный способ сетецентрической войны, без которого действительно трудно обойтись, если всерьез готовиться к возможным высокотехнологичным войнам будущего.

При этом следует констатировать, что сетевую войну можно выиграть (успешно вести) только сетевыми методами и средствами [182] (2011).

математическая оценка сецентрической войны — в настоящее время ряд ведущих зарубежных экспертов признают, что при всех оче-

видных достоинствах новых сетецентрических принципов и положительных результатах применения группировок войск, оснащенных современными цифровыми системами связи и передачи данных в вооруженных конфликтах и на опытных учениях, точного математического аппарата количественной оценки влияния новой концепции на повышение боевых возможностей и эффективность действия войск до сих пор нет. Подтверждением этому можно считать и доклад специалистов лаборатории MIT Lincoln на конференции 2007 года «Количественные методы оценки в обеспечении обороноспособности и национальной безопасности».

По заключению экспертов, в настоящее время существует ряд теорий, которые могут быть применены для оценки степени влияния сетецентричности на боевые возможности и повышение эффективности применения группировок войск и сил. Среди наиболее известных теория Джона Бонда «The OODA Loop», раскрывающая контур цикла управления; классическая модель Ендслей (Endsley) «Situation Awareness», содержащая ряд статических оценочных параметров; комплексная теория Моффата «Complexity Theory; Network Centric Warfare» и др. Вместе с тем часть данных разработок, хотя и содержит предложения некоторых количественных оценок, по сути являются концептуальными описательными моделями.

Также иностранные специалисты отмечают, что за последнее время не было проведено достаточного количества исследований в области математического обоснования повышения возможностей боевых формирований при объединении их системой единого информационно-коммуникационного сетевого обеспечения. Более того, многие западные ученые попросту используют хорошо известный закон Меткалфа, взятый из коммерческой сферы, и пытаются его применить для военных нужд. Закон Меткалфа гласит, что ценность сети пропорциональна квадрату количества пользователей сети. Закон часто иллюстрируется примером применения факсимильных аппаратов. Один факс сам по себе бесполезен, но подключение к сети каждого нового аппарата увеличивает их количество, следовательно, и количество людей, с которыми первый обладатель факса может связаться, чтобы передать им сообщение. То есть десять пользователей позволяют сформировать сотню возможных каналов, а сотни средств позволяют установить десятки тысяч соединений.

Для военных исследований закон может быть применен только как индикатор числа средств, участвующих в формировании данных

ситуационной осведомленности, и то без учета достоверности и своевременности этих данных [117] (2009).

парадигма сетецентричной войны — парадигма, которую можно охарактеризовать следующим образом: «Вместо нескольких «птиц» или «акул» (в зависимости от среды боевых действий) со «сверхдальнозоркими» органами чувств, развитым интеллектом и большой физической силой целесообразно иметь «рой насекомых» или «стаю пираний». Каждое из этих «насекомых» существенно уступает «птице» по любому из сенсорных и силовых параметров и в прямом сопоставлении ей безнадежно проигрывает. Однако противостоять хорошо организованному «рою» неизмеримо сложнее, чем «птице», хотя бы потому, что обнаружить отдельное «насекомое», а значит, и уничтожить его гораздо труднее» [224] (2008).

терминология сетецентрической войны — нельзя не согласиться с мнением некоторых отечественных исследователей, что при переводе зарубежных материалов по вопросам сетецентрической войны читатель столкнулся с несколько некорректным переводом понятийного аппарата [179] (2012).

сетевая война[2] — концепция ведения боевых действий оперативного и стратегического масштаба, суть которой заключается в достижении успеха в вооруженной борьбе не за счет преимущества в численности и огневой мощи войск, а в результате превосходства в информационных возможностях и применения воинских формирований, построенных по принципиально новой сетевой структуре.

Эти формирования, рассредоточенные по всей поверхности земного шара (территории театра войны, зоны конфликта), благодаря широкому использованию новейших коммуникационных технологий будут способны автономно вести совместные действия, находясь на значительном удалении друг от друга и от координирующих звеньев (органов управления). При этом значение иерархии отступает на второй план, а роль горизонтальных связей между боевыми частями и подразделениями существенно повышается.

Подобные организационные структуры, качественно отличающиеся от классических отсутствием строгой вертикали подчиненности, возникали на протяжении значительного периода истории человечества. К ним можно отнести, например, практически все партизанские движения. Несмотря на то, что эти движения почти всегда управлялись

государством, горизонтальные связи между отдельными отрядами оказывали значительное влияние на общий успех проводимых операций.

В современных условиях идея сетевой войны стала актуальной в связи с появлением угрозы национальной безопасности со стороны всевозможных террористических, криминальных и других организаций, участники которых объединены в некие сетевые структуры. Данные организации не имеют четкой иерархической подчиненности, зачастую у них нет даже единого руководства, а координация их деятельности осуществляется с использованием средств глобальной коммуникации. Для них характерно наличие единой стратегической цели и отсутствие четкого планирования действий на тактическом уровне. Террор сегодня — это война, в которой участвуют государства и их правительства, политические партии, силовые министерства и ведомства, транснациональные коммерческие структуры и др. [180] (2005).

сетевая война[3] — есть несколько ключевых моментов, которые отличают такую войну от войны традиционной. Первый заключается в использовании географически распределенной силы. Второй состоит в том, что силы, участвующие в «сетевой войне», высокоинтеллектуальны. Используя знания, полученные от всеохватывающего наблюдения за боевым пространством и расширенного понимания намерений командования, эти силы становятся способными к самосинхронизации своей деятельности, более эффективными при автономных действиях. Третий — наличие развитых и надежных коммуникаций (связей) между их элементами в боевом пространстве, что позволяет им осуществлять совместные действия, быстро приспосабливаясь к ситуации [220] (2003).

особенности сетевой войны — отличия по сравнению с традиционной войной в нынешнем ее понимании, состоящие в следующем:

1) Широкая возможность использования географически распределенной силы. Действия ударных сил США и НАТО в Югославии и Ираке — яркое тому свидетельство. Это же касается и средств обеспечения. Ранее было необходимо, чтобы элементы тылового обеспечения располагались в одном районе в непосредственной близости к противнику или к обороняемому объекту. Новая концепция принципиально снимает эти ограничения, что и было подтверждено практически в ходе войны в Ираке, где армия США, используя распределенную информационную автоматизированную систему MTS, добилась гибкого и

своевременного тылового обеспечения своих войск на всем театре войны.

2) Силы, участвующие в ней, высокоинтеллектуальны. Пользуясь знаниями, полученными от всеохватывающего глобального наблюдения за боевым пространством и расширенного понимания намерений командования, эти силы будут способны к самосинхронизации деятельности, станут более эффективными при автономных действиях. Более того, до 80% боевых вылетов авиации США начиная с операции в Афганистане уже производится «вслепую», т.е. когда в памяти бортовых компьютеров нет целей, информация о них поступает от наземных частей непосредственно с передовой (система боевого планирования и управления авиацией на ТВД TBMCS — Theater Battle Management Core Systems). Кроме того, в войне в Ираке армия США уже использовала новую распределенную информационную систему боевого управления FBCB2 (Force XXI Battle Command Brigade or Below), охватывающую уровень «бригада — батальон — рота». Эта система воспроизводит на дисплее компьютера командира боевую обстановку в деталях с привязкой к рельефу местности. Информационная система собирает и распределяет данные, поступающие от всех источников разведывательной информации: спутников, самолетов, вертолетов, танков, БМП и даже отдельного пехотинца.

3) Наличие эффективных коммуникаций между объектами в боевом пространстве. Это дает возможность географически распределенным объектам проводить совместные действия, а также динамически распределять ответственность и весь объем работы, чтобы приспособиться к ситуации. Именно поэтому более чем в семь раз по сравнению с 1991 годом увеличилась суммарная полоса пропускания каналов спутниковой связи, арендованных Пентагоном для передачи информации. В результате в 2003 году в Ираке американцы для нанесения воздушных ударов применили до 80% высокоточного оружия против 10% в ходе операции «Буря в пустыне» (1991) и 40% — в Югославии (1999) [224] (2008).

3.2.1. Эволюция войн «центрического» характера

платформо-центрическая война[2] (ПЦВ) — война в линию. Определенные функции, выполняемые основными боевыми машинами, распределяются между несколькими боевыми бронированными машинами, интегрированными в АСУ [92] (2011).

сетецентрическая война[8] (СЦВ) — война на плоскости. Управление боевыми действиями на основе единого информационно-коммуникационного пространства и достижения платформо-центрической войны [92] (2011).

инфомационно-центрическая война (ИЦВ) — война в пространстве. Внедрение высокотехнологичных систем сбора, моделирования, визуализации данных и поддержки принятия решений в режиме реального времени. Способность к структурной и функциональной адаптации и достижения сетецентрической войны [92] (2011).

знание-центрическая война (ЗЦВ) — война во всех средах и смысл. Передача знаний вместо обстановки в условиях децентрализованного управления силами и средствами с опосредствованным участием личного состава. Опережение противника в принятии и реализации решений. Переход от «стреляющего» к «управляющему» солдату и достижения инфомационно-центрической войны [92] (2011).

3.2.2. Достоинства и недостатки концепции сетецентрической войны

Национальная военная стратегия США — стратегия, принятая в апреле 2004 года, в которой отражено новое направление развития вооруженных сил на ближайшую и среднесрочную перспективу, описаны способы их применения в зависимости от военно-стратегической обстановки, силы и средства, необходимые для достижения превосходства над противником в военных операциях XXI века.

В основу принятой стратегии было положено полное превосходство над противником, достигаемое не за счет подавляющего перевеса сил и средств, а за счет создания необходимых условий для более эффективного их применения даже в условиях недостатка сил.

Новой стратегией развития вооруженных сил США признавалось необходимым их преобразование в единые сетецентричные и распределенные силы на основе качественного совершенствования системы сбора, обработки и распределения информации. С этого времени Пентагон приступил к развертыванию глобальной информационной сети и практической отработке технологий нового вида войн — сетецентричной (сетецентрической, сетевой) войны [224] (2008).

отрицательные стороны концепции сетецентрической войны — космическая и воздушная разведки коалиционной группировки противника не обнаружила из-за применения иракцами классических способов маскировки, а также учета времени пролета космического аппарата разведки. Основной вывод, который был сделан американцами из произошедшего, состоял в том, что батальонная оперативная группа перемещалась быстрее информации, получаемой разведслужбами.

Штаб коалиционных сил, находившийся в Кувейте, имел полную картину, складывающуюся на текущие сутки, но непосредственно на местах командиры такой информации не имели. По мнению американцев, одной из основных причин такого несовпадения являлись недостатки архитектуры автоматизированной системы управления. Действительно, единственным способом получить разведданные в реальном масштабе времени для войскового командира было остановить войсковую колонну и войти в связь с терминалом армейской системы мобильной связи. Процесс подключения мог занимать до нескольких часов. Такое положение дел приводило к тому, что вступать в бой приходилось практически вслепую либо применять классические способы и приемы войсковой разведки.

В ходе боевых действий был выявлен ряд недостатков созданной системы сбора, обработки и передачи данных, особенно в АСУ тактического звена. Например, оказалось, что многие радиостанции не совместимы друг с другом. Проявились трудности в управлении мобильными действиями войск, потребовались более компактные и защищенные машины и др. Но в целом система была признана достаточно эффективной.

Общая сумма денег, израсходованных в США на реализацию идей сетецентризма, скоро превысит триллион долларов. Между тем многие специалисты считают, что сетецентрическая война в ее нынешнем исполнении — афера века. И нужна она прежде всего тем, кто связан с производством сверхмощных ЭВМ и компьютерных программ. Каким бы совершенным ни был компьютер, «зависнуть» он может в любой момент. Действительно, военный Интернет не реагирует на внешнее радиоэлектронное противодействие, но он абсолютно беспомощен перед угрозой внутреннего вторжения. Сетецентрическую войну в ее нынешнем виде может выиграть один человек, имеющий USB с супервирусом и доступ к вражеской сети интернет-управления. Однако и зарубежные, и отечественные специалисты зачастую игнорируют

опасность профессиональной хакерской атаки. Утверждается, что можно создать абсолютную антивирусную защиту [179] (2012).

противодействие концепции сетецентричной войны — невозможно без эффективного решения вопросов создания трех ключевых компонентов:

1) сверхнадежной коммуникационной среды, обеспечивающей эффективное функционирование компьютерных сетей воинских формирований и их объединение в глобальную информационную сеть ВС РФ;

2) распределенной в пространстве группировки средств разведки, управляемых, достаточно информативных, надежных, долговечных и малозаметных для противника, объединенных в общую компьютерную сеть;

3) распределенной программной среды, обеспечивающей в реальном времени комплексную многоуровневую интеллектуальную обработку потоков малоинформативных и порой противоречивых первичных сведений о проявлениях объектов, а также позволяющей при необходимости оперативно изменять логику этой обработки по мере изменения состава и возможностей средств разведки, получения новых знаний о контролируемой группировке и т.п. [224] (2008).

недостатки концепции сетецентрической войны — в доктрине «Единый взгляд 2020» американскими военными выделяются элементы, большая часть которых в той или иной степени связана с человеческим фактором: эффекты опасности и напряжения, наличие неопределенности и случайности, непредсказуемые действия других участников боя, недостатки техники и недостаток информации, люди.

Характерно, что даже по самому «технологически зависимому» пункту американские специалисты замечают, что совместимость технических средств («интероперабельность») является необходимым, но не достаточным условием для обеспечения эффективности операций. Немаловажную роль здесь играет способность лиц, принимающих решения, правильно оценивать возможности друг друга и учитывать ограничения, исходящие от процедурных и организационных элементов.

В целом при изучении американских документов, посвященных перспективному облику вооруженных сил, складывается впечатление, что их авторов больше занимают проблемы, связанные именно с человеческим фактором. Вся концепция сетецентрических войн, если аб-

страгироваться от фантастических проектов, связанных с ней или приписываемых ей, стоит на двух «китах»: обеспечении военных руководителей всей полнотой информации о боевой обстановке и повышении активности и боевых возможностей самых мелких подразделений, составляющих, тем не менее, основу боевых порядков и несущих наибольшую нагрузку в бою.

Информационное превосходство, как свидетельствует доктрина, например, ценно не само по себе, а для достижения «превосходства в решениях — лучших решениях, принятых и реализованных быстрее, чем соперник мог отреагировать (на них)...». Ничего особо «революционного» в этом положении нет: командиры всегда стремились принимать решения на основе как можно более полной информации о противнике. Но даже в этом случае, на что обращает внимание устав FM 22-100, количество информации и быстрота ее прохождения не является безусловным благом, поскольку большие объемы данных серьезно «нагружают» органы чувств и психику, что ведет к быстрому утомлению и переутомлению лиц, принимающих решения: «...необходимо учитывать влияние техники на время, за которое вы должны анализировать проблемы, принимать решения и действовать. События сегодня протекают быстрее, и вы обнаружите, что уровень стресса у армейского руководителя соответственно возрастает... Психологическое давление, сопровождающее принятие решения, растет, в то время как время для проверки и подтверждения информации сокращается».

Концепция сетецентрических войн не представляет собой ничего революционно нового, являясь логическим развитием существовавших в военной науке подходов, спроецированных на расширение возможностей систем вооружения и средств коммуникации. Анализ американской доктрины перспективного развития вооруженных сил и документов военного управления показывает, что в центре вооруженной борьбы продолжает оставаться человек, требования к подготовке которого растут пропорционально качественному совершенствованию эксплуатируемой им боевой техники [123] (2014).

3.2.3. Сетецентрицеская война в терминологии разных стран

сетецентрическая война, терминология других стран — ВС других стран имеют свою собственную терминологию для определения этой оперативно-стратегической категории. Например, командова-

ние ОВС НАТО использует термин «сетецентрические возможности ВС» (Network Centric Capability, NCC); командование ВС Великобритании — «комплексные сетевые возможности ВС» (Network Enabled Capability, NEC); командование ВС Франции — «информационно-центрическая война» (Info-Centric Warfare, ICW); командование ВС Австралии — «комплексная сетевая война» (Network Enabled Warfare, NEW). Командование ВС Нидерландов разработало оперативную концепцию «сетецентрические операции» (Network Centric Operations, NCO), а командование ВС Швеции — концепцию «оборона (защита), базирующаяся на использовании сетей связи», или «сетевая защита (оборона)» (Networked Based Defense, NBD). В некоторых странах применяются и другие понятия, например, «научно-обоснованные управление и контроль» (Knowledge-Based Command and Control, KBCC) [57] (2006).

комплексные сетевые возможности НАТО [NATO Network Enabled Capabilities, NNEC] — концепция, предназначенная для решения вопросов организации взаимодействия высокотехнологичных формирований национальных вооруженных сил в современных и будущих вооруженных конфликтах.

Основные положения новой концепции были отражены еще в 2005 году в документе «Defense Requirements Review». Главной ее целью является внедрение перспективных информационных технологий в военную сферу для противодействия современным вызовам и угрозам национальной и коалиционной безопасности.

По мнению зарубежных военных экспертов, реализация новой концепции НАТО позволит осуществлять эффективное информационно-разведывательное обеспечение всего возможного спектра операций. Вместе с тем военные специалисты НАТО подчеркивают, что NNEC — это не только интеграция систем управления и связи, но и возможность повысить уровень взаимодействия всех участников операции (боевых действий), в том числе и средств поражения, органов и пунктов материально-технического обеспечения и др. В конечном же счете достигается необходимый уровень боевых возможностей перспективных формирований [117] (2009).

глобальная информационная инфраструктура — система для вооруженных сил Великобритании, представляющая собой единую информационно-управляющую сеть со специализированными систе-

мами обеспечения безопасности и единым семейством программного инструментария.

В будущем возможности формируемой информационной инфраструктуры планируется расширить и для организации взаимодействия и обеспечения доступа к информационным ресурсам вооруженных сил союзников: США, Канады, Новой Зеландии и Австралии [117] (2009).

сетевые возможности [Network Enabled Capability] — сетецентрическая концепция ВС Великобритании [116] (2008).

система оснащения и вооружения личного состава [Infanterist der Zuknft] — перспективная система Бундесвера, позволяющая реализовать новые принципы управления и связи между боевыми формированиями и вышестоящими органами управления.

Проводимые работы включают разработку перспективных средств разведки, персональных компьютерных систем, систем управления и связи типа «тактический Интернет», дающих возможность организовать взаимодействие между аналоговыми средствами связи и цифровыми системами передачи данных [117] (2009).

информационно-центрическая война [Guerre Infocentre] — концепция Франции, которая в большей степени акцентирует внимание на информационных потоках, а не на собственно сетях (как принято у американцев).

Первоначально эта концепция реализовывалась в рамках программы «Перспективная воздушно-наземная система боевого управления», позволяющей объединить разнообразные боевые платформы для осуществления мероприятий объединенного огневого поражения объектов и целей [117] (2009).

сетецентрические операции [Network Centric Operation] — сетецентрическая концепция ВС Нидерландов [116] (2008).

сетецентрическая война (Австралия) [Network Centric Warfare] — сетецентрическая концепция ВС Австралии [116] (2008).

сетевая оборона [Network Based Defense] — сетецентрическая концепция ВС Швеции [116] (2008).

интегрированная сетевая и электронная война [Integrated Network-Electronic Warfare, INEW] — термин ВС Китая, отражающий

современную китайскую концепцию, сравнимую с концепцией «сетецентрической войны (операции)» ВС США [117] (2009).

система боевого управления, связи, вычислительной техники, разведки, наблюдения и огневого поражения [Command, Control, Communications, Computers, Intelligence, Surveillance, Recognizance & Kill] — сетецентрическая концепция ВС Китая [116] (2008).

ведение боевых действий в едином информационно-коммуникационном пространстве — трактовка подхода сетецентрической войны в отечественных источниках [116] (2008).

3.2.4. Сфера сетецентрической войны

сфера сетецентрической войны — совокупность информационной, физической и когнитивной сферы.

Информация будет поступать не от отдельных «платформ» (боевой техники, средств разведки, наблюдательных постов, групп разведки, вертолетов, авиации, ИСЗ и др.), а из информационной сферы, тесно связанной с двумя другими сферами (физической и когнитивной) [57] (2006).

сферы сетецентрической войны — сетецентризм в управлении реализуется только на пересечении четырех сфер — социальной, когнитивной, информационной и физической [200] (2014).

физическая сфера[1] — включает все силы и средства, действующие в традиционных сферах вооруженной борьбы (наземное, воздушное, морское и космическое пространство), а также информационно-коммуникационные сети этих сил [200] (2014).

физическая сфера[2] — место развития ситуации, на которую оказывается военное влияние.

В ней (на суше, в воде, воздухе и космосе) развертываются военные действия и действуют «физические платформы», соединенные коммуникационными сетями [57] (2006).

информационная сфера[2] — совокупность сенсоров и технологий сбора, обработки и передачи (обмена) информации.

Именно здесь осуществляется добывание и производство информации, формируются знания обстановки командирами и штабами воинских формирований [200] (2014).

информационная сфера[3] — в ней осуществляется обмен информацией, передача решений командира, контроль и управление войсками, формируются и накапливаются знания, представления о физической сфере, т.е. происходит ее отражение в виртуальной реальности.

В борьбе за информационное превосходство она является «основополагающим плацдармом». При этом разработчики теории сетецентрической войны считают, что информационное превосходство характеризует состояние информационной сферы, когда одна из сторон получает «превосходящие информационные позиции» [57] (2006).

когнитивная сфера — нематериальная сфера, отражающая способность командиров всех звеньев боевого управления адекватно и точно оценивать сложившуюся обстановку и принимать выверенные и максимально эффективные решения.

Элементами данной сферы являются качество подготовки, знания и опыт командного и личного состава, морально-психологическое состояние войск и их сплоченность, ситуационная осведомленность [200] (2014).

когнитивная (рационально-ментальная) сфера — складывается в умах участников конфликта и характеризуется, с одной стороны, такими понятиями, как представление, осознание, понимание, убеждение, ценности, а с другой — процессом принятия решений.

К этой же сфере относится лидерство, моральное состояние, сплоченность, уровень подготовки и боевого опыта, общественное мнение, мыслительные процессы командиров, способы принятия решений, интеллект и эрудицию [57] (2006).

3.2.5. Сетецентрическая система

модель сетецентрической войны[1] — система, состоящая из трех подсистем, имеющих структуру решетки: информационной, сенсорной (разведывательной) и боевой.

При этом основой системы считается первая подсистема, на которую накладываются вторая и третья. Элементами второй подсисте-

мы являются силы и средства разведки (на наш взгляд, она и является основной), а третьей — средства поражения, боевая техника и личный состав отдельных тактических подразделений, объединенные органами управления и командованием [57] (2006).

модель сетецентрической войны[2] — система, состоящая из трех решеток-подсистем: информационной, сенсорной и боевой.

Информационная решетка-подсистема пронизывает всю систему в полном объеме. Элементами **сенсорной** системы являются «сенсоры» (средства разведки), а элементами **боевой** решетки — средства поражения. Эти две группы элементов объединяются общими военными органами управления и командования.

Представление сетецентрической системы управления в качестве «решеток» и «сенсоров» не совсем качественно отражает ее основное содержание, и само понятие «сетецентрическая война» претерпит еще не одно изменение, потому что война — это конфликт, происходящий в форме вооруженного противоборства, военных (боевых) действий между вооруженными силами, при котором выживание противника не рассматривается в качестве граничного условия [27] (2014).

инфраструктура сетецентрической войны — в США по заказам министерства обороны активно проводится комплекс НИОКР в области новых средств автоматизации управления, связи и разведки, направленных на создание для вооруженных сил глобальной информационной инфраструктуры, функционирующей на базе системно-технологических решений, лежащих в основе сети Интернет [194] (2011).

сетецентричная система (СЦС) — центральное место и самостоятельная роль в сетецентричной войне отводится **информационной подсистеме**. В ней осуществляется прием информации сенсорной подсистемы, приказов, анализ, выработка решений по управлению воинскими формированиями, данных целеуказания, информации об обстановке для органов управления.

Сенсорную подсистему создают средства разведки и наблюдения. Обе подсистемы объединяются в **систему управления**.

Боевая подсистема, информированная об обстановке и целях, способна с получением данных от «сенсоров» и приказов немедленно осуществить маневр и поразить цели. Ее связь с информационной подсистемой обеспечит применение «роев» «простых» средств поражения и средств РЭБ.

Сетевая связь сенсорной, боевой подсистем, органов управления дает большую информированность компонентам сетецентричной системы, как системотехнической основы СЦВ. Сбор, накопление, обработка данных в динамике обеспечат командирам больше возможностей по восприятию действий противника, своих войск. Всестороннее, правильнее станут анализ, оценка обстановки. Появится возможность массирования и сил, и результатов. Подчеркнуто неприятие автоматического управления в боевых действиях, хотя представления о сетецентричности как об «абсолютном разуме» децентрализованно действующих в войне автоматов все же появляются.

Концепция предполагает, что управление станет оперативнее (сократится время на принятие и реализацию решений), огневое, тактическое взаимодействие — точнее. Организационный базис взаимодействия определяется как способность самоорганизации военных структур снизу для выполнения самостоятельно (инициативно) принимаемых задач.

Однако война не сетевое явление. Охватить военные действия сторон единой сетью невозможно; она, в принципе, не соответствует содержанию войны. Военные действия, информация являются категориями военной науки и практики. Адаптация частных технологических решений, даже сетевых, к организации и ведению боевых действий и операций, не означает, что они станут разновидностью сетевых процессов [95] (2010).

сетецентрическая система — единое информационно-коммуникационное пространство, объединяющее между собой сети разведки, связи и управления, сети средств поражения и подавления, а также сети боевого и тылового обеспечения.

Это принципиально увеличивает скорость принятия решений и боевого применения войск.

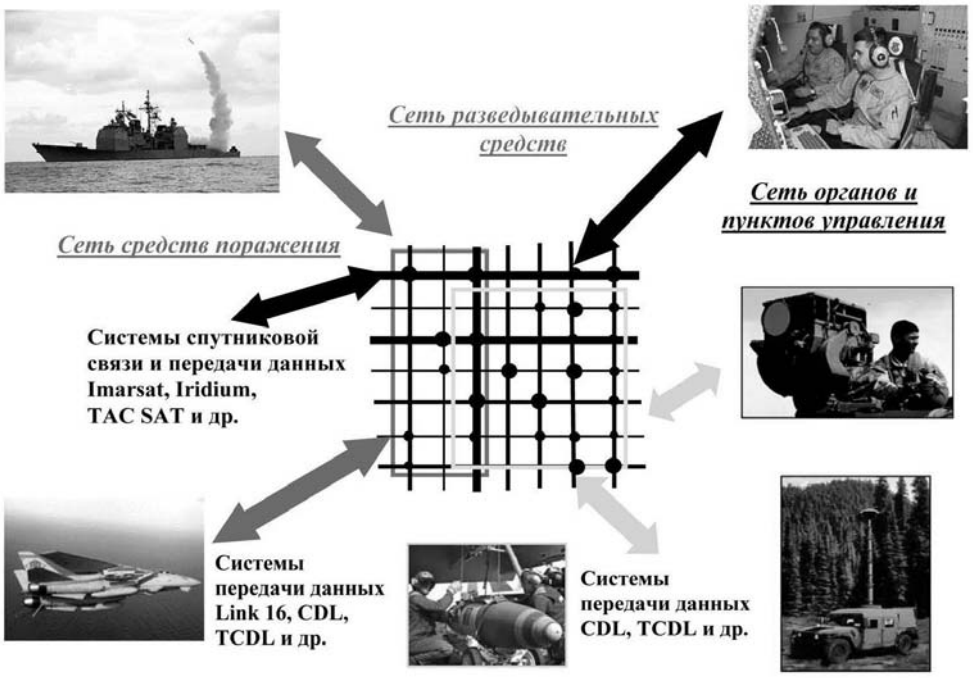
Сетецентрические системы вооруженной борьбы являются технической основной ведения сетецентрических войн [182] (2011).

боевое пространство[2] — сложная система, обеспечивающая надежное функционирование системы управления при наличии тесных и взаимопроникающих связей внутри себя.

Оно включает информационную, разведывательную и боевую подсистемы [148] (2008).

сетецентрические условия — информационно-коммуникационные элементы, объединяющие силы и средства вооруженной борьбы в систему [74] (2011).

объединенная разведывательно-ударная система — единая «система систем», функционирующая в едином информационном пространстве (рис.).



Объединенная разведывательно-ударная система

Разработчики новых сетецентрических концепций утверждают, что такие системы оказывают влияние не только на организацию и эффективность управления и разведки. Повышение боевых возможностей формирований является прямым следствием возрастания уровня информационного обмена и квалификации сотрудников. Одновременно с этим повышаются огневые, маневренные возможности формирований и их живучесть (в первую очередь на тактическом уровне).

Один из основоположников концепции Джон Гарстка отмечал, что «сетецентрическая война для войны то же самое, что электронный бизнес (e-business) для бизнеса» [117] (2009).

информационно-управляющая система (ИУС) — совокупность (интеграция) систем управления и разведывательно-информационного обеспечения.

Это понятие является основополагающим в концепции США «Сетецентрическая война» [75] (2017).

3.2.5.1. Информационная подсистема

единое глобальное (региональное, локальное) боевое информационное поле — концептуальная основа сетецентрических действий.

Оно постоянно подпитывается информацией посредством разветвленной системы сенсоров. Кроме того, непременное условие — его доступность для элементов боевых систем всех уровней военного искусства, а также наличие широкой сети рассредоточенных, высокомобильных боевых платформ и способных эффективно действовать на земле группировок войск [97] (2008).

единая глобальная информационная сеть — коммуникативно-информационное пространство для установления полного контроля и управления всеми участниками боевых действий [27] (2014).

единое информационное поле[1] — для получения достоверных данных требуется одновременное наблюдение цели с помощью различных средств. Именно поэтому для реализации концепции сетецентрической войны предполагается создать единое информационное поле, в котором все средства разведки действуют по единому замыслу в реальном масштабе времени.

Кроме этого, в единую информационную сеть входят системы передачи данных [179] (2012).

единое информационное поле[2] — в сетецентрических операциях каждая группировка непосредственно взаимодействует с любой другой через единое информационное поле. Командиры разновидовых боевых тактических групп, действующие в едином информационном поле, не могут принимать независимые от командиров других групп сети решения [181] (2008).

информационные поля (контуры) — множества соответствующей информации, в совокупности формирующие единое информационное пространство [180] (2005).

сетевая информационная инфраструктура — высокоэффективная информационная сеть, обеспечивающая организацию взаимодействия и информационного обмена среди всех участников операции (боевых действий) [117] (2009).

глобальная информационная решетка (ГИР) — основа информационно-коммуникационного пространства войны будущего, представляющая собой мощную группировку разведывательных, коммуникационных и навигационных космических летательных аппаратов США на околоземной орбите, а также воздушных судов, оснащенных новейшим оборудованием приема и передачи данных [179] (2012).

3.2.5.2. Сенсорная подсистема

видовая разведка — в вооруженных силах ведущих зарубежных стран — применение фото, оптико-электронных, радиолокационных и других средств разведки, позволяющих получать изображения местности или объектов [117] (2009).

3.2.5.3. Боевая подсистема

боевое пространство[3] — обладает объемными свойствами, так же как и сеть, построенная на трех уровнях в данном пространстве. Объединение в сети уровней информационно-разведывательных датчиков, ударных средств и органов управления посредством информационно-коммуникационной среды позволило достигать успеха в операции не за счет преимущества в количественных и огневых показателей группировок войск (сил), а в результате превосходства в информационных возможностях. Процессы управления в подобных операциях становятся более динамичными, отсутствуют паузы в действиях войск (непрерывное воздействие), а классическое понимание этапов операции заменяется многовариантностью, дальнейшей ее непредсказуемостью и возможностью изменения плана операции в ходе ее проведения [74] (2011).

3.2.6. Сетевые архитектуры в сетецентрической войне

таксономия — теория классификации и систематизации сложноорганизованных областей действительности, имеющих иерархическое строение.

Более того, таксономия может использоваться при планировании операций, организации возможных способов противодействия и строительстве своих вооруженных сил.

Одним из возможных подходов к изучению сетевых архитектур является таксономия сетей, базирующаяся на таких понятиях, как «равноценность» («неравноценность») и «однородность» («неоднородность»), а также подразделение таких архитектур на централизованную, запросную, стайную (в виде «роя») и на их комбинацию.

При данном подходе можно предположить, что сетевая архитектура равноценна, если все подключенные средства идентичны и потеря одного из них равнозначна потере другого. И наоборот, архитектура сети неравноценна, если одно подключенное средство имеет большую ценность по отношению к другим. Например, потеря самолета «Авакс» намного критичней, чем потеря одного контролируемого им истребителя. Следовательно, данная сетевая архитектура неравноценна и строится вокруг ключевого узла — «Авакса».

Другим критерием оценки может быть однородность и неоднородность сетевых архитектур. Можно предположить, что сетевая архитектура однородна, если все подключенные пользователи идентичны, и неоднородна при неидентичности пользователей. Между двумя этими понятиями есть определенный спектр состояний (горизонтальная ось). Комбинируя данный спектр с предыдущим критерием, можно получить «треугольник возможностей», потому что однородная архитектура может быть как «ценно-симметричной» (равноценной), так и неравноценной (с ключевым «хабом»).

Каждая из опций этого треугольника соответствует сетевой архитектуре. Можно выделить три типа основных сетевых архитектур: централизованная, архитектура сети «по запросу», стайная архитектура (архитектура «роя»). Вместе с тем наиболее реалистичными будут варианты, представляющие собой комбинации основных трех типов архитектур, так называемые смешанные архитектуры [116] (2008).

хаб — ключевой узел, обеспечивающий соединение всех пользователей сети и без которого сама сеть не может функционировать или ее возможности будут существенно ограничены.

«Хаб» одновременно является и концентратором или множителем возможностей отдельных средств, подключенных к сети, обеспечивая при этом синергетический эффект. В соответствии с теорией немецкого военного теоретика и историка Клаузевица такой «хаб» является центром тяжести сети (группировки) [116] (2008).

централизованная архитектура — архитектура, в которой используется один ценный «хаб», окруженный множеством других средств меньшей ценности.

Как правило, центральный «хаб» повышает возможности средств, которые он объединяет. Например, командование британских вооруженных сил во время конфликта на Фолклендах обнаружило, что объединение в сеть боевых самолетов с помощью центрального «хаба» в виде топливозаправщика повышает боевые возможности всего формирования.

Центральный «хаб» имеет периоды, когда он доступен и недоступен (отдых экипажа, дозаправка, ремонт и т.д.). И чтобы «хаб» был всегда доступен, необходимо как минимум три аналогичных узла для обеспечения операции в зоне ответственности. Например, до недавнего времени ВМС США имели на вооружении 12 авианосцев для одновременного обеспечения двух-трех океанских операций.

При применении централизованной архитектуры центральный «хаб», как правило, очень хорошо защищен, потому что боевые формирования не могут без него выполнять задачи. В свою очередь, уязвимость «хаба» требует отвлечения на его защиту определенных средств. Например, каждый авианосец сопровождают около восьми судов обеспечения (фрегаты, подводные лодки, крейсеры и др.). Несмотря на то что они оснащаются наступательным ракетным вооружением, основной их задачей является обеспечение безопасности центрального «хаба» (авианосца).

Иногда возникает закономерный вопрос: зачем рисковать таким дорогим узлом и отвлекать на его защиту значительные силы и средства? Объясняется это тем, что центральный «хаб» действует как «множитель», значительно повышая эффективность всего формирования. Здесь и проявляется синергетический эффект, когда центральный «хаб» объединяет средства (участников операции) для совместного

выполнения задачи. Это как раз тот случай, когда комбинированное действие двух или нескольких боевых средств превышает эффективность действия, оказываемого каждым средством в отдельности. Например, самолет «Авакс» значительно повышает возможности применения боевых самолетов.

Вместе с тем полностью централизованной система управления и связи может быть только тогда, когда решены основные оперативные и тактические задачи, «хаб» имеет доступ ко всей требуемой информации и необходимые возможности для подготовки принятия решения и быстрого распределения информации. Кроме того, такая полностью централизованная схема больше подходит для воздушного и морского пространства, но не для наземной операции, а ее применение с использованием такого «хаба» и концентрацией в нем большого количества средств управления и связи возможно и тем более уместно, если такой «хаб» предназначен для объединения средств разведки и наблюдения [116] (2008).

архитектура сети по запросу — архитектура, представляющая собой комбинацию одинаковых по ценности, но неоднородных сил.

Особенностью такой архитектуры является то, что она состоит из средств, имеющих узкую специализацию (средство разведки, средство управления, средство огневого поражения и т.д.), но высокое качество выполнения конкретного типа задач.

Например, запрос на уничтожение может быть направлен в секцию огневой координации (обеспечения), которая выбирает подходящее средство поражения. Средство огневого поражения, получив задачу, при необходимости запрашивает более точную информацию (координаты) от другого подключенного к сети средства разведки. По мере выполнения задачи формируется комплексная сеть запросов, которая требует наличия эффективной и устойчивой сети связи [116] (2008).

архитектура роя — архитектура, представляющая собой комбинацию полностью равноценных и однородных средств (сети боевых самолетов, морских кораблей, боевых машин пехоты, танков и т.д.).

Каждое из таких средств имеет свое (хотя и с ограниченными возможностями) средство разведки, средство поражения и средство связи и управления. Для эффективного выполнения задачи такие средства должны обмениваться между собой информацией, самоорганизовываться и самосинхронизироваться для повышения возможностей

подключенных средств. Иногда «рой» идентичных средств дополняется специальным центральным «хабом».

Архитектура «роя» свойственна и разведывательным сетям. Она применяется для организации обмена разведывательной информацией между отдельными средствами и ее распределения в интересах подготовки данных ситуационной осведомленности и синхронизации действий. При таком построении разведывательных сетей может применяться управляемый (Orchestrated Swarming), иерархический (Hierarchical Swarming) и распределенный (Distributed Swarming) «рой» [116] (2008).

управляемый рой — архитектура, в которой одно из средств выбирается в качестве временного «лидера» (разница с централизованной архитектурой в том, что все средства идентичны, т.е. равноценны и однородны).

Выбор центрального узла («лидера») осуществляется с учетом обстановки на поле боя и других факторов. Такой подход иногда применяется в группах сил специальных операций, где члены группы могут принимать управление на себя. В этом случае данные разведки посылаются средству-«лидеру», где они обрабатываются и интегрируются в данные о ситуационной осведомленности и определяется дальнейший план действий. Затем эта сформированная информация о ситуационной осведомленности распределяется между другими потребителями. В случае каких-либо непредвиденных ситуаций сеть может быть реконфигурирована и появится новый «лидер». Эта архитектура ограничивает количество пользователей сети, но предоставляет большие возможности по эффективному управлению [116] (2008).

иерархический рой — архитектура, близкая к традиционной централизованной архитектуре построения системы управления и наиболее подходящая для решения комплексных задач.

При использовании такой архитектуры построения общая картина данных ситуационной осведомленности и замысел операции (боя) подготавливаются центральным (командным) средством, спускаются вниз в тактическое звено, где они детализируются до необходимого командирам этого звена управления уровня. При отсутствии компьютеров такая архитектура была наиболее предпочтительной, но она не обеспечивала необходимую скорость принятия решения и управления подчиненными силами и средствами [116] (2008).

распределенный рой — архитектура, в которой нет центрального узла («лидера»), а все решения принимаются в результате достижения консенсуса или определенных договоренностей.

Каждое средство подготавливает свои данные о ситуационной осведомленности. Такое построение требует большой пропускной способности сети, но если сеть ее обеспечит, то будет достигнута и высокая эффективность управления [116] (2008).

смешанная архитектура — архитектура, использующая одновременно и архитектуру «роя» и архитектуру сети «по запросу».

Такой способ построения сети применяется при использовании равноценных и неоднородных средств (в чем-то схожих, в чем-то различных). Например, подразделения сил специальных операций имеют общие возможности, но одновременно с этим разную специализацию (медик, связист, взрывотехник и др.) [116] (2008).

объединенная сеть — архитектура, объединяющая в себе все имеющиеся сетевые архитектуры и присущая в первую очередь операциям объединенных сил.

Высокоценный «хаб» в такой объединенной архитектуре сети будет выполнять задачи именно «хаба», т.е. коммутатора. Группы равноценных и равнозначных средств будут объединяться архитектурой сети «рой» и использовать методы запроса, приемлемые для неоднородных сетей [116] (2008).

центр тяжести — базовый термин, уже давно используемый в военно-теоретических изысканиях ведущих зарубежных стран.

Немецкий военный теоретик и историк Клаузевиц первым начал обсуждать и создавать теорию центров тяжести, утверждая, что центр тяжести — это некоторая «центральная точка» вооруженных сил и государства, вокруг которой все и вращается. С другой стороны, доктор Стрэйндж и полковник ВС Великобритании Ричард Айрон в своей работе «Понимание центров тяжести и уязвимых элементов» отмечали, что «центральная точка», имеющая отношение к вооруженным силам противника, может быть как физической, так и моральной и может находиться на стратегическом, оперативном или тактическом уровне.

В доктрине НАТО центр тяжести описывается как потенциал или место, где государства, альянсы, боевые формирования или другие типы группировок концентрируют свои возможности для достижения

свободы действий, физической мощи (силы) и готовности вести борьбу [116] (2008).

3.3. Сетецентрические войска (силы)

сетецентричные силы — силы, способные реализовать концепцию сетецентричной войны [140] (2007).

сетецентричные свойства — свойства систем, средств, оружия, образующиеся в ходе их создания и модернизации с использованием методов, технологий интеллектуального управления, сетевого взаимодействия.

Группировкам войск эти свойства придаются при создании систем управления, связи, разведки, информационного обеспечения, интегрированных баз данных о противнике, целях, условиях выполнения боевых задач органов управления, разведки [95] (2010).

группировка войск в сетецентрической войне — состоит из четырех основных системообразующих компонентов:

1) автоматизированной системы управления войсками и оружием сетецентрического типа, основным предназначением которой является завоевание превосходства в управлении над противником;

2) основных исполнительных элементов, претворяющих в жизнь достигнутое АСУВ сетецентрического типа начальное информационное превосходство путем последующего непосредственного физического (огневого, радиоэлектронного, информационного) воздействия на соответствующие объекты противника;

3) сил и средств обеспечения боевых действий (разведки, радиационной, химической и биологической защиты, инженерного, тылового, технического, гидрометеорологического, топографического, морально-психологического обеспечения), создающих благоприятные условия для своевременной и качественной подготовки исполнительных элементов к выполнению поставленных (уточненных) боевых задач;

4) системы информационного обеспечения (коммуникационной системы связи и обмена данными), предоставляющей любым компонентам (элементам) группировки войск все виды необходимых данных с требуемым уровнем сервисных услуг [214] (2012).

3.3.1. Сетецентрические вооруженные силы

сетецентрическая стратегия — универсальный способ быстрого комплексирования в применении стратегических, оперативных и тактических ударных сил и средств при решении важнейших задач, а также идеальная база их взаимодействия.

При этом комплексирование реализуется по границе антропологического и технологического компонентов воинских формирований, а созданная суперсистема (система) вооруженной борьбы является принципиально интерактивной, человеко-машинной.

Для успешной реализации этой стратегии требуется надежное функционирование всех систем, поддерживающих существование боевого информационного поля, массированный взлом и развал боевых информационных систем противника, достижение превосходства в скорости и внезапности действий, а также ведение их без пауз в форме непрерывных, высокоскоростных операций и боев.

Стратегия обеспечивает массированную, стремительную, четко согласованную и автоматически управляемую атаку критических объектов противника стратегического и оперативного значения «стаями птиц», «роями насекомых» и даже *гетерогенными формированиями*, состоящими из «птиц», «насекомых», «акул» и «пираний».

В интересах реализации сетецентрической стратегии вооруженные силы развитых стран со второй половины XXI века могут принять структуру, показанную на рис. на с. 196.

Вооруженная борьба, видимо, будет иметь глобальный и объемный характер, вестись в космосе, на всех воздушно-космических направлениях, на земле, под землей и в водной среде, представлять собой сплошную цепь огневых ударов, информационных и защитных акций, реализуемых действующими по направлениям аэромобильными, высокомобильными сухопутными, амфибийными силами и специальными войсками [97] (2008).

гетерогенные формирования — неоднородные по составу формирования, включающие соединения и части, предназначенные для решения стратегических и оперативно-тактических задач в различных физических средах [97] (2008).

ударные стратегические силы — оперативные объединения ударных платформ смешанного, наземного, океанского (морского) и космического базирования [97] (2008).

Возможная структура вооруженных сил развитых стран
со второй половины XXI века

силы информационного обеспечения и противоборства — оперативное объединение обеспечения и поддержки глобального боевого информационного поля, объединение взлома информационных систем противника и объединение стратегической информационной защиты [97] (2008).

сухопутные силы — несколько оперативных объединений, имеющих комплексную структуру и сложную организацию.

Основу объединений могут составить разведывательно-боевые соединения ударных платформ оперативного назначения, а также линейные воздушно-наземные соединения, предназначенные для выполнения основных задач в ближнем бою [97] (2008).

силы воздушно-космического противоборства — оперативное объединение космического противоборства и несколько объединений воздушного противоборства [97] (2008).

силы океанско-морского противоборства — оперативные объединения океанских зон и обороны побережья [97] (2008).

воинские формирования видов и родов войск вооруженных сил — в оперативных объединениях всех этих трех видов вооруженных сил должны присутствовать соединения ударных платформ, соединения информационного противоборства, а также соответствующие комплекты соединений и частей родов войск, специальных войск и служб.

Тактические соединения и части, входящие в состав сухопутных сил, сил воздушно-космического и океанско-морского противоборства, а также аэромобильных и амфибийных войск в своей структуре, несомненно, будут иметь части и подразделения ударных, в основном летающих, боевых и транспортных платформ и информационного противоборства [97] (2008).

войска специального назначения — соединения и части вывода боевых формирований в районы оперативного предназначения, обеспечения их действий, а также боевые соединения и части, предназначенные для выполнения задач в стратегическом и оперативном тылу врага [97] (2008).

3.3.2. Сетецентрические воинские формирования

требования к организационной структуре общевойсковых соединений — структура должна, на наш взгляд, обеспечивать:

по адекватности — равенство боевых возможностей отечественных формирований и однотипных воинских формирований потенциального противника;

по гибкости — варьирование различных способов построения боевого порядка;

по защищенности — способность выполнять боевые задачи в любых условиях обстановки с применением всех видов оружия, сохраняя высокую автономность действий, живучесть и управляемость на поле боя;

по характеру воздействия — достаточные возможности, позволяющие эффективно осуществлять энергетическое и огневое поражение всех элементов построения боевого порядка противника в условиях сетецентрических действий [42] (2014).

автономный боевой модуль — бригада, способная к самостоятельному ведению боевых действий.

Достигается путем перехода от дивизий численностью в 15—20 тыс. человек к основным боевым элементам в виде небольших бригад (модульных групп) численностью 3—5 тыс. человек.

В определенных условиях боевой модуль может быть и более мелкого масштаба, например, отдельный батальон, усиленная рота и даже взвод или группа спецназа. Главное, чтобы она обладала необходимой степенью автономности и боевыми возможностями, позволяющими успешно выполнить поставленную задачу [180] (2005).

информационный модуль — воинское формирование, обеспечивающее взаимодействия между боевыми частями и командно-штабными центрами путем создания единого информационного пространства.

В задачи информационного модуля входят: обеспечение непрерывного управления; информирование своих войск и дезинформирование противника, нарушение его информационных сетей и защита своих; формирование нужного отображения реальности в общественном сознании, а также психологическое подавление противника. Исходя из содержания этих задач в состав информационного модуля, по нашему мнению, должны войти части и подразделения разведки и психологических операций, радиоэлектронной борьбы, информационного противоборства, группы космической поддержки, обслуживания АСУ и связи [180] (2005).

информационные войска — принципиально новые формирования для ведения сетевой войны, посредством которых будут формироваться автономные информационные модули.

Информационные войска на сегодняшний день аналогов не имеют, хотя очевидно, что в XXI веке невозможно добиться победы над противником, проиграв при этом информационную войну. Ярким тому подтверждением являются результаты боевых действий США и их союзников в Югославии и Ираке [180] (2005).

войска информационно-радиоэлектронной борьбы — целесообразно, на наш взгляд, подумать и о дальнейшем совершенствовании службы РЭБ ВС РФ, в частности о ее трансформации в такие войска.

В видах ВС США в 2001—2003 годах уже созданы органы (центры планирования информационных операций и управления ими), а в ВВС США — первые части информационной войны. Кроме того, определены силы и средства ведения информационной войны в воен-

ной области (силы и средства борьбы с системами боевого управления), основу которых составляют силы и средства радиоэлектронной войны [57] (2006).

командно-штабные центры — органы управления в сетевой организации, во-первых, выполняющие функции лишь координатора (диспетчера), а не руководителя, как в иерархических организациях, а во-вторых, принимающие решения на ведение боевых действий децентрализованно [180] (2005).

3.3.3. Сетецентрические воины

автономные роботы — роботы, создание которых реально в среднесрочной перспективе. Они могут получить возможность адаптироваться к окружающей среде и самостоятельно вести сражения, поскольку будут способны воспринимать и интерпретировать данные и принимать решения. Это означает, что они в состоянии не только заменить солдат на поле боя, но и взять на себя функции командования и управления. Независимое поведение уже сегодня свойственно многим компонентам оружия и робототехники. Однако в сочетании с возможностью самовоспроизводства искусственной жизни это может привести к возникновению вышедших из-под контроля войн.

С появлением автономных роботов реальными становятся также перспективы создания других форм рукотворной жизни. В классификации искусственных посредников, предложенной известным итальянским философом Лучиано Флориди, наиболее естественным типом, по природе своей ближе всего стоящим к человеку, считается семейство андроидов. За ними следуют киборги. Но андроидов с учетом возможности их создания, как нам представляется, следует все же поставить после роботов и киборгов [155] (2011).

киборги (кибернетические организмы) — подтверждают свою технологическую осуществимость результатами успешных экспериментов по вживлению искусственных органов чувств людям или систем внешнего управления животным. НАСА доказывает потенциальные преимущества «изменения, замещения и приращения организмов астронавтов экзогенными компонентами, чтобы сделать жизнь в космосе более удобной». В военной сфере киборги могли бы стать супер-

солдатами благодаря усилению бойцовских качеств обычных людей [155] (2011).

андроиды — это пока область научной фантастики. Однако успехи в генной инженерии и развитии информационных технологий дают надежду на практическую осуществимость биохимической имитации человека.

Цепочка роботы — киборги — андроиды отражает общую траекторию современного развития от механического, создаваемого каждый раз заново, к биологическому, способному воспроизводить себя самостоятельно [155] (2011).

3.4. Сетецентрические действия

сетецентрические боевые действия — концепция, ориентированная на повышение боевых возможностей разновидовых и разноведомственных вооруженных формирований в вооруженном противоборстве за счет достижения информационного превосходства, объединения участников боевых действий в единую сеть [218] (2015).

сетецентрические действия — ключевыми словами этого термина являются понятия «сеть» и «центр».

Под **сетью** здесь понимается встроенная в единое боевое информационное поле совокупность распределенных в существующих физических средах пространства ударно-огневых элементов различного назначения, а также средств использования результатов их ударов. Эта сеть может развертываться в глобальном, региональном и локальном масштабах.

Центрические действия подразумевают способность образуемой сетью боевой суперсистемы (системы) централизованно и в кратчайшие сроки концентрировать ее боевые усилия в любом районе мира, региона или поля боя в соответствии с определенной программой.

Другими словами, сетецентрические действия требуют разветвленной сети хорошо информированных, пространственно рассеянных, но способных к быстрой концентрации сил и средств.

Сетецентрические действия позволяют модернизировать способы ведения вооруженной борьбы на всех уровнях военного искусства. Традиционные способы ее ведения (длительное изнурение, последовательное или «одномоментное» сокрушение противника) в условиях ве-

дения сетецентричнеских действий трансформируются в новые, более скоротечные и более эффективные формы. Эти формы характеризуются двумя отличительными чертами: быстрота управления и самосинхронизация [97] (2008).

центрально-сетевые действия — удары, наносимые по отдельным ключевым элементам системы государственного и военного управления, частям и подразделениям «сил ответного удара (сил возмездия)» небольшими автономными и разнородными мобильными формированиями с последующим наращиванием их усилий основными силами.

Образно это можно представить так, как будто на всю страну будет «наброшена сеть» военных действий. «Узлы» данной сети — болевые точки государства, именно против них и будут вестись активные военные действия. При этом на остальной территории обороняющейся стороны активные наступательные действия могут вообще не проводиться.

Важнейшей особенностью ведения центрально-сетевых совместных действий являются заранее спланированные информационные кампании, операции и акции, целенаправленно проводимые в интересах дезорганизации системы государственного и военного управления, снижающие возможности противостоящей стороны по анализу данных о складывающейся военно-стратегической обстановке.

К новым положениям теории и практики ведения центрально-сетевых действий можно отнести:

— создание новых объединенных оперативных формирований, включающих в свой состав мобильные соединения и воинские части всех видов вооруженных сил;

— применение соединений сухопутных войск и кораблей военно-морских сил для поддержки действий военно-воздушных сил, а не наоборот, как это было до настоящего времени;

— повышение эффективности действий соединений и воинских частей специальных операций на всей территории противника в целях установления контроля над складами ядерного оружия и других видов оружия массового поражения, захвата (уничтожения) пусковых установок межконтинентальных баллистических ракет, самолетов стратегической авиации и атомных ракетоносных подводных лодок в пунктах (на аэродромах) базирования.

Важной особенностью центрально-сетевых военных (боевых) действий может явиться то, что в начальный период войны не будет приграничных общевойсковых сражений, но в глубине территории обороняющейся стороны очаговые боевые действия могут сопровождаться инцидентами, носящими характер псевдопартизанских (псевдотеррористических) действий, а также управляемыми техногенными катастрофами и спровоцированными выступлениями населения под сепаратистскими, религиозными, этническими и т.п. лозунгами [140] (2007).

центрально-сетевые совместные действия — действия, суть которых состоит в том, что смешанные (разновидовые) тактические группировки ОВС НАТО (ВС США), управляемые из единого стратегического центра, будут одновременно действовать по отдельным ключевым элементам системы государственного и военного управления, частям и подразделениям «сил ответного удара (возмездия)» на всей территории государства.

Захват стратегической инициативы предполагается осуществить с первых минут войны переносом боевых действий в стратегическую глубину обороняющихся войск: военные действия могут начаться не традиционно (с фронтальных приграничных столкновений передовых группировок вооруженных сил сторон), а в глубине территории обороняющейся стороны [70] (2004).

фазы ведения сетецентрической войны — в общем плане ведения сетецентрической войны применительно к любому театру военных действий предусматривается четыре основные фазы ведения боевых действий:

1) достижение информационного превосходства посредством опережающего уничтожения (вывода из строя, подавления) системы разведывательно-информационного обеспечения противника (средств и систем разведки, связи и передачи данных, сетеобразующих узлов, центров обработки информации и управления);

2) завоевание превосходства (господства) в воздушно-космической сфере за счет подавления (уничтожения) системы воздушно-космической обороны;

3) последовательное уничтожение оставшихся без управления и информации средств поражения противника, в первую очередь ракетных комплексов, авиации, артиллерии, бронетехники;

4) окончательное подавление или уничтожение очагов сопротивления противника [182] (2011).

быстрота управления[1] — в представлении американских специалистов подразумевает три аспекта.

Первый. Войска быстро достигают информационного превосходства.

Второй. Благодаря информационному превосходству над противником ВС претворяют в жизнь принцип массирования результатов, а не массирования сил (по нашему мнению, авторы имели в виду увеличение эффективности применения отдельных частей и подразделений, одновременно действующих по нескольким направлениям, вместо массирования сил на одном направлении).

Третий. В результате информационного воздействия противник лишается возможности вести успешные боевые действия и впадает в состояние шока [57] (2006).

быстрота управления[2] — подразумевает четыре аспекта:

Первый аспект — **завоевание информационного превосходства** за счет своевременного получения, постоянного обновления и более высокого уровня осознания поступающей информации и на основе этого достижение более глубокого понимания стратегической, оперативной и тактической обстановки, а также тенденций ее развития в интересах быстрого принятия оптимальных решений.

Второй аспект — решительная реализация **информационного превосходства над противником** посредством претворения в жизнь принципа массирования результатов, а не массирования сил. Реализация этого принципа дает возможность, применяя ограниченные силы, значительно быстрее добиваться того же эффекта, что и при применении крупных сил за счет принципиально нового уровня их качества и качества управления. Именно информационное превосходство дает возможность быстро и точно определять критические пункты функциональных систем противника и последовательно концентрировать против них рассеянные в пространстве ударно-огневые силы, упреждая его в защитных мерах. Кроме того, информационное превосходство позволяет концентрировать на поле боя боевые усилия средств поражения всех уровней — от стратегического до тактического, что может резко увеличить их эффективность и быстроту воздействия на критические объекты противника. Именно оно позволяет совершать стремительный упреждающий маневр для последовательного нанесения

мощных огневых ударов и немедленного использования их результатов. Все это в совокупности и создает условия для реализации принципа массирования результатов.

Третий аспект — **достижение шокового эффекта** с целью подчинить противника своей воле путем широкого, одновременного воздействия ударно-огневых средств по его многочисленным критическим объектам экономической, государственной и военной инфраструктуры или объектам оперативного и тактического значения.

Четвертый аспект — **немедленное закрепление достигнутого успеха** посредством быстрого взятия под контроль аэромобильными, высокоманевренными сухопутными, амфибийными силами и силами специального назначения отдельных ключевых районов территории противника, района проведения операции или поля боя, а также важнейших объектов [97] (2008).

принцип самосинхронизации структуры войск и их систем управления — взят авторами из теории сложных систем, в соответствии с которой все сложные явления, структуры и системы в наилучшей степени организуются по принципу «снизу-вверх» [57] (2006).

самосинхронизация[1] — термин взят не из понятийного аппарата военной науки. Это термин теории систем. Его аналогом в военной науке может быть термин «взаимодействие». Говоря о самосинхронизации, мы имеем в виду высшую степень взаимодействия [179] (2012).

самосинхронизация структуры войск и их систем управления — способность военной структуры и систем управления самоорганизовываться снизу, а не изменяться в соответствии с указанием сверху.

При этом авторы концепции считают, что структура войск (сил), формы и методы выполнения ими боевых задач, а также системы управления будут видоизменяться по своему усмотрению, но в соответствии с потребностями вышестоящего командования.

Далее авторы концепции полагают, что самосинхронизация позволит достичь превосходства над противником в скорости и внезапности действий; исчезнут тактические и оперативные паузы, которыми мог бы воспользоваться противник; все процессы управления и сами военные действия станут более динамичными, активными, результативными и приобретут форму не последовательных боев (операций) с оперативными паузами, а непрерывных высокоскоростных боевых действий с решительными целями [57] (2006).

самосинхронизация[2] — способность военной структуры реорганизовываться синхронно с изменениями обстановки снизу, а не изменяться в соответствии с указаниями сверху.

Другими словами, воинские формирования будущего должны иметь чрезвычайно гибкую организационно-штатную структуру и многофункциональный арсенал средств ведения вооруженной борьбы, позволяющие в зависимости от специфики решения боевых задач самостоятельно и быстро менять организационные формы, а также способы ведения вооруженной борьбы в интересах их эффективного выполнения с наименьшими затратами ресурсов.

Самосинхронизация позволяет достичь превосходства над противником в быстроте и внезапности действий, исключить тактические и оперативные паузы и превратить вооруженную борьбу в непрерывные и скоростные операции (боевые действия), преследующие исключительно решительные цели [97] (2008).

принцип сетецентричности — переход от фронтального противостояния к концентрации усилий в тех областях, где удается выявить уязвимость в вооружении и способах боевых действий противника, определение главного звена в системе его боевого построения и управления, нарушение которого и является целью действий войск.

Рассредоточение боевых усилий во времени и пространстве на многих направлениях, объемность, многосторонность воздействия на противника, согласованное применение разнородных и разновидовых сил и средств в бою составляют **содержание** принципа сетецентричности. В этом заключается его отличие от **принципа массирования**, при котором боевые усилия войск концентрируются на узком участке фронта и создается их плотная группировка.

Тактика сетецентрических действий предполагает решительную активизацию войск (сил) не на отдельных направлениях, а одновременно на всем боевом пространстве расположения противника, превращение поля боя в своего рода «муравейник», где по противостоящей стороне наносятся «роевые удары» неожиданными для нее способами [43] (2011).

сетецентричность — уход от фронтального противоборства. Достижение сетецентрического эффекта путем концентрации усилий на избранном направлении в сочетании с одновременным рассредоточением сил и средств на других направлениях в целях активизации всего боевого пространства и введения противника в заблуждение. Приме-

нение «роевой тактики», «тактики стаи», «тактики муравейника», «тактики боевых групп». Переход в тактическом звене от огневого воздействия по противнику к информационно-огневому и энергетическому. Увеличение глубины ближнего и дальнего боя. Трансформация факторов поля боя — скорости, времени, пространства, фронта и тыла, «цены успеха», «боевых и маневренных возможностей», соотношения сил и средств. Превалирование глубинного боя над ближним, неконтактных действий над контактными. Действия в длительном отрыве от своих войск, «с перевернутым фронтом», дерзкие аэромобильно-наземные рейды. Нацеленность действий войск на выявление и уничтожение «критических объектов» (пунктов управления и средств поражения) [43] (2011).

новая система взглядов на характер будущих операций и тактических действий — наступление новой эпохи в военном деле, когда появилась возможность решать тактические задачи, значительно возросшие по масштабу. Так, если раньше батальон армии США вел боевые действия в наступлении по фронту до 5 км, а в обороне батальонной тактической группе назначался район обороны 5—6 км по фронту и 8—12 км в глубину, то по опыту последних учений эти нормативы по фронту составляли соответственно 10 и 15 км.

Повышение требований к точности и качеству информационного обеспечения в целях выработки оптимальных управленческих решений.

Возникает необходимость разработки теории применения мобильных оперативных формирований и тактических соединений в новых условиях информационной эпохи [42] (2014).

сетецентричный принцип обнаружил — уничтожил — краткая образная формула, допускающая множественность понимания и требующая специальных исследований.

Она не может быть принята как нормативное определение. Методов, средств надежного автоматического и автоматизированного распознавания целей по информации технических средств разведки и наблюдения пока нет. По этой же причине принцип нельзя воплотить в конструкции и программах систем разведки и оружия. Проблемна реализация алгоритмов определения степени их опасности, важности и приоритета поражения, которые опираются на экспертные оценки и не имеют удовлетворительных программных решений [95] (2010).

3.4.1. Сетецентрические операции

характер современных операций — в настоящее время на содержание военных действий влияют две противоречивые тенденции: уменьшение количественного состава вооруженных сил и повышение боевых возможностей отдельных высокотехнологичных систем вооружения. Соответственно стала меняться и концепция ведения современной войны, заключающаяся в переходе от широкомасштабных «линейных» действий против многомиллионных армий противника к маневренной войне нового поколения. Акцент стал делаться на мобильность и максимальную реализацию боевых возможностей небольших группировок войск за счет новых возможностей систем разведки, управления и обеспечения.

Взаимодействие стали организовывать не путем объединения в решающих пунктах раздельных групп войск, а путем объединения их огневых и информационных возможностей. Это позволило впервые в истории военного искусства преодолеть пространственный, временной и информационный разрыв между войсками и органами управления.

Операции получают новое содержание, изначально предполагающее проведение быстрых и решительных маневров не только на флангах, но и в глубоком тылу противника [216] (2006).

сетецентрическая операция (СЦО) — военная операция, в которой используются самые современные информационные и сетевые технологии для интеграции географически рассредоточенных органов управления, средств разведки, наблюдения и целеуказания, а также группировок войск и средств поражения в высокоадаптивную глобальную систему.

СЦО позволяют повышать боевую эффективность формирований, состоящих из надежно связанных и хорошо информированных географически распределенных сил и средств. При этом повышение боевой эффективности обеспечивается достижением большей оперативности принятия решений и управления, снижением времени реакции средств огневого поражения, живучестью и оперативностью своих формирований[36] [5] (2014).

[36] Наставление КНШ JP 6-0 «Объединенные коммуникационные системы» от 10 июня 2010 года.

сетецентричная операция — операция, в которой в соответствии с ее замыслом и планом создается сетецентричная система, охватывающая разведку, информационное обеспечение, планирование ударов, связь, осуществляется сетецентричное управление, проводятся сетецентричные бои, сражения, удары и огневое поражение войск и критически важных объектов противника [95] (2010).

центрально-сетевые операции — зона многочисленных сражений, боев и ударов, проводимых рассредоточенными по всему пространству ТВД взаимосвязанными и взаимозависимыми тактическими группировками войск (сил).

При этом наличие единой информационно-управляющей среды позволяет рассматривать совокупность таких группировок как группировку оперативно-стратегического или стратегического масштаба. Количество сил, развернутых (базирующихся, дислоцирующихся) в конкретном объеме пространства, будет не столь существенно, как возможность по своевременному наращиванию ими усилий в любом районе боевых действий.

Поэтому, основным фактором, определяющим характер современных операций, является не соотношение пространства и численности вооруженных сил, а наличие новых межвидовых мобильных соединений и частей, реализующих свои потенциальные возможности на основе сетецентрических методов разведки, управления и обеспечения. Существующий с давних времен принцип сосредоточения сил и средств на решающем направлении трансформируется в принцип сосредоточения усилий, реализуемый не методом сосредоточения войск (сил) на избранном направлении, а главным образом путем массированного согласованного применения средств дальнего огневого, радиоэлектронного и информационного поражения. Командиру каждой из относительно автономных группировок (групп) нет необходимости иметь в непосредственном подчинении какие-то конкретные специфические дорогостоящие системы вооружения — ему лишь необходимо сделать через сеть заявку на их применение в заданном районе в заданное время для решения конкретной задачи или довести текущую обстановку до вышестоящего командира, который, владея большей информацией, может принять более корректное решение с привлечением более разнообразных и наиболее соответствующих складывающейся обстановке средств вооруженной борьбы.

Основная задача центрально-сетевых операций — с первых минут войны захватить стратегическую инициативу переносом боевых действий в стратегическую глубину обороняющихся войск и не дать возможности обороняющейся стороне осуществить не только стратегическое, но и оперативное развертывание своих группировок вооруженных сил. По существу, речь идет об операциях «молниеносной» войны нового поколения.

Особенностью центрально-сетевых операций является то, что сетецентрические методы разведки, управления и обеспечения позволяют применять силы и средства вооруженной борьбы не в одной линии приложения боевых усилий, а сразу во всей глубине театра военных действий соответственно своим боевым и маневренным возможностям. При этом совместное применение разновидовых группировок войск значительно повышает результативность операций [216] (2006).

сетецентричные боевые действия — совместные действия привлекаемых сил и средств разведки, информационного обеспечения, ударных (огневых) комплексов ВТО, систем связи и обмена данными по выполнению поставленных перед СЦС задач.

Сетецентричные боевые действия характерны созданием КОУ для каждого удара по целям [95] (2010).

сетецентричный огневой, ударный контур (КОУ) — кратковременный анклав в рамках СЦС, в котором происходит прямое сетевое взаимодействие привлекаемых сил для удара по конкретной цели в заданное время, сквозное от комплекса разведки до ударного комплекса.

Возникновение данного анклава (КОУ) санкционируется органом управления огневым поражением по данным доразведки и в соответствии с планами огневого поражения и РЭБ. КОУ формируется автоматически при наличии сопряженных в системотехническом отношении средств разведки, оружия, связи, информационного обеспечения, целераспределения, целеуказания, подготовки полетных заданий и эталонной разведывательной информации [95] (2010).

адаптивные операции — действия войск (сил), в которых были определены основные объекты удара, абсолютно достоверно в реальном масштабе времени разведано их местоположение и выявлены основные объекты системы ПВО; определены силы и средства для нане-

сения удара и на основании многократного моделирования выбраны наиболее эффективные способы их действий.

Полученные на моделях показатели эффективности и потерь вполне удовлетворили командование коалиционной группировки вооруженных сил США и НАТО. Последующий удар средствами воздушного нападения по выбранным объектам подтвердил результаты моделирования. Цель действий была достигнута в кратчайшие сроки и с минимальными потерями [224] (2008).

операция базовых эффектов (ОБЭ) [effects-based operations] — совокупности действий, направленных на формирование модели поведения союзников, нейтральных сил и противника в ситуации мира, кризиса и войны.

Проведение таких операций является центральной задачей ведения сетевых войн.

Ведение операций базовых эффектов означает заведомое установление полного и абсолютного контроля над всеми участниками актуальных или возможных боевых действий и тотальное манипулирование ими во всех ситуациях — как во время мира, так и во время войны. В этом вся суть сетевой войны — она не имеет начала и конца, она ведется постоянно, и ее цель — обеспечить тем, кто ее ведет, способность всестороннего управления всеми действующими силами человечества. Таким образом, проведение ОБЭ есть не что иное, как прямой планетарный контроль, направленный на достижение мирового господства нового типа, когда управлению подлежат не просто отдельные субъекты, а даже их мотивации, намерения и действия. Это проект глобальной манипуляции и тотального контроля в мировом масштабе.

Целевой установкой ОБЭ является формирование структуры поведения не только друзей, но также нейтральных сил и врагов. Таким образом, и враги, и занимающие нейтральную позицию силы по сути заведомо подчиняются навязанному сценарию, действуют не по своей воле, а по воле тех, кто осуществляет ОБЭ, т.е. США, и заведомо превращаются в управляемых марионеток еще до того, как следует окончательное их поражение. Операции базовых эффектов в равной мере применяются в период военных действий, в моменты кризиса и в периоды мира. Это означает тотальный характер сетевых войн. Они развязываются не в момент напряженного противостояния и в отношении противника, как классические войны прошлых лет, а намного раньше — в периоды мира и кризиса, и не только в отношении противника, но

и в отношении союзника или нейтральных сил с целью абсолютного контроля над всеми участниками исторического процесса в мировом масштабе [224] (2008).

3.4.2. Тактика сетецентрических действий

переход от современной тактики к тактике сетецентрических действий — смена устоявшихся ориентиров, исходный импульс для поиска новых решений.

Тенденция такова, что тактика как искусство боя становится все более свободной от нормативности и схематизма.

Осознать всю глубину происходящих на данном этапе преобразований, связанных с переходом современной тактики к тактике сетецентрических действий, можно на основе того, как происходит реформирование содержания их основополагающих принципов [43] (2011).

тактика сетецентрических действий — тактика в условиях меняющихся методов управления, которые с полной уверенностью можно охарактеризовать как сетецентрические, а также внедрения ВТО.

При этом методы сетецентрического управления являются производными от изменений в теории управления войсками (силами) в операции (бою), а применение ВТО зависит от уровня развития теории огневого поражения [42] (2014).

отличия тактики сетецентрических действий — система взаимодействия войск должна стать более адаптивной и гибкой, способной своевременно и эффективно реагировать на постоянные изменения обстановки.

Наличие ВТО позволяет вести боевые действия, основываясь на принципе не сосредоточения группировок войск (сил), а концентрации усилий, трансформации боевых действий в систему высокоточного поражения противника.

Качество подготовки тактических действий в условиях применения сетецентрических методов управления напрямую зависит от степени внедрения и освоения новых информационных технологий.

Разрешение противоречия между необходимостью сокращения объема боевого приказа или распоряжения и требованиями к его со-

держанию, которое должно включать и отражать всю сложность боевой обстановки.

При ведении сетецентрических тактических действий по существу должны остаться два способа разгрома противника: одновременное или последовательное поражение группировок его войск (сил). Способ одновременного поражения всех элементов тактического построения войск противника станет основным.

Боевые задачи частям и подразделениям будут в основном ставиться не по рубежам, а по объектам атаки.

Основная роль в достижении успеха будет принадлежать батальонам и бригадам, применяющим новые тактические приемы и обладающим тактической и особенно огневой самостоятельностью [42] (2014).

единение боевых усилий в информационно-коммуникационном пространстве — объединение боевых усилий «ударного блока» (средств поражения) со «вспомогательным блоком» (средствами обеспечения) по правилу «все в одном». Согласование действий «боевых модулей» (автономных боевых групп) в достижении общей цели через единое информационное поле боя, позволяющее поднять взаимодействие на качественно новый уровень, повысить степень согласованности и целенаправленность действий общевойсковых подразделений и частей со средствами поддержки. Модель сетецентрического взаимодействия заключается во взаимоувязке элементов сети (частей и соединений) с управляющим блоком, командно-штабным центром и блоком обеспечения (разведкой, РЭБ, РХБЗ, инженерным обеспечением) [43] (2011).

ударно-огневой маневр — основывается на триаде: превентивность, мобильность, внезапность. Цели маневра: концентрация и перераспределение усилий ударно-огневых средств с одного направления (объекта) на другое; эффективное использование результатов огневого поражения; своевременное сосредоточение, наращивание и перенос усилий; распределение ударов и огня для одновременного или последовательного захвата (поражения) одного или нескольких объектов в тактической глубине; маневр поражением, средствами РЭБ, инженерными заграждениями; противодействие маневру противника [43] (2011).

бой будущего — электронно-роботизированный бой.

В ближайшие годы войска будут оснащаться роботизированными средствами, достигающими уровня «искусственного интеллекта». Специалисты видят будущее робототехники главным образом в создании роботизированных боевых машин, способных действовать автономно и при этом самостоятельно «мыслить».

В частности, в армии США в ближайшей перспективе планируется применение безэкипажных транспортных средств для ведения разведки на переднем крае; роботизированных наземных средств для наблюдения и целеуказания; роботов-разведчиков; ДПЛА для наблюдения и целеуказания; БЛА для обнаружения минных полей; роботов-минеров; роботизированных средств постановки дымовых завес и проделывания проходов в минных полях; роботов-разведчиков водных преград; наземных роботизированных платформ; роботизированных средств для развертывания антенн; роботизированных вспомогательных средств постановки заграждений; летающих роботизированных платформ; роботизированных систем дегазации, дезактивации и дезинфекции боевой техники; вспомогательных средств для ремонта боевой техники, устройств для подачи артиллерийских снарядов; многоцелевых роботов и манипуляторов-погрузчиков боеприпасов; роботов-дозаправщиков; роботов-погрузчиков ракет на вертолеты; роботизированных устройств для загрузки боеприпасов в танк; систем обслуживания и обеспечения бронетехники; роботов-погрузчиков ядерных боеприпасов [38] (2002—2003).

синергетический эффект («эффект шока») — первоочередной вывод из строя «критических объектов»; достижение «энергетической внезапности» путем массового ввода в действие ранее неизвестных противнику видов оружия; неожиданное для противника создание зон энергетического поражения в уязвимых для него местах; применение новых способов боевых действий — нанесение «обезоруживающего», «мгновенного», «нарастающего» удара; массированная роботизированная атака (ввод в действие информационно-управляемых роботов) [43] (2011).

структурная защита — активно-упреждающий характер; ориентир на защиту не только от существующих, но и от перспективных видов оружия; комплексность защиты (сочетание тактических, технических и специальных мероприятий, направленных на противодействие радиоэлектронным, энергетическим ударам и информационно-психологическому воздействию противника). Блоки структурной защиты:

разведывательно-информационный; инженерно-технический; войсковой [43] (2011).

3.5. Сетецентрическое управление

сетецентричное управление — имеет два аспекта: первый — управление привлекаемыми силами и средствами при выполнении задач по предназначению на основе сетевых решений, охватывающих комплексы разведки, информационного обеспечения, пункты управления, ударные комплексы; второй — управление в операции созданием, функционированием и обеспечением СЦС и образуемых КОУ [95] (2010).

проблемы внедрения сетецентрических методов управления войсками (силами) — в обстановке широкого внедрения сетецентрических методов управления войсками (силами) обозначился ряд общих проблем, от решения которых напрямую зависит дальнейшая работа по обеспечению живучести системы управления общевойсковыми формированиями:

1) Возрастание возможностей противника по вскрытию и выведению из строя элементов системы управления современными средствами поражения наряду с постепенным переходом на *сетецентрические принципы организации управления*, предусматривающие увеличение числа источников первичной информации.

2) Стремительные темпы внедрения в процесс управления информационных технологий, компьютеризации и информатизации органов управления, что, с одной стороны, неизбежно приведет к созданию единого *информационного пространства*, в котором будут органически аккумулированы средства сбора, накопления, обработки, обмена и хранения информации всех уровней управления, а с другой стороны, повысится уязвимость элементов системы управления от электронного (огневого) воздействия противника, и, следовательно, снизится ее живучесть.

3) Недостаточная проработка современной теории живучести системы управления, в частности, понятийного аппарата, взаимосвязей и взаимозависимостей соответствующих мероприятий, проводимых органами управления различного уровня.

В частности, давно назрела необходимость уточнить само понятие «*живучесть системы управления*», которое в общем виде тракту-

ется как ее способность противостоять неблагоприятным воздействиям, адаптироваться к новым, изменившимся и, как правило, непредвиденным ситуациям, выполняя при этом свою целевую функцию за счет соответствующего изменения структуры и поведения[37]. Однако такое определение не дает четкого, однозначного толкования, не указывает, каким образом противостоять неблагоприятному воздействию противника и как адаптироваться к новым условиям, сохраняя необходимый уровень функционирования, что является наиболее актуальным вопросом в ходе подготовки и ведения боевых действий.

В военной терминологии, кроме термина «живучесть системы управления», используются понятия «обеспечение живучести системы управления», «повышение живучести системы управления», «сохранение живучести системы управления» и др. Некоторые из них приняты и закреплены руководящими документами и применяются в документообороте, однако также без достаточно полного и однозначного толкования этих понятий [130] (2014).

сетецентрические принципы организации управления — принципы, позволяющие реализовать режим ситуационной осведомленности благодаря формированию и поддержанию единой для всех уровней управления целостной, контекстной информационной среды и включению в процесс ее актуализации возможно большего числа источников первичной информации[38] [130] (2014).

сетецентрическая технология управления войсками — идея интеграции всех сил и средств в ЕИП, которая позволяет увеличить эффективность их боевого применения.

Внедрение сетевых технологий в военную сферу стало действительно революционным шагом, направленным на повышение боевых возможностей ВС, но уже не только за счет повышения огневых, маневренных и других характеристик индивидуальных платформ вооружения, а в первую очередь за счет сокращения цикла боевого управления, т.е. уменьшения времени на принятие решения [27] (2014).

интеграционное управление войсками и оружием — переход от иерархической строго централизованной системы управления к бо-

---

[37] Додонов А.Г. К вопросу живучести корпоративных информационных систем. Регистрация, хранение и обработка данных. М.: Инфра-М, 2004. С. 33—41.

[38] ГОСТ Р ИСО/МЭК 15026—2002. — *Прим. сост.:* в указанном стандарте термин не найден.

лее гибкой модели управления разновидовыми тактическими группами в едином информационном поле; смена алгоритма работы командира и штаба, переход от последовательного метода планирования к параллельному за счет автоматизации обработки информации; формирование единой цифровой карты оперативной обстановки, позволяющей повысить качество восприятия обстановки на поле боя, а также создания информационно-управляющей сети, где тесно связаны между собой органы управления и объекты управления; ввод в действие систем человек — оператор, человек — машина [43] (2011).

требования к управлению войсками и оружием в условиях сетецентризма — в содержании данных требований должны найти отражение следующие аспекты:

придание основным элементам оперативного построения войск большей самостоятельности;

достижение функциональной совместимости всех составных частей группировки войск;

обеспечение общей ситуационной осведомленности компонентов (элементов) группировки;

реализация максимальной согласованности в действиях компонентов (элементов) группировки [214] (2012).

тенденции развития процесса управления вооруженными силами — к основным из них можно отнести:

возможность воздействия на личный состав противника, участвующий в процессе управления, вплоть до «обезглавливания» руководства;

сокращение звеньев и самого цикла управления;

повышение эффективности, информативности и оперативности управления;

глобальное расширение информационного поля, вплоть до любого региона мира и даже космического пространства;

доступ к информации любого звена управления до командира взвода, отдельного боевого комплекса («платформы») включительно;

полнота, достоверность и актуальность информации, поступление ее к потребителю в реальном или близком к реальному масштабе времени в условиях визуализации поля боя;

бесшовная сопрягаемость систем информационной структуры и систем управления;

возможность опережающего принятия решений, полностью адекватных сложившейся оперативной (боевой, радиоэлектронной) обстановке;

перенос акцента вооруженного противостояния в информационно-интеллектуальную область [57] (2006).

сетецентричное планирование — при его рассмотрении выявляются этапы (как совокупность процессов): первый — планирование создания и функционирования СЦС и КОУ в операции; второй — планирование выполнения задач разведки, ударов, РЭБ с использованием СЦС, которое осуществляется в ходе общего планирования разведки, огневого поражения противника и РЭБ в операции; третий этап — как часть непосредственного и детального планирования применения средств разведки, огневого поражения, РЭБ, управления и связи (расчет параметров и условий формирования и функционирования КОУ) [95] (2010).

3.5.1. Система управления войсками

неиерархическая система управления войсками — необходимо четко уяснить принципиальное отличие иерархических структур от неиерархических. Для первых характерно наличие управляющих (командных) подсистем. Во вторых — управляющие функции распределены между всеми элементами или группами, когда каждая подсистема непосредственно взаимодействует с любой другой. Важная особенность неиерархических структур состоит в том, что в них нет подсистем, принимающих независимые от других подсистем решения [181] (2008).

сетецентрическая система управления — единое информационное пространство (ЕИП), состоящее из нескольких уровней.

Наземный (морской) уровень — это солдаты, танки, БМП, БТР, артилерийские и зенитные ракетные установки (наземные войска), экипированные и оснащенные системами связи и оптической разведки (камерами). Они являются одними из главных пользователей разведывательной информации. Каждый солдат благодаря единому информационному полю точно определяет свои координаты и расположение относительно «своих» и «чужих», наблюдает за происходящим как на всем поле боя, так и на отдельных его участках благодаря наличию оп-

тических систем, которыми экипируются все участники боевых действий.

Воздушный уровень можно разделить на две части. На малых высотах (до 2000 метров) основным действующим элементом информационного поля являются беспилотные летательные аппараты (БПЛА), которые в зависимости от предназначения могут вести оптическую и радиолокационную разведку или наносить точечные удары по группировкам противника. На высотах свыше 20 000 метров — это самолеты типа «АВАКС», ведущие всевозможные виды разведок и осуществляющие управление авиационной группировкой в районе ведения боевых действий, а также ударная составляющая (истребители, бомбардировщики, штурмовики и т.д.) в зависимости от решаемых задач.

Космический уровень составляют искусственные спутники Земли (ИСЗ), производящие фото- и видеосъемку земной поверхности, в частности участка ведения боевых действий, с последующей передачей информации на наземные или воздушные пункты управления в реальном или близком к реальному масштабу времени [27] (2014).

управление боевыми группами со стороны командно-штабного центра — координация действий боевых групп в рамках единого информационного поля.

И именно сосед «слева» и (или) «справа» будет обеспечивать боевые действия автономной боевой группы, а вот координацию этого обеспечения будет производить командно-штабной центр путем обслуживания заявок, поступающих от автономных групп. При этом необходимо заметить, что командиры боевых групп не всегда представляют, кто ими на самом деле управляет. Кроме того, решение на ведение боевых действий может осуществляться децентрализовано [181] (2008).

взаимодействие войск — единое информационное поле позволяет повысить качество восприятия текущей обстановки, создать единообразное для своих сил представление о текущей ситуации, поднять взаимодействие своих войск на качественно новый уровень, повысить степень согласованности и целенаправленности их действий [181] (2008).

3.5.2. Живучесть системы управления

живучесть системы управления войсками (силами) или ее отдельных элементов (органов управления, пунктов управления, средств управления) — ее (их) способность (свойство) сохранять или быстро восстанавливать свои функции в условиях воздействия различных средств поражения (подавления) противника[39] [130] (2014).

живучесть системы управления — ее свойство (способность) сохранять свои функциональные возможности в условиях ограниченных ресурсов в течение заданного времени путем проведения командованием, штабом, начальниками родов войск и специальных войск комплексных, взаимосвязанных мероприятий организационного, технического и морально-психологического характера.

Такая формулировка позволит, во-первых, четко определить содержание комплекса организационно-технических мероприятий путем конкретизации компонентов (критериев) живучести системы управления, а во-вторых — проводить прогноз ее живучести по обобщенному (интегральному) критерию — показателю эффективности управления.

Установлено, что в современных условиях подготовки и ведения боевых действий за показатели живучести системы управления целесообразно принять следующие компоненты ее состояния: защищенность, выживаемость и восстанавливаемость; а в плане эффективности — аспекты функционирования: боевую и техническую оперативность, боевую и техническую надежность и качество информационных технологий [130] (2014).

защищенность системы управления — способность противостоять вскрытию разведкой противника ее структурных элементов на всех уровнях, обеспечивать их надежную охрану и оборону, инженерное оборудование, маскировку и др. [130] (2014).

выживаемость системы управления — возможность сохранения необходимой степени ее работоспособности при нанесении противником огневых и радиоэлектронных ударов [130] (2014).

восстанавливаемость системы управления — свойство системы управления восстанавливать свою работоспособность до необхо-

[39] Военный энциклопедический словарь. М.: Воениздат, 2007. С. 258. — *Прим. сост.:* на указанной странице указан термин «живучесть» с другим определением.

димого уровня, обеспечивающего возможность выполнять свои функции после воздействия поражающих факторов [130] (2014).

боевая и техническая оперативность, боевая и техническая надежность и качество информационных технологий — способность системы управления эффективно функционировать в условиях применения противником электромагнитных излучений различного характера (электромагнитного оружия) и информационного оружия [130] (2014).

3.5.3. Работа должностных лиц

работа должностных лиц органов управления войсками и оружием по подготовке и принятию решений, доведению их до войск и выполнению в сетецентрической войне — последовательное выполнение ряда функций (задач), логически законченных и полностью обоснованных действий по обработке входных и формированию выходных событий.

Таковыми могут быть решение оценочных информационно-расчетных и прогнозных оперативно-тактических задач, работа с электронной картой местности и с базой данных, разработка боевых документов, нанесение огневых ударов и ударов войск, создание системы инженерных заграждений и т.д. [214] (2012).

информация для принятия решений — в современных условиях значительно увеличился объем информации, необходимой для принятия политических и военных решений, возросла и динамичность самой информации, поскольку она быстро устаревает. В современной операции командующему (командиру) для принятия адекватного решения необходима только свежая и точная информация в реальном масштабе времени, отражающая сложившуюся на данный момент оперативную (боевую, радиоэлектронную) обстановку. Сложность и динамичность информации требуют значительно больше времени для ее анализа, а современный характер боевых действий — принятия решений в возможно более короткие сроки, а в отдельных случаях — мгновенно.

Как оценивают специалисты ВС США, командующий объединением (в существующей пока еще системе управления) из-за дефицита времени принимает решение только на основе 30% обработанной его

штабом информации. В итоге боевой приказ (оперативная директива) не всегда адекватен складывающейся обстановке. Отсутствие полноты данных о противнике и своих войсках является нынешней традиционной особенностью организации управления ВС.

Объясняется это наличием раздельных «платформ», используемых для сбора, обработки и распределения информации, ее анализа, подготовки предложений командующему для принятия решения, планирования операции (боя), передачи боевых приказов (оперативных директив) и распоряжений войскам (т.е. для осуществления разведки и целеуказания, организации связи и боевого управления), что значительно сдерживает и ограничивает весь процесс управления вооруженными силами. Никакие системы сопряжения существующих разрозненных «платформ», даже в условиях автоматизации, не могут полностью обеспечить своевременного и тем более мгновенного принятия решения, адекватного сложившейся обстановке.

Поэтому вероятностный (предположительный) характер сведений о противнике и жизненная необходимость постоянного видения поля боя, а также исключительно высокие требования к обоснованности принимаемых решений — одно из острых противоречий управления современным боем. Неполнота данных о противнике и своих войсках, как никогда ранее, является недопустимой, так как ведет к росту неопределенности обстановки и ошибкам в принимаемых решениях [57] (2006).

3.6. Асимметричное противодействие в сетецентрической войне

асимметричные угрозы — использование фактора неожиданности во всех его оперативных и стратегических измерениях, а также использование оружия такими способами, которые не планируется США[40] [185] (2008).

асимметричность — противодействие противнику в захвате огневой и тактической инициативы, упреждение его в действиях по принципу «первым разведал — первым поразил»; применение по всей глубине расположения противника ВТО большой и малой дальности,

[40] Согласно определению Института национальных стратегических исследований Национального университета обороны Соединенных Штатов.

сопряжение действий средств поражения с системами разведывательно-информационного обеспечения; применение малых разведывательно-ударных БПЛА, наземных разведывательно-ударных комплексов, роботов; опережение противника циклом разведки, применение «сетевых» принципов управления оружием, применением энергетических ударов, оружия на новых физических принципах в сочетании с применением оружия ближнего и дальнего боя с оптическими, лазерными и радиолокационными системами наведения на цель; активность боевых действий во всех сферах — на земле, в воздухе, информационном пространстве; держать противника в постоянном напряжении; потребность в 3—7 раз увеличения глубины информационно-энергетического воздействия на противника и в 1,5—2 раза — интенсивности нанесения огневого удара [43] (2011).

ассиметричное направление развития ВВСТ в условиях ведения сетецентрической войны — создание образцов, обеспечивающих кратковременное воздействие с выводом из строя средств противника на определенный срок и резкий отказ от копирования сетецентрических систем противника с переходом на «ручное» управление в тактическом звене вплоть до батальона.

Направления развития эффективных средств для противодействия вероятному противнику в сетецентрической войне включают в себя перечисленные ниже.

В области **компоновочных решений** необходимо создавать образцы:

имеющие возможность разделения свойств (функций) по отдельным входящим в их состав элементам (подсистемам, машинам);

позволяющие образовывать не линейный, а плоскостной боевой порядок на достаточно большой площади («боевой рой»);

с уменьшенными массогабаритными характеристиками с целью увеличения количества целей для противника.

В области **совершенствования поражающей и подавляющей мощи** необходима разработка средств, обеспечивающих:

поражение воздушного противника над своей территорией — ждущих (кочующих) средств ПВО; БПЛА, действующих против крылатых ракет («птица Рух»); тактического ОМП бригадного (батальонного, ротного) звена (сверхмалых высотных боеприпасов воздушного взрыва);

воздействие на территорию (инфраструктуру) противника — ждущих (кочующих) средств артиллерии; тяжелых ударных БПЛА; тактического ОМП бригадного (батальонного, ротного) звена;

борьбу с сетецентрическим управлением противника, т.е. создание барьерных электромагнитных рубежей с боеприпасами, генерирующими электромагнитные волны в широком диапазоне, например, мины электромагнитного поля, или образцов для стрельбы реактивными снарядами, предназначенными для распыления (разброса) боевых элементов, агрессивных материалов или продуктов.

В области **защищенности** необходима разработка средств:

защиты подразделений на новых физических принципах (пучковые, ускорительные — «зонтики» над своими силами и средствами);

создания электронных образов ВВСТ;

аэрозольного противодействия, позволяющих «укутывать» подразделения в целом до роты включительно;

«активной» обороны — сверхмалых ракет и снарядов для борьбы против мини- и микроустройств противника; поверхностей с «активной» защитой, способных противодействовать проникающим средствам противника или уничтожать такие средства; «сторожевых» мини-, микро- и нанороботов для самых разных сред действия, включая космос, окружающую среду или даже клетки организма; летающих минных полей на основе БПЛА.

В области **мобильности** необходима разработка средств:

действующих в трехмерном пространстве (3D-оборона);

для динамической перегруппировки образцов при опасности огневого поражения площади, на которой они расположены;

для обеспечения защитного маневрирования.

В рамках **организации управления** по сетевому принципу в будущем потребуется создание и внедрение средств поддержки процедур коллективной выработки и принятия решений, а также алгоритмов для представления информации в виде визуально-ориентированных динамических моделей решаемых проблем, позволяющих вовлекать в решение задач интуитивные возможности и ассоциативное мышление людей. Такой порядок разведывательно-информационного обеспечения превращает каждое боевое средство в информационно-ударный (огневой) комплекс. При этом вывод из строя пункта управления может гораздо более длительное время не влиять на боевую устойчивость войскового формирования, поскольку сетевой принцип информационного взаимодействия исполнительных элементов позволяет им доволь-

но продолжительный период сохранять системные свойства группировки войск. Это особенно важно в современных условиях, когда значительно возросли возможности по дезорганизации системы управления войсками. Для реализации данной концепции каждое боевое средство должно быть оснащено специальным комплектом цифровых средств, включающих средства обработки данных, приемник навигационной системы, радиостанцию УКВ диапазона, радиосредства автоматизированной системы определения местоположения, опознавания и передачи данных [81] (2011).

3.7. Критика концепции сетецентрической войны

критика концепции сетецентрической войны — одни обозреватели ставят под сомнение эффективность «сетецентрических операций», их уместность в различных конфликтах, включая ближний бой в городских условиях. Другие оспаривают тезис о 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, ставятся вопросы: о совместимости информационных систем объединенных и коалиционных войск; о наличии достаточной емкости частот для «сетецентрических операций»; о возможности непредвиденных последствий, когда организации полагаются на системы, зависимые от информации и т.д.

Как показывает анализ открытых источников, в последнее время в американской печати значительно уменьшилось количество публикаций по вопросам «сетецентрических войн», появляются материалы критического характера. Некоторые эксперты предостерегают от превращения концепции «сетецентрической войны» в панацею.

Надежды Пентагона на то, что инновации принесут победу на поле боя так же, как они дают прибыль в бизнесе, несостоятельны, засилье технократизма в виде концепции «сетецентрической войны» ведет к следующим ошибкам:

— переоценка способности человека адекватно перерабатывать большой объем противоречивой информации;

— упрощенное видение противника через сведение его стратегии к асимметричным действиям;

— недостаточный учет изменчивой природы боя и неоправданная бюрократизация процесса управления;

— явная или неявная посылка, что военная победа есть конечная цель всей кампании.

Некоторые слабые стороны концепции «сетецентрических операций» представлены ниже [119] (2011).

механистический взгляд на природу войны — сторонники концепции «сетевых войн» имеют свою точку зрения на природу войны, весьма отличную от взглядов Карла фон Клаузевица и других классиков военной мысли. Они твердо убеждены в том, что ходом войны можно управлять, как работой хорошо сконструированной машины. Они считают, что в новую, информационную эру классическая военная теория потеряла свое значение. Между тем взгляды Клаузевица на характер войны остаются такими же актуальными, как они были в его время. Никакой технический прогресс, каким бы значительным он ни был, не может изменить истинную природу войны [119] (2011).

механическое перенесение моделей ведения бизнеса в военную сферу — идеи ведения «сетецентрических войн» были заимствованы из сферы бизнеса. Оппоненты концепции «сетецентрических войн» считают, что бизнес-схемы не могут быть применимы в военном деле, так как вооруженная борьба и бизнес, несмотря на некоторые сходные моменты, — это диаметрально противоположные сферы деятельности. Если в предпринимательской деятельности наиболее важным показателем является прибыль, то в вооруженной борьбе — боевая эффективность. Бизнес-модели в неизменном виде невозможно использовать даже в материально-техническом обеспечении военных действий. Условия рынка и условия боевой обстановки различаются между собой. Ошибки в доставке или невозможность доставить определенные товары на рынок не вызовут потери в живой силе или разрушение материальных средств, в то время как недостаток горючего, боеприпасов или воды может привести к неудачам в вооруженной борьбе и большим потерям в живой силе.

Вместо того чтобы сосредоточиться на проблемах управления войсками, говорят оппоненты, в вооруженных силах США делается упор на менеджмент и производительность, применяются методы количественной оценки действий войск в бою, используются термины из бизнеса для описания военной деятельности. Все это ведет к ослаблению внимания к вопросам управления войсками и ведению боевых действий [119] (2011).

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 господствующей роли в ущерб человеческим факторам, лежащим в основе процесса управления войсками, — говорят их оппоненты. — Слишком большое внимание к скорости управления может привести к поспешным и непродуманным решениям. Выигранное при этом время должно быть использовано для наилучшего анализа информации и планирования» [119] (2011).

ограниченные возможности для противоповстанческих действий в условиях города — когда сетецентрические действия ведутся против обычных, регулярных войск, датчики обнаруживают цель, передают информацию в систему принятия решений, выбирается имеющееся в наличии наиболее эффективное средство, и цель поражается. Однако, когда противник прячется за стенами, в коллекторах и внутри зданий, сетецентрическим датчикам будет трудно его обнаружить. Если противнику легче прятаться, чем американским войскам его находить, то американские войска становятся более уязвимыми [119] (2011).

недооценка противника — успех проведения «сетецентрических операций» в значительной степени зависит от развертывания системы датчиков для обнаружения движения и местоположения своих войск и войск противника. Однако в результате исследований пришли к выводу, что «по мере того как удаленные средства становятся более совершенными, возникает вероятность того, что вооруженные силы потенциального противника будут развивать контртехнологии и становиться более подготовленными в вопросах организации защиты, оборудования укрытий, обмана и радиоэлектронной борьбы. С учетом всего этого сетевой эффект на самом деле превратится в уменьшение знания обстановки и в конечном итоге ситуационной осведомленности на поле боя».

Противники Соединенных Штатов в Ираке и Афганистане предпринимали действия, чтобы обойти американские «сетецентрические» датчики и свести на нет их высокотехнологичное оружие. Примером этому может служить использование в террористических акциях смертников с минами замедленного действия, смешивание войск про-

тивника с местным населением, привлечение партизан и снайперов, которые, действуя на коротком расстоянии, наносили удары и затем быстро рассеивались.

Другими способами борьбы с противником, ведущим военные действия на основе единого информационно-коммуникационного пространства, могут быть: использование мощных устройств направленной энергии для подавления сигналов с коммерческих спутников, применение малогабаритных устройств направленной энергии, для того чтобы на расстоянии сжечь элементы компьютерных схем, а также введение в информационную сеть вредоносных компьютерных кодов с целью нарушить работу сложных систем оружия [119] (2011).

чрезмерная зависимость от информации — некоторые специалисты предостерегают, что значение огромных информационных ресурсов как средства разработки и проведения эффективных военных операций может быть переоценено и что процесс принятия важных военных решений нельзя сводить только к мыслительному анализу информации. Они утверждают, что дискуссии о трансформации вооруженных сил были чрезмерно сфокусированы на преимуществах, которые дает информация, и что виды вооруженных сил, органы обеспечения национальной безопасности и разведывательное сообщество не изучили как следует риски, связанные с военной доктриной, в основе которой лежит информация.

Вот некоторые проблемы, которые были подняты специалистами:

— опора на современные информационные системы может привести к самоуверенности управленческого персонала;

— количественные изменения в информации и ее анализе очень часто ведут к изменениям в поведении отдельных людей и организаций, которое иногда приводит к обратным результатам. Например, информационные технические средства позволяют обнаруживать большее количество целей, боеприпасы могут расходоваться быстрее, что ведет к большей зависимости от материально-технического обеспечения;

— обстановка, характеризующаяся обилием информации и возможностей, может изменить ценность информации, заставить пересмотреть цели военной миссии и, возможно, увеличить вероятность принятия ошибочных решений [119] (2011).

необходимость работы с чрезмерным объемом информации — распространение датчиков на поле боя создало проблему «перегруз-

ки информацией». Огромные потоки входящей информации могут ошеломить пользователей и создать угрозу для процесса принятия решения. Министерство обороны изучает вопрос использования центров «слияния информации», в котором будет применяться специальное программное обеспечение, для того чтобы фильтровать информацию о боевой обстановке, которая не нужна военнослужащим, ведущим боевые действия. Кроме того, для того чтобы обеспечить контроль и защиту радиочастот от помех противника, Центр электронных систем ВВС США работает над созданием универсального средства под названием «Система поддержки работы офицера по контролю единого информационного пространства, который будет управлять радиообменом в тактическом звене» [119] (2011).

увеличивающаяся сложность боевых систем — боевые системы и программное обеспечение становятся все более сложными. Программное обеспечение предназначено для обработки информации, определения положения противника и своих войск, комплекса целей, подачи сигнала тревоги, 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.

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, они увеличивают вероятность технических аварий, ошибок пользователей и других отказов в работе. Обычные технические сбои вполне естественно возникают в сложных системах. Частота обычных сбоев в работе увеличивается в зависимости от количества соединений в системе [119] (2011).

уязвимость программного обеспечения военного назначения и данных — военные компьютеры постоянно подвергаются атакам со стороны хакеров или других злоумышленников.

Существует растущее расхождение во мнениях по вопросу, должны ли вооруженные силы США полагаться на открытое, имеюще-

еся в продаже программное обеспечение общего доступа для выполнения функций командования, оперативного управления, связи в перспективных системах, предназначенных для танков, самолетов и других комплексов. Примером открытой программы является популярная компьютерная операционная система, известная под названием Линукс (Linux), разработанная международным сообществом программистов.

Агентство национальной безопасности США исследовало защищенную версию Линукса, но до сих пор не ясно, будут ли все военные компьютерные системы ограничены в соответствии с этим исследованием. Одни эксперты считают использование открытого программного обеспечения нарушением многих принципов безопасности: открытыми программами могут воспользоваться противники, которые тайно введут разрушительный код, для того чтобы вывести из строя комплексные информационные системы военного назначения. Другие эксперты с этим не согласны, утверждая, что именно потому, что Линукс открыто проверяется международным сообществом программистов, он обладает безопасностью, которая не может быть легко поставлена под угрозу со стороны иностранной организации. Открытый доступ многих участников является гарантией от внедрения вредоносного кода [119] (2011).

уязвимость боевой техники от воздействия средств радиоэлектронной борьбы — американские войска могут быть уязвимы от применения средств радиоэлектронной борьбы, в частности от электромагнитного импульса, который представляет собой кратковременное мощное электромагнитное поле, способное перегрузить или разрушить на расстоянии многочисленные электронные системы и высокотехнологичные микроцепи, особенно чувствительные к такому воздействию. Единичный, специально предназначенный ядерный взрыв малой мощности высоко над районом боевых действий может вызвать электромагнитный импульс, охватывающий большую площадь, и привести к разрушению электронных технических средств без потерь в живой силе, которые обычно возникают из-за взрывной волны или радиации. Такой же эффект электромагнитного импульса, но более ограниченного масштаба может быть произведен микроволновым устройством высокой мощности, приведенным в действие обычным взрывным устройством.

В настоящее время для тылового обеспечения действий американских войск и поддержки сложных боевых систем широко исполь-

зуются коммерческие электронные технические средства. Сейчас в вооруженных силах США значительный объем административной информации проходит через гражданский Интернет. Многие коммерческие спутники связи, особенно находящиеся на низкой орбите, могут снизить свои функциональные возможности или выйти из строя из-за электромагнитных ударов, наносимых с большой высоты. Для того чтобы в будущем уменьшить уязвимость коммерческих спутников, необходима специальная защита [119] (2011).

возможные информационные перегрузки — так, по мнению ряда военных экспертов, многократное увеличение количества средств разведки и как следствие существенное возрастание информационного потока может не только привести к информационным перегрузкам технических систем, но и создать серьезные проблемы в процессе принятия решений должностными лицами органов военного управления [117] (2009).

повышение комплексности и сложности формируемых систем — например, некоторое время назад была опубликована работа сотрудников университета Корнеги-Меллона, в которой утверждалось, что с возрастанием комплексности и сложности военных систем большинство из них станут «безразмерными», потому что будут включать огромное количество пользователей или заставлять (вынуждать) индивидуальных пользователей действовать совместно в сети даже в отсутствии необходимой для них информации [117] (2009).

критически уязвимые элементы сетецентрических военных действий — самым уязвимым элементом является информационно-коммуникационная сеть. Если нарушить работоспособность этой сети противника в целом, то он будет лишен не только возможности ведения военных действий такого характера, но и не сможет централизованно управлять всей группировкой войск (сил). Вывод же из строя отдельных элементов сети не приведет к должному эффекту, потому что одним из основных свойств сети является свойство ненарушения связи между сохранившимися элементами при прекращении функционирования отдельных ее элементов [74] (2011).

3.8. Доктрина «Единый взгляд 2020»

доктрина «Единый взгляд 2020» [Joint vision 2020] — концепция развития вооруженных сил, целью воплощения которой признается достижение «полного спектра доминирования» на театрах военных действий и на поле боя, которое должно достигаться «через взаимозависимое применение маневра, четкого взаимодействия, целенаправленного материально-технического обеспечения и всеобъемлющей защиты при приоритете маневра»[41] [123] (2014).

американская система воспитания военнослужащих — сердцем этой системы является категория эффективного лидерства, находящая отражение и на уровне языка, поскольку понятия «лидерство» и «руководство» в английском языке обозначаются одним словом. Это подтверждается одним из положений полевого устава армии США FM 22-100 Army Leadership: «Не имеет значения, какая техника у вас есть или как применение техники затронет вас в ближайшем будущем. Возможности техники по-прежнему зависят от ответов на те же основные вопросы, на которые пытались ответить руководители времен гражданской войны, когда их посылали в линию застрельщиков: Где я? Где мои друзья? Где враг? Как мне победить его?». Следует отметить, что указанный документ отличается именно направленностью на воспитание лидерства в среде руководящего состава армии США.

В качестве иллюстрации ограниченных возможностей техники устав приводит пример ошибки американской службы воздушной разведки, оснащенной новейшей на то время техникой, и, несмотря на это, не заметившей сосредоточения четвертьмиллионной китайской армии в 1950 году во время Корейской войны [123] (2014).

обязанности военных руководителей в сетецентрической войне — доктрина Joint vision 2020 подытоживает их так: «Во-первых, руководители Объединенных сил должны проанализировать и понять смысл единства части в контексте малых, широко рассредоточенных подразделений, которые сейчас только предвидятся. Во-вторых, лица, принимающие решения на всех уровнях, должны понять значение новых технологий, которые непрерывно работают в любых условиях, при том, что люди не способны на такую выносливость. В-третьих, что новые информационные технологии, системы и процедуры делают до-

[41] Joint vision 2020: America's Military: Preparing for Tomorrow.

ступной подробную информацию на всех уровнях подчиненности цепочки командования; руководители должны понять их значение для процессов принятия решений, обучения лиц, принимающих решения на всех уровнях, организационных структур и процедур» [123] (2014).

4. Автоматизированные системы управления войсками (силами)

автоматизированная система управления войсками (АСУВ) — автоматизированная система, основное предназначение который заключается в обеспечении качественного выполнения войсковыми формированиями боевых задач в интересах достижения целей операции (боя), проводимой общевойсковыми объединениями (соединениями, частями) [102] (1998).

автоматизированная система управления войсками (силами)[1] (АСУВ) — должна характеризоваться, во-первых, как система, предназначенная для повышения эффективности боевого применения войск (сил) и средств, управление которыми осуществляется с использованием АСУВ (боевая эффективность АСУВ), и во-вторых, как система, предназначенная для эффективного решения задач по обработке информации и управлению (функциональная эффективность АСУВ) [109] (2004).

автоматизированная система управления войсками (силами)[2] (АСУВ) — состоит из разнообразных технических, информационных и программных компонентов.

Функциональная составляющая АСУВ — программное обеспечение (ПО). Оно в свою очередь делится на общее программное обеспечение (ОПО), общесистемное программное обеспечение (ОСПО) и специальное программное обеспечение (СПО). Каждый из этих компонентов играет важную роль в обеспечении функционирования АСУВ, так как снижение качества любого из них по критерию «гарантированного результата» уменьшает возможности системы в целом.

ОПО и ОСПО обеспечивают функционирование системы в целом. СПО, которое разработчики называют «мозгами» системы, — основное средство расчетно-информационной поддержки (в перспективе и интеллектуальной) деятельности должностных лиц (ДЛ) органов военного управления (ОВУ).

Несмотря на существенную роль СПО в подготовке оптимальных в некотором смысле управленческих решений, построению системы расчетно-информационных задач и математических моделей, относящихся к категории специального математического обеспечения (СМО), на основе которого и формируется ПО, не всегда уделяется достаточное внимание. Иногда автоматизация сводится к внедрению в ОВУ компьютеров и разработке СПО АСУВ под сложившиеся ранее алгоритмы работы ДЛ. Это в корне противоречит самому понятию «автоматизация управления». В такой постановке роль ЭВМ сводится к функциям арифмометра или технического средства информационного обмена [210] (2012).

автоматизированные системы управления и связи — техническая основа управления войсками в настоящее время.

При значительном росте стоимости новейших видов оружия и военной техники достичь требуемой боевой мощи экономически выгоднее не путем количественного наращивания вооружений, а посредством обеспечения высокой степени автоматизации управления войсками и оружием, совершенствования разведки и РЭБ. Именно на этом принципе должны строиться Вооруженные Силы России и, соответственно, определяться пути развития систем управления оперативного звена [84] (2005).

4.1. Образцы автоматизированных систем военного назначения

автоматизация системы управления Вооруженными Силами — выполнение программ развития элементов системы управления, принятых в 90-х годах, должно было к началу XXI века существенно повысить эффективность управления.

Программы предусматривали создание систем стратегической и оперативной разведки, предупреждения о ракетном нападении, контроля космического пространства, принятия решений и санкционирования применения ядерного оружия, управления стратегическими ядерными силами, группировками войск (сил). Основной акцент как по срокам, так и по объемам финансирования делался на систему управления СЯС.

Практически к началу 90-х годов большинство планов и программ находилось в стадии завершения. Органы видов стратегической

и частично оперативной разведки приграничных военных округов и групп войск оснастили средствами автоматизации и вычислительной техники. Была создана АСУ фронта, армии и соединений Сухопутных войск. Планировалось производство разведывательно-ударных и огневых комплексов. В конце 80-х — начале 90-х годов стали проводить испытания автоматизированной системы управления стратегическими объединениями на ТВД, обеспечивающей управление объединениями различных видов ВС на Западном, Юго-Западном, Южном направлениях и Дальнем Востоке.

Совершенствование материальной базы управления осуществлялось путем внедрения средств вычислительной техники. Проводились работы по объединению вычислительных центров войск, создавалась информационная сеть, в штабах началось использование математических моделей операций, боевых действий.

Вместе с тем часть работ по созданию АСУ ВС выполнялась с заметным отставанием. Имели место параллелизм и дублирование разработок. Ведомственный подход привел к тому, что многие из них оказались несовместимыми между собой. Уже тогда стало очевидным: многие разработки не соответствуют заданным требованиям и не могут быть реализованы при существующем уровне базовых технических средств, а сами требования нередко субъективны и трудновыполнимы [19] (1996).

4.1.1. Автоматизированные системы высшего звена управления Вооруженными Силами

система «Экран» — большим шагом вперед в развитии ИС явилось создание в начале 1970-х годов под руководством В.И. Богатырева этой системы, которая была поставлена на объекты высшего звена управления Вооруженными Силами, а источниками информации являлись штабы округов (флотов) и групп войск. Система имела в своем составе все элементы и средства, присущие современным АСУ, а именно: сбора информации от удаленных источников; организации и ведения информации в системе; организации справочной службы; обработки картографической информации (информации об оперативной обстановке) с выдачей ее на экраны и табло коллективного пользования; защиты и разграничения доступа к ресурсам системы.

Система «Экран» была доведена до опытной эксплуатации на объекте Министерства обороны, где работала под управлением обслуживающей системы, разработанной коллективом Н.И. Рахманова.

В военно-научном сопровождении разработки и внедрении этих систем на объекты Министерства обороны принимали участие Х.И. Сайфетдинов, А.Я. Беляев, Н.В. Ястребов, М.М. Сапожников, Е.И. Пепеляев, В.П. Таран, А.М. Крюков, Л.В. Тришина и др. [99] (2009).

информационная система «СПО-397» — вершиной собственных разработок 27 ЦНИИ МО явилась данная ИС. Она разрабатывалась под руководством О.Н. Филиппова, при активном участии Ю.В. Гайковича, Г.Г. Белоногова, А.М. Бухтиярова, И.Л. Милешкина. В основу были положены получившие дальнейшее развитие методы и средства, реализованные в ИПС, разработанной под руководством Г.Г. Белоногова, и САК РЗ, разработанной под руководством Б.Н. Абрамова.

Система «СПО-397» имела все средства, необходимые для функционирования в АСУ, а именно: ведения баз данных; формирования документов; информационного обеспечения процессов решения моделей и задач; общения (диалога) пользователей с системой; управления функционированием системы; защиты и разграничения доступа к информации; повышения вычислительной устойчивости.

Отдельные компоненты этой системы разрабатывались под руководством А.П. Новоселова, Л.И. Озеранского, Л.И. Соколова, А.Н. Нечаева.

«СПО-397» была первой разработанной на базе ЕС ЭВМ системой, которая была доведена до практической реализации и в течение ряда лет использовалась в высшем звене управления, в вычислительных центрах (ВЦ) штабов округов (флотов) при проведении мероприятий оперативной подготовки, а также в органах государственного управления. Наибольший вклад во внедрение системы на объекты Министерства обороны внесли Е.И. Якутин, В.И. Ермолкин, А.Ю. Крупский, В.А. Середа, Л.И. Соколов, О.А. Афонин, Д.И. Сотсков, М.А. Лебусов, В.В. Золин, Ю.П. Калинин, О.В. Рысенко, И.Л. Калмыков, С.В. Бастанов, В.Б. Смольников и многие другие.

На последнем этапе создания системы ее компоненты были доведены до инструментальных средств, на базе которых можно было разрабатывать различного рода информационные системы, в том числе

автоматизированные информационно-управляющие системы. Это позволило придать новое качество системе в виде базовых автоматизированных средств обработки данных (БАСОД) «СПО-397».

В 1985 году за создание и внедрение на объекты Министерства обороны РФ системы информационного обмена, разработанной на базе БАСОД «СПО-397», В.Н. Козичеву и С.П. Селезневу в составе авторского коллектива была присуждена премия имени Ленинского комсомола [99] (2009).

командная система боевого управления (КСБУ) — автоматизированная система, которая связала между собой прежде всего стратегические ядерные силы (СЯС), а также силы и средства, имеющие в боевом составе тактическое ядерное оружие.

Данная система является аналогом Интернета того времени. Свойство сети сохранять свою работоспособность при разрушении большей части единиц сети обеспечивалось за счет математического обеспечения и протоколов системы обмена данных, созданных в Советском Союзе. в Ереване в 70-е годы XX века.

При отказе или уничтожении отдельных элементов КСБУ маршрутизатор перенаправлял команды на боевое применение ядерных сил и средств через сохранившиеся элементы КСБУ. Аналогичные принципы использовались при создании в 70-е годы прошлого столетия и еще ныне действующей системы ПВО города Москвы С-50.

Командная система боевого управления была построена как территориально распределенная вычислительная сеть. Вычислительные ресурсы КСБУ делились на три класса: комплексы средств автоматизации управления (КСА), комплексы средств автоматизации системы обмена данными (КСА СОД) и комплексы средств автоматизации объектов связи (КСА ОС).

КСА управления и КСА ОС являлись абонентами сети обмена данными, а КСА СОД — элементами самой сети КСБУ. Оконечными элементами КСБУ были объектовые, бортовые КСА, устанавливаемые на КП дивизий, полков РВСН и ДА, кораблях и подводных лодках ВМФ. Все КСА СОД были разделены на главные и территориальные. Главные КСА СОД объединены между собой по принципу каждый с каждым высокоскоростными каналами связи и представляли собой базовую систему обмена данными. Каждый территориальный КСА СОД имел выход на один из главных КСА СОД и по крайней мере еще на один из КСА СОД. Такая организация позволяла повысить живучесть

СОД до требуемых величин (требуемого времени доведения информации до абонентов с заданной вероятностью).

То есть уже в 60—70 годы прошлого столетия использовались отдельные свойства системы коммутации элементов сети, в большинстве случаев тогда выражавшиеся в наборе технических характеристик. Но кроме набора технических свойств сеть обладает еще рядом системных характеристик и набором свойств, комплексное использование которых и послужило толчком к информационной революции в военном деле: сеть обладает свойствами системы; она позволяет интегрировать потенциалы своих единиц (элементов); комбинации сочетающихся единиц сети приводят к появлению бесчисленного множества новых ее элементов; элементами сети могут стать любые объекты независимо от их расположения в пространстве; при прекращении функционирования отдельных элементов сети, связь между оставшимися ее элементами не нарушается [74] (2011).

автоматизированная информационная система «Глобус» — явилась наиболее развитой системой, созданной в институте для АСУ на основе СУБД диалоговой системы обработки данных (ДИСОД). Это многопользовательская ИС с интегрированной для нескольких предметных областей базой данных. Первые концептуальные положения по ее созданию были подготовлены в 1985 году Л.И. Озеранским и В.В. Богдановым, а работы по практической реализации начались в 1986 году и проводились под руководством Ю.Г. Уварова, В.В. Золина и В.Д. Шепеля.

АИС «Глобус» предназначена для работы с фактографической информацией и имела в своем составе полный набор функциональных средств, необходимых для эффективного функционирования АСУ. Ее база данных построена с использованием утвержденных ГШ классификаторов. В состав системы входили следующие подсистемы: управления информационно-вычислительными процессами; управления базой данных; формирования документов; информационного обслуживания моделей и задач; ведения архива документов; диалога с пользователями; организации взаимообмена информацией с объектами АСУ; обеспечения устойчивого функционирования; обеспечения безопасности.

АИС «Глобус» имела простой язык общения пользователей с системой, который базировался на использовании функциональной клавиатуры и элементов «подсказки». Средства, используемые в АИС «Гло-

бус», позволяли строить базы данных многопланового содержания с возможностью их расширения и развития.

Система находилась в опытной эксплуатации в ГШ, на протяжении ряда лет использовалась для проведения мероприятий оперативной подготовки и была включена в качестве функциональной подсистемы в состав информационно-расчетной системы Генерального штаба ВС РФ [99] (2009).

Графическая информационная подсистема Генерального штаба ВС (ГИП ГШ) — положительный опыт применения ЦОП ВАГШ и средств электронной картографии в 1990 году позволил задать предприятиям промышленности разработку опытного участка этой подсистемы Генерального штаба ВС. ГИП ГШ создавалась с целью автоматизации работы оперативного состава на объектах управления Генерального штаба ВС как дальнейшее развитие идей, заложенных при разработке ЦОП ВАГШ.

ГИП ГШ, введенная в эксплуатацию в 1992 году, предназначена для автоматизации процессов подготовки и ведения боевых графических документов, передачи оперативной информации между рабочими местами системы в локальных и региональной (по каналам связи) сетях передачи данных, ее хранения, документирования и отображения на средствах индивидуального и коллективного пользования в процессе повседневной деятельности и при проведении оперативных мероприятий.

ГИП ГШ включает в себя объекты управления нескольких уровней, объединенных в региональную сеть. Основу программного и информационного обеспечения комплекса средств автоматизации каждого объекта составляют графическая информационная система с комплектом электронных карт различной номенклатуры, обеспечивающая ведение оперативной обстановки на электронных картах; система меню, настраиваемая на потребности должностных лиц органов военного управления; средства телекоммуникации, обеспечивающие передачу информации между объектами ГИП ГШ.

Программные и информационные компоненты ГИП ГШ были разработаны сотрудниками института, которые принимали непосредственное участие и в работах по вводу в эксплуатацию объектов ГИП ГШ.

Опыт применения ГИП ГШ показал необходимость и своевременность ее создания с точки зрения потребностей повседневного

управления войсками. В 1990-е годы она была практически единственной системой, обеспечивающей постоянный и надежный обмен различного рода информацией между ГШ ВС, главными штабами видов ВС РФ, штабами военных округов, флотов, а также штабами соединений и частей. Исключительно важную роль ГИП ГШ сыграла в обеспечении управления войсками при ведении боевых действий в «горячих» точках, как в Российской Федерации, так и за рубежом, в том числе при проведении контртеррористической операции в Северо-Кавказском регионе [99] (2009).

Информационно-расчетная система Генерального штаба (ИРС ГШ) — предназначена для обеспечения руководства ВС и должностных лиц управлений Генерального штаба ВС данными о боевом и численном составе, положении, состоянии и возможностях войск (сил), их боевой и мобилизационной готовности, о результатах проведения оперативных расчетов и моделирования операций (боевых действий), а также необходимыми сведениями для прогнозирования военно-политической и военно-стратегической обстановки.

Под руководством Ю.Г. Уварова, В.Д. Шепеля, Ю.П. Калинина, В.В. Золина, Е.И. Якутина, А.А. Симоняна, Л.И. Озеранского осуществлялась разработка основных требований и проектных материалов по созданию ИРС ГШ. Кроме того, было разработано методическое обеспечение комплексных проверок системы.

В 1991—93 годах сотрудниками института были подготовлены исходные данные для создания опытного образца системы и разработаны макеты информационно-расчетных задач и моделей операций (боевых действий), многие из которых положены в основу специального математического и программного обеспечения (СМПО) системы.

В 1996—2000 годах при активном участии В.И. Котлярова, А.А. Иванова и других сотрудников института осуществлялась подготовка и проведение испытаний по переводу головного объекта ИРС ГШ на новую программно-техническую основу, а также проведение испытаний по проверке функционирования системы при переходе на даты нового тысячелетия [99] (2009).

4.1.2. Автоматизированные системы Главных и Центральных управлений Генерального штаба

Система информационного обеспечения расчетных задач — была создана в начале 1980-х годов для обеспечения данными комплекса задач планирования Главного оперативного управления Генерального штаба ВС. В ее разработке участвовали Б.А. Артамонов, Б.П. Симонов, И.В. Коротова и др. [99] (2009).

Информационная система обработки документов табельной отчетности — разработана в 1985 году в интересах Главного организационно-мобилизационного управления (ГОМУ) Генерального штаба ВС. Принятые при разработке системы решения обеспечили независимость прикладных программ от физической структуры данных. Это достигнуто за счет введения объектно-характеристических таблиц, в которых задаются структура входного документа, алгоритмы контроля, коррекции и обработки данных, структура выходного документа. Сочетание непрямых методов сбора информации, развитые средства контроля и коррекции информации и возможность настройки на обработку заданных структур данных обеспечили достаточную достоверность результатов и удобство системы в эксплуатации. В разработке системы принимали активное участие И.С. Федотов, А.Д. Чебыкин, С.Х. Шамсутдинов и др. [99] (2009).

Автоматизированная система ведения и обработки штатной информации (АСОШИ) — разрабатывалась под руководством А.И. Сизинцева в интересах ГОМУ Генерального штаба ВС и принята в эксплуатацию в 1983 году. Активное участие в разработке системы принимали В.Д. Шепель, А.В. Прибытков, М.Ю. Крюков, Г.Н. Седов и др. Создание системы явилось итогом многолетней совместной работы института и организационного управления ГОМУ Генерального штаба ВС по разработке системы классификации штатной информации, разработке и вводу в действие классификаторов, унификации и формализации штатов и перечней изменений.

Проделанные работы позволили найти общий подход к построению ИС с использованием компонентов СУБД и технологии проектирования баз данных. Были созданы развитые средства контроля и диагностики, удобные средства диалога, обеспечена высокая степень защиты и сохранности данных. Все корректировки базы данных регистрировались в журнале изменений. Максимальное использование класси-

фикаторов, являющихся элементами базы данных, позволило существенно сократить время поиска и выборки данных, сократить объем базы данных и упорядочить информационный процесс. Большой вклад в создание классификаторов и словарей для данной системы внесли Е.И. Пепеляев, Ю.И. Тимофеев, Н.В. Алтухова, Д.Д. Кирюшин и др. Система функционировала как в диалоговом, так и в пакетном режиме и была внедрена во все органы-разработчики штатов МО, оснащенные ЕС ЭВМ, что обеспечило переиздание и ввод в ЭВМ всех штатов военно-учетных специальностей ВС [99] (2009).

информационная система «Арбат» — значительным шагом в развитии идеологии построения и использования ИС в органах управления МО явилось создание этой ИС. Ее создание начато в 1988 году под руководством Ю.В. Гайковича и Ю.Н. Голубева. В дальнейшем эти работы велись под руководством И.И. Быстрова и Ю.П. Калинина.

ИС «Арбат» предназначалась для работы как с документальной, так и с фактографической информацией в административно-правовом контуре Управления делами министра обороны, в секретариатах заместителей министра обороны и в секретариатах Главных и Центральных управлений Министерства обороны. Она явилась первой системой, созданной для персональных ЭВМ (ПЭВМ), работающих в рамках локальных вычислительных сетей (ЛВС). При ее создании использовались инструментальные средства ИРИС и СУБД CLIPPER. В процессе создания системы унифицированы электронные формы документов аппаратов министра обороны и его заместителей; объединены в ЛВС рабочие места должностных лиц, а ЛВС связаны между собой; построены распределенные базы данных (РБД) в рамках ЛВС; внедрены в ИС элементы искусственного интеллекта.

Первая очередь ИС сдана в эксплуатацию на объектах ряда главных и центральных управлений Министерства обороны. Опыт ее создания и применения позволил усовершенствовать методы работы должностных лиц с информацией и повысить эффективность ее использования.

Дальнейшее развитие системы осуществлялось под руководством А.А. Иванова и В.Н. Каргина, сотрудниками института В.В. Бондаренко, В.Г. Лапшиным, В.Н. Козичевым, А.Н. Горбуновым и другими совместно с организациями промышленности. Работы были направлены на перевод ИС на новые защищенные технические (оптоволоконная сеть) и программные (операционная система МС ВС, СУБД «Линтер»)

средства. Исследовались также вопросы применения современных информационных технологий в ИС, методы построения единой для службы документационного обеспечения управления ВС информационной среды, создания и ведения нормативно-правового фонда ВС [99] (2009).

4.1.3. Автоматизированные системы управления Сухопутными войсками

Полевая автоматизированная система управления войсками — создавалась и совершенствовалась в 1970—80-х годах. В этой системе объединенными усилиями промышленности и научно-исследовательских институтов Минобороны были реализованы самые передовые для того времени идеи и технологии автоматизации управления войсками, в том числе и непосредственного управления войсками в ходе боевых действий. Комплексы средств автоматизации размещались на подвижных единицах, обеспечивали работу как в движении, так и на стоянке. При этом обеспечивалась приоритетная дисциплина обработки информации, в том числе и в условиях радиоэлектронного воздействия противника.

Информационная составляющая системы обеспечивала необходимыми данными как деятельность должностных лиц органов управления, так и проведение автоматизированных расчетов. При этом были созданы оригинальные и эффективные операционная система, система управления базами данных, система трансляции сообщений и другие, не уступавшие зарубежным аналогам. Адаптированные комплексы полевой автоматизированной системы управления войсками поставлялись не только в Вооруженные Силы СССР, но и в армии государств — участников Варшавского Договора.

Большой вклад в создание системы внесли сотрудники института Б.И. Стрельченко, А.П. Царев, В.Л. Феоктистов, Б.Б. Лазаренко, В.А. Романов, Ю.С. Лавринович, В.П. Лещинский, В.В. Сафонов, В.И. Ещенко и многие другие [99] (2009).

требования к автоматизированной системе управления Сухопутными войсками — сводятся к тому, что необходимо создавать целостную автоматизированную систему управления, которая должна охватывать все уровни управления от командования и штаба объединения (соединения) до отдельного военнослужащего. Кроме того, как

показал опыт контртеррористической операции в Северо-Кавказском регионе, такая система должна строиться на единой информационно-технической основе, позволяющей обеспечить эффективное управление группировками войск, которые состоят как из объединений, соединений и частей Сухопутных войск, так и войсковых формирований другой ведомственной принадлежности [150] (2004).

4.1.3.1. Перспективная автоматизированная система управления тактического звена

управление в тактическом звене — должно быть направлено (помимо повышения оперативности обработки значительных объемов информации) на разрешение противоречия между высокой маневренностью и живучестью войск и низкой подвижностью пунктов управления, их высокой уязвимостью от средств поражения и радиоэлектронного подавления противника, что возможно лишь путем внедрения АСУ войсками и оружием, построенной на базе современных средств и технологий приема, передачи, обработки и визуализации информации. При этом необходимо не просто совершенствование, а радикальное изменение всей системы управления с тем, чтобы она могла удовлетворять следующим оперативно-тактическим требованиям:

быть адаптивной, т.е. структура, состав и взаимосвязи элементов системы управления должны соответствовать условиям, в которых действуют соединения и части;

обладать высокой живучестью в условиях активного огневого и радиоэлектронного воздействия противника. Для этого пункты управления должны быть компактны и трудно отличимы от других элементов боевых порядков. Принципиально важно, чтобы командно-штабные машины (КШМ) по внешнему виду не отличались от боевых, а их мобильность и степень защиты были не ниже;

обеспечивать всестороннее обоснование принимаемых командиром решений с проведением в необходимом объеме оперативно-тактических расчетов, разработку планирующих документов, выполнение графических работ, в том числе и на картографическом фоне, а также своевременное доведение до подчиненных команд и распоряжений, поддержание надежной связи с взаимодействующими органами управления в реальном масштабе времени;

позволять командирам тактического звена оперативно менять, когда этого требует обстановка, свое местонахождение без потери (да-

же кратковременной) управления всеми имеющимися силами и средствами;

осуществлять передачу управления на дублирующие пункты управления за минимальное время и в полном объеме без каких-либо значительных изменений структуры системы управления;

обеспечивать скрытность управления, обладать малой вероятностью обнаружения и опознавания противником ее элементов, исключать возможность несанкционированного доступа в систему, перехвата и раскрытия информации [195] (2002).

автоматизированная система управления тактического звена — автоматизированная система управления, построенная на принципах распределенной обработки данных в локальных вычислительных сетях (ЛВС), состав элементов которой и их функциональные возможности позволяют адаптировать ее структуру к реальной обстановке без организационной и технической перестройки.

Для этого система должна иметь модульную структуру, а состав должностных лиц на ПУ и их техническое оснащение средствами автоматизации и связи для каждого модуля соответствовать определенному уровню иерархии системы управления.

В ходе боевых действий АСУ будет представлять собой совокупность модулей управления, рассредоточенных в пределах боевого порядка соединения (части) и объединенных в единую систему соответствующим комплексом средств автоматизации и связи. Каждый из модулей может размещаться в одной или нескольких КШМ.

Рассмотрим некоторые подходы к построению АСУ указанного типа на примере дивизионного звена управления. В структурном отношении она, на наш взгляд, может иметь: общевойсковую подсистему управления (включает субподсистемы — командную, управления разведкой, РЭБ, инженерным обеспечением, РХБЗ, связью, топогеодезическим обеспечением), а также подсистемы управления огневым поражением, ПВО, тыловым и техническим обеспечением.

Кроме того, для решения задач управления в АСУ следует предусмотреть возможность обмена информацией (в цифровом формате) между органами управления и должностными лицами; формирования единого информационного пространства поля боя с его отображением на электронных картах; обеспечения безопасности информации [195] (2002).

общевойсковая подсистема управления — центральная подсистема в АСУ, обеспечивающая сбор, обработку и отображение на электронных картах автоматизированных рабочих мест (АРМ) информации о положении и состоянии своих войск, противника, условиях боевых действий.

Поступающая от средств разведки, других источников информация о противнике обрабатывается в целях ее идентификации и распределяется по ПУ и АРМ должностных лиц с детализацией, необходимой для выполнения своих обязанностей. В общевойсковой подсистеме решаются задачи по оценке обстановки, определению замысла и формированию решения, планированию боя, а также по управлению войсками в ходе боя.

Ее командная субподсистема обеспечивает управление войсками и может иметь в своем составе по три пункта боевого управления (ПБУ) в дивизионном, полковом (бригадном) и батальонном звеньях управления и по одному — в ротном и взводном. Остальные подсистемы включают модули ПУ соответствующих начальников родов войск и служб, командиров подчиненных им подразделений, которые функционально объединены в ЛВС. Этим достигается дублирование органов управления, их приближение к объектам управления, что способствует повышению устойчивости и оперативности управления [195] (2002).

пункты боевого управления (ПБУ) — предназначаются для оперативного управления войсками в ходе боя. Оперативный состав таких пунктов размещается в одной КШМ, оборудованной на шасси основных боевых машин соединения (БТР, БМП), что обеспечивает их высокую мобильность, способность не выделяться из основной массы боевых машин, успешно использовать естественные укрытия и защитные свойства местности, своевременно выходить из зон огневого и радиоэлектронного воздействия противника. Расчеты пунктов боевого управления должны возглавлять первые лица командования соединения. При этом ПБУ, возглавляемый командиром, является основным, начальником штаба — запасным, а заместителем командира — резервным пунктом управления (на время совместного выполнения боевой задачи последний может действовать в интересах соединений и частей других видов ВС или силовых структур). Для обеспечения непрерывности управления на всех КШМ следует предусмотреть индикацию о

состоянии ПУ и о том, какой из них в данный момент является основным [195] (2002).

подсистема управления огневым поражением — подсистема, которая имеет пункт управления огневым поражением, включающий модули управления начальника артиллерии соединения, начальника группы боевого управления авиацией и начальника штаба артиллерийского полка.

Возглавлять этот ПУ должен начальник артиллерии. На этапе подготовки боевых действий здесь осуществляется общее планирование огневого поражения, а также непосредственное планирование ударов и огня для штатных, приданных и поддерживающих средств поражения. В ходе боевых действий имеющимся силам и средствам ставятся задачи на огневую поддержку войск. Наведение авиации на цели возлагается на передовых авиационных наводчиков, которые должны быть в каждом батальоне первого эшелона, располагаться в КШМ командиров батальонов и иметь комплекс средств связи с авиацией [195] (2002).

подсистема управления противовоздушной обороной — подсистема, которая включает пункт управления ПВО, объединенный в ЛВС с КП зенитного ракетного полка. На нем решаются задачи планирования ПВО и доведения результатов планирования (расположение позиций, зон ответственности, секторов и эшелонов высот обстрела целей) до нижестоящих ПУ и КП огневых комплексов [195] (2002).

подсистема управления тыловым обеспечением — подсистема, которая объединяет в ЛВС пункт управления начальника тыла и КП отдельного батальона материального обеспечения [195] (2002).

подсистема управления техническим обеспечением — подсистема, включающая пункт управления заместителя командира по вооружению и КП отдельного ремонтно-восстановительного батальона [195] (2002).

4.1.3.2. Автоматизированная система управления ракетными войсками и артиллерией

единая межвидовая автоматизированная система управления — ядро единой общевойсковой разведывательно-огневой системы

(РОС), обеспечивающей интеграцию средств РВиА со средствами поражения других родов войск.

К сожалению, в настоящее время эффективность ракетных ударов и огня артиллерии в значительной степени ограничена низким уровнем автоматизации управления РВиА. В частности, не автоматизировано управление противотанковой, полковой и батальонной артиллерией, частями и подразделениями технического, топогеодезического и метеорологического обеспечения [98] (1999).

основная задача АСУ РВиА — обеспечение внутреннего информационного взаимодействия, а также обеспечение взаимодействия с аналогичными системами других родов войск.

Поэтому проблема информационной совместимости по своей актуальности и значимости сегодня одна из важнейших. Суть проблемы, по нашему мнению, заключается в том, чтобы достичь информационной совместимости между различными типами комплексов средств автоматизации (КСА).

Опыт проектирования и создания КСА из состава АСУ РВиА для различных уровней управления позволил определить основные причины информационной несовместимости. К ним следует отнести: нарушение принципов системности, централизации и унификации при создании АСУ военных округов; несогласованность в вопросах проектирования и создания информационно-лингвистического обеспечения (ИЛО) АСУВ между научно-исследовательскими учреждениями (НИУ) МО, осуществляющими военно-научное сопровождение разработки, и предприятиями оборонного комплекса; нарушение технологии разработки основных видов обеспечения АСУВ (в первую очередь — информационно-лингвистического) [114] (2004).

недостатки создания АСУ РВиА — принятое в начале 90-х годов XX века решение о сосредоточении в военной промышленности практически всех функций по созданию автоматизированных систем управления (от производства современных вычислительных средств до разработки всех видов программного обеспечения) должно было гарантировать существенный прорыв в этой области. Однако сегодня, в условиях ограниченного финансирования, автоматизацию стали связывать лишь с поставкой в войска вычислительных средств.

Так, в рамках создания локальных информационных систем современные электронно-вычислительные средства были поставлены на стационарные пункты управления ряда военных округов. Но, на наш

взгляд, это не вполне оправданно. Во-первых, автоматизацию стационарных пунктов управления нельзя отнести к первоочередным задачам; во-вторых, поставка техники не сопровождается разработкой специального математического и программного обеспечения (СМПО); в-третьих, создание подобных, далеко не полных информационных систем может обеспечить лишь автоматизацию повседневной деятельности органов управления.

Необходимо обратить внимание и на то, что невозможность одновременного финансирования разработки всех подсистем АСУ чревата опасностью нарушения «идеологии» автоматизации в целом. Неблагополучная картина складывается и в области разработки комплексов средств автоматизированного управления ракетных, артиллерийских и разведывательных формирований. Здесь явно наблюдается дублирование работ, когда одно предприятие разрабатывает новый комплекс, а другое — основательно модернизирует старый, предназначенный для тех же целей, что и первый.

Как показывает анализ, значительная часть информационно-расчетных задач, предназначенных для органов управления РВиА оперативного и тактического звена, находится в стадии оперативно-тактических исследований или разработки постановок и алгоритмов, многие из них требуют приведения в соответствие с новыми возможностями вычислительной техники. Главные причины такого положения мы видим в крайне ограниченных возможностях организаций — разработчиков СМПО.

На наш взгляд, принятое в 1991 году решение о снятии с военных НИИ и передаче в промышленность функций по разработке специального программного обеспечения военных АСУ было недостаточно обоснованным. Предприятия промышленности берутся за разработку специального программного обеспечения неохотно, так как такая работа требует не только хорошего владения электронно-вычислительной техникой, но и профессиональных военных знаний. В результате интенсивность появления новых разработок резко упала, а их надежность оставляет желать лучшего [98] (1999).

информационная совместимость внутри АСУ и с взаимодействующими системами — регламентируется соответствующими протоколами, разработанными главными конструкторами на основе нормативно-технической и методической документации. Действие этих документов (независимо от срока их давности) никем не отменено, хо-

тя часть из них не в полной мере соответствует реальной действительности и требует уточнения.

Информационная совместимость модернизируемых и вновь создаваемых КСА, сопрягаемых с АСУ РВиА военного округа, обеспечивается «Протоколами организационной, информационной и технической совместимости», разработанными с учетом принятых решений. Указанные документы готовятся для каждой пары комплексов и должны содержать все характеристики информационного обмена КСА. Для КСА управления ракетными формированиями и формированиями РСЗО крупного калибра это согласование осуществлено только по одному комплексу. Разработка документов, регламентирующих информационный обмен КСА управления артиллерийскими формированиями, находится в таком же состоянии.

«Протоколы организационной, информационной и технической совместимости» представляют собой очень объемные документы. При этом все циркулирующие сообщения должны быть согласованы по целому ряду показателей, от каждого из которых в той или иной степени зависит информационная совместимость. Разработка протоколов и их согласование должны проводиться на этапе технического проектирования. Однако реально такая работа нередко начинается только тогда, когда комплекс «выкатывают» на испытания и приступают к проверке его совместимости с сопрягаемыми объектами. Причем эти согласования могут тянуться годами из-за организационных неувязок, вызванных прежде всего некоординированными действиями предприятий оборонного комплекса и НИУ МО, которые осуществляют военно-научное сопровождение [114] (2004).

программа первоочередных мер — должна предусматривать:

1) Завершение модернизации разработанных, но по различным причинам не принятых на вооружение средств автоматизации.

2) Существенную минимизацию количества типов машин управления за счет их унификации. В частности, органы управления РВиА оперативного звена могут использовать комплекс средств автоматизации ракетных формирований. Необходимы лишь соответствующее СМПО и каналы связи для информационного обмена. При работе начальников РВиА (артиллерии) объединений (соединений) на передовом пункте управления может быть использован комплекс общевойскового командующего (командира) [98] (1999).

программа долгосрочных мер — в перспективной системе управления достаточно будет иметь лишь пять унифицированных комплексов средств автоматизации, предназначенных для органов управления: оперативно-стратегического звена; тактического звена; ракетных формирований, формирований реактивных систем залпового огня крупного калибра и ракетно-технических частей; артиллерийских и противотанковых формирований; разведывательных формирований.

Разработка унифицированных комплексов средств автоматизации позволит создать унифицированное СМПО и существенно сократить сроки подготовки оперативного состава и расчетов.

При реализации программы основные усилия разработчиков информационного и лингвистического обеспечения нужно сосредоточить на обеспечении информационной совместимости всех комплексов средств автоматизации управления РВиА, а также на создании условий для их интеграции в единую межвидовую АСУ.

Выполнение программ развития основных видов обеспечения АСУ дает возможность использовать потенциал средств огневого поражения на уровне 80—90%.

Необходимо создание в РВиА ВС РФ специализированного опытного участка (СОУ), предназначенного для проведения практических экспериментов по проверке и испытанию вооружения и военной техники рода войск в условиях, близких к боевым [98] (1999).

4.1.4. Автоматизированные системы управления в ВКС

требование к системе управления противовоздушной обороной — возможность представления в любой момент времени информации, непосредственно обеспечивающей поддержку принятия решения на применение войск (сил) ПВО в соответствии со складывающейся обстановкой.

Только при условии ее постоянного отслеживания силами и средствами разведки различных видов, начиная с дальних подступов, своевременного выявления и постоянного отображения всех ее изменений органы управления противовоздушной обороной могут функционировать устойчиво, с максимальным использованием своих возможностей при ведении боевых действий.

При этом должна отображаться обстановка не только в воздухе на подступах и в районах прикрываемых войск и объектов, но и в

районах функционирования наземных систем управления, базирования, навигации средств воздушного нападения, воздействие по которым ударными силами нашей авиации способствует более успешному решению задач ПВО. В каждый момент времени органы управления должны располагать информацией в интересах подготовки и ведения как оборонительных, так и наступательных действий ВВС, на которые в новой оргструктуре возложены задачи противовоздушной обороны.

Сложность информационных процессов возрастает в связи со все более широким применением эффективных средств в космической сфере. Вместе с этим существенно выросли объемы информации, необходимой для решения задач отражения воздушного (воздушно-космического) нападения [159] (2006).

4.1.4.1. Автоматизированные системы противовоздушной обороны 50—60 годов XX века

территориальная автоматизированная система радиолокационного оповещения, управления и наведения истребительной авиации «Воздух-1» — система противовоздушной обороны, созданная еще в 50-е годы XX столетия.

Она была построена на телекоммуникационной сети взаимодействующих радиолокационных узлов (РЛУ) и командных пунктов (КП) на базе аналоговых счетно-решающих приборов, что существенно ограничивало ее функциональные возможности [135] (2011).

глобальная телекоммуникационная сеть радиолокационных узлов — впервые, начиная с 1956 года, на ЭВМ «Урал-1» началось моделирование алгоритмов обработки радиолокационной информации и сопровождения движущихся воздушных объектов в **имитированном, псевдореальном времени**. На ЭВМ с производительностью 100 операций в секунду и общей памятью две тысячи слов, занимавшей огромное помещение, начинали решаться очень сложные комплексные задачи **с имитацией реального времени**. Моделировались исходные координаты, отражающие движение и маневр наблюдаемых радиолокаторами объектов. По этим данным имитировалось обнаружение динамических объектов; формировались траектории их движения, отождествление и объединение траекторий динамических объектов в реальном времени от различных радиолокационных узлов. В 1959 году уже

на более мощной машине М-20 моделирование было продолжено и значительно расширено [135] (2011).

территориальная информационная система противовоздушной обороны страны (аванпроект «Электрон») — система, впервые в стране в реальном времени предусматривающая объединение в глобальной сети ряда компьютеров на узлах сбора и обработки радиолокационной информации о воздушных объектах и на КП управления активными средствами ПВО.

Все элементы в системе обработки информации и управления должны были работать на ЭВМ в реальном масштабе времени при несинхронных потоках сообщений от удаленных независимых движущихся объектов — источников информации. На каждом узле обработки радиолокационной информации и КП управления средствами ПВО следовало иметь объединенные в локальную сеть графические терминалы различных типов для визуализации воздушной обстановки и обеспечения функционирования оперативного и командного состава с временем отклика, измеряемого долями секунды. Система на цифровых вычислительных машинах должна была базироваться на совокупности транспортабельных радиолокационных узлов, создававших почти сплошное поле радиолокационного обнаружения различных динамических объектов во всем воздушном пространстве страны [135] (2011).

крупные научно-технические задачи создания программных средств реального времени для обработки радиолокационной информации на специализированных ЭВМ — в начале 1960-х годов был промоделирован, исследован, решен и практически апробирован ряд таких задач. Функциональные алгоритмы и программы обеспечили прием и обработку в ЭВМ траекторий и команд о «чужих» и «своих» воздушных объектах, визуализацию данных для операторов сопровождения.

Для обеспечения взаимодействия радиолокационных узлов друг с другом и обмена информацией между ними была создана **телекоммуникационная сеть** на базе специально выделенных каналов обычных телефонных линий связи.

В начале 1960-х годов впервые был разработан и реализован ряд базовых принципов и методов построения больших комплексов программ реального времени, взаимодействующих в **глобальной телекоммуникационной сети**.

Особые трудности при разработке системы ПВО были связаны с динамическим тестированием и испытаниями программ радиолокационных узлов в реальном времени, взаимодействующих в телекоммуникационной сети.

В сферу исследования и разработок в 60-е годы прошлого века впервые вошел и был апробирован новый широкий класс компьютерных систем и телекоммуникационных сетей реального времени. Этот опыт может представлять интерес для специалистов, интересующихся историей развития отечественной вычислительной техники в оборонной промышленности, значительно опережавшей научно-технические достижения других отраслей вычислительной техники, в том числе закрытые для публикации [135] (2011).

автоматизированная система обработки радиолокационной информации «Межа» — автоматизированная система, заданная для разработки в 1960 году для реализации функций радиолокационных узлов (РЛУ) системы ПВО страны (главный конструктор Владимир Алексеевич Шабалин, за создание аппаратуры отвечал Анатолий Николаевич Коротоношко, за алгоритмы и программы — Владимир Васильевич Липаев).

В состав РЛУ входили следующие крупные аппаратные компоненты:

— две радиолокационных станции кругового обзора («П-35» и комплекс «Алтай—П-80»);

— радиолокационные высотомеры «ПРВ-11»;

— электронная полупроводниковая мобильная цифровая вычислительная машина «Курс-1»;

— прицепы управления РЛУ, сопряженные с радиолокационными станциями кругового обзора и высотомерами с индикаторами для съема и цифровой обработки информации о воздушных целях;

— прицеп резервного автономного энергопитания всех систем РЛУ.

Кроме того, на РЛУ могла поступать информация о целях от маловысотных постов (МВП) «Низина» с аналоговой автоматизированной системой сопровождения целей и индикаторной аппаратурой рабочих мест операторов сопровождения. МВП были оборудованы радиолокационными станциями кругового обзора «Тропа» («П-15» или «П-19»).

Производство модернизированной системы «Межа» прекратилось в 1987 году. РЛУ «Межа» размещены по стране и эксплуатируются до настоящего времени от западных границ до Камчатки. РЛУ обеспечивают контроль за «чистотой неба» России и готовность радиолокационной информации для применения активных средств ПВО по воздушным целям противника [136] (2013).

4.1.4.2. Комплекс моделей для радиотехнических войск

комплекс штабных математических моделей боевого применения радиотехнических войск (КШММ РТВ) — комплекс, предназначенный для расчета и оценки разведывательно-информационных возможностей и эффективности разведывательно-информационных действий радиотехнических соединений и частей при планировании боевого применения войск, проведении тренировок и несении боевого дежурства [196] (2003).

4.1.5. Автоматизированные системы управления в ВМФ

информационно-расчетные задачи и математические модели ВМФ — задачи и модели, разработанные 24 ЦНИИ МО и другими НИУ ВМФ в тесной связи с оперативным составом ГШ ВМФ и штабов флотов по сбору и обработке информации об оперативной обстановке на океанских и морских театрах военных действий (в том числе о космической, радиоэлектронной, радиационной, бактериологической и химической обстановке, ядерных и химических ударах), об элементах тылового, специального и технического обеспечения сил; по учету тактико-технических характеристик, боевых потенциалов и нормативов использования сил, оружия и технических средств ВМФ и ВМС иностранных государств; по сбору, обработке и оценке физико-географических, климатических и погодных условий в районах проведения операций (боевых действий), а также других факторов, влияющих на выполнение боевых задач; по автоматизации процессов управления ракетными подводными крейсерами специального назначения; по оценке обстановки и выработке предложений в замысел и решение команду-

ющих (командиров) на проведение операций (боевых действий) [115] (2005).

Библиотека методик ВМФ — собрание информационно-расчетных задач для широкого использования при 24 ЦНИИ МО, получивших положительные оценки пользователей и прошедшие опытную эксплуатацию.

Уже к 1968 году в ней содержалось более 100 полноценных информационно-расчетных задач применительно к ЭВМ, внедряемым на объектах ВМФ. Данные научно-методические материалы широко использовались в повседневной деятельности должностными лицами ГШ ВМФ и штабов флотов при заблаговременном планировании операций (боевых действий сил), в организации и непосредственном управлении силами боевой службы и боевого дежурства, а также на мероприятиях оперативной подготовки (командно-штабных учениях) [115] (2005).

система автоматизированного распределения исходных данных — система, обеспечивающая эффективное применение «Библиотеки методик ВМФ» [115] (2005).

единая система автоматизации расчетов (ЕСАР) — система, обеспечивающая эффективное применение «Библиотеки методик ВМФ» и облегчение труда оперативного состава органов управления [115] (2005).

работы по созданию унифицированного информационно-лингвистического обеспечения — работы, поддерживающие решение информационно-расчетных задач для автоматизированных систем управления ВМФ.

При этом главное внимание уделялось разработке информационных языков представления содержаний боевых и административных документов, а также записи данных в запоминающих устройствах ЭВМ. Разрабатывались синтаксис, семантика, классификаторы и кодировочные словари, способы формализации документов, ключевых фраз для формализации содержаний оперативных и разведывательных сводок — такие, как формулярный, анкетный, табличный и другие, которые применяются и в настоящее время. Обосновывались предложения по разработке типового программного обеспечения для реализации информационных задач в ЭВМ, которые впоследствии явились основой автоматизированных информационно-поисковых систем докумен-

тального и фактографического типов, а также современных систем управления базами данных [115] (2005).

единое информационное поле данных ВМФ — прототип современного единого информационного ресурса обеспечения решения задач «Библиотеки методик ВМФ» [115] (2005).

автоматизированная система МВУ-Б2 — система, внедренная (с января 1975 года) в штабах флотов и ГШ ВМФ [115] (2005).

оперативная фактографическая информационная система (ОФИС) — уникальная многофункциональная система на ЭВМ типа «БЭСМ», являющаяся совместной отечественной разработкой специалистов Центрального научно-исследовательского института комплексной автоматизации (г. Москва) и 24 ЦНИИ МО (Б.Т. Шрейбер, С.И. Вайнштейн, Л.Л. Бубер, Н.Г. Никитин, Ю.Г. Храбров).

Программное обеспечение ОФИС выполняло функции инструментальных средств создания информационных систем, а также информационно-поисковых систем фактографического и документального типов.

Кроме того, с его помощью осуществлялись: формирование и поддержка в актуальном состоянии и соответствии документальных и фактографических баз данных; обработка входящих документов (сообщений и запросов), формализованных упомянутыми способами на русском языке (для запросов); поиск и выдача операторам в требуемом виде (табличном, текстовом, анкетном) информации о реальной обстановке на индикаторные устройства из баз данных по указанным атрибутам и в формулярном виде на устройства наглядного отображения (экраны и планшеты) системы МВУ-Б2; поиск и выдача информации в единую систему автоматизации расчетов для решения расчетных задач из «Библиотеки методик ВМФ», для чего на основе ОФИС в системе МВУ-Б2 была создана и поддерживалась в актуальном состоянии база данных о силах, оружии и средствах ВМФ и ВМС вероятного противника, гидрометеообстановке на океанских и морских театрах военных действий, береговых объектах, командных пунктах и системах управления, боевых потенциалах и нормативах по применению сил и оружия; обеспечение и контроль доступа пользователей к базам данных; разграничение доступа к различным разделам баз и конкретным записям об объектах и их элементах; администрирование процесса обработки информации и контроль функционирования ее компонентов.

Программное обеспечение ОФИС представлялось в виде множества отдельных процедур различных уровней, которые автоматически интегрировались для выполнения заданий, изложенных в сообщениях или запросах. ОФИС была выполнена в виде «многоязыковой системы», способной вести обработку и выдачу фактографической информации на нескольких языках. Это достигалось за счет применения единой системы кодирования словарных терминов [115] (2005).

Центр по разработке специального математического и программного обеспечения для автоматизированных систем ВМФ при 24 ЦНИИ МО — центр, обеспечивающий реализацию информационных технологий в ОВУ флота.

В результате совместной деятельности специалистов центра, Военно-морской академии, НИУ ВМФ, ГШ ВМФ, штабов флотов и промышленности в этот период практически осуществляется автоматизация процессов обработки информации об оперативной обстановке на океанских и морских театрах военных действий в ГШ ВМФ, штабах флотов, штабах флотилий разнородных сил и военно-морских базах. Одновременно проводится автоматизация формирования и представления командованию срочных табельных донесений (оперативных и разведывательных сводок, документов по составу и состоянию сил боевой готовности объединений ВМФ, документов по составу и состоянию оружия на складах и арсеналах флота), реализуется «межмашинный» обмен информацией между автоматизированными системами объектов управления различных уровней, а также автоматизированное доведение командной и справочной информации до кораблей в море.

Вместе с тем разрабатывается и внедряется в практику деятельности оперативного состава центрального командного пункта ВМФ и командных пунктов флотов автоматизированный комплекс задач планирования и контроля боевой службы и боевого дежурства.

В дополнение к уже существующим задачам и методикам разрабатываются комплексы задач по обоснованию вариантов боевого применения сил в морских операциях (боевых действиях), различных видов оперативного, тылового и технического обеспечения, по планированию и боевому применению сил разведки, связи, РЭБ, ПВО в операциях флота (боевых действиях).

Параллельно всесторонне совершенствуется комплекс задач по автоматизации процессов управления и обеспечения боевой устойчи-

вости ракетных подводных крейсеров стратегического назначения [115] (2005).

математическая модель имитационного моделирования двусторонних боевых действий — модель в интересах оценки эффективности принимаемых командованием решений на проведение операций (боевых действий), а также для проведения оперативно-тактической подготовки должностных лиц органов военного управления.

Впоследствии эта математическая модель была разработана в нескольких модификациях (ответственные исполнители А.Б. Чевалкж, А.В. Уланов, И.С. Кудинова), успешно прошла испытания в Военно-морской академии, оперативном управлении ГШ ВМФ, Военной академии ГШ ВС и в настоящее время успешно применяется на мероприятиях оперативной подготовки, постоянно совершенствуется по предложениям пользователей [115] (2005).

единая интегрированная автоматизированная система управления ВМФ (ИАСУ ВМФ) — автоматизированная система, создаваемая с 1990 года в рамках комплексной автоматизации процессов управления ВМФ на основе существующих комплексов средств автоматизации, вновь разрабатываемых автоматизированных систем управления путем массового внедрения персональных ЭВМ и локальных вычислительных сетей, современных автоматизированных систем телекоммуникации и связи.

Для ее создания 24 ЦНИИ МО разработана методология обоснования состава и содержания информационных технологий и потребного информационного ресурса для реализации в ИАСУ ВМФ функциональных систем и подсистем. В ее основу положен системный анализ функциональной, системной и технической архитектур проектируемой функциональной системы (подсистемы) и автоматизированной системы управления в целом.

Одновременно проводятся работы по созданию уникального программного комплекса, адаптируемого на языке оператора высокого уровня для реализации функциональных технологий.

Совместно с промышленностью в автоматизированных системах внедряются современные базовые информационные технологии, и в первую очередь: электронная почта, Web-технология (в том числе создания, ведения и поддержания в актуальном состоянии баз данных и хранилищ информации), геоинформационная система системы обеспе-

чения безопасности информации, организации решения функциональных задач [115] (2005).

единый информационный ресурс в ИАСУ ВМФ — одна из главных составляющих проектирования функциональных систем и подсистем ВМФ [115] (2005).

единое информационное пространство в ИАСУ ВМФ — см. *единый информационный ресурс в ИАСУ ВМФ* [115] (2005).

4.1.5.1. Автоматизированная система управления связью ВМФ

автоматизированная система управления связью Военно-Морского Флота (АСУС ВМФ) — иерархически организованная совокупность органов, пунктов управления, средств связи и автоматизации, взаимодействующих между собой по каналам межмашинного обмена сети передачи данных.

АСУС имеет свою внутреннюю архитектуру, ряд подсистем, из которых выделяются основные: система принятия решений и система их исполнения. Ее организационно-функциональная структура базируется на нескольких уровнях: административный (верхний); управление услугами связи; управление сетями связи и управление элементами сети (нижний уровень). Функциональные уровни определяются размерами сетей и их функциональным предназначением, т.е. зависят от принадлежности сети к стратегическому, оперативно-стратегическому, оперативному, оперативно-тактическому или тактическому звену управления силами ВМФ. На основе функциональных уровней в системе управления образуются организационно-технические уровни, имеющие организационно-технические единицы — пункты управления, состоящие из технического персонала и программно-технических средств.

На верхних уровнях иерархии АСУС управление имеет преимущественно организационный характер, на нижних — технологический. На уровне организационного управления осуществляется анализ состояния системы связи и выработка вариантов решения на этапах оперативного управления и планирования (в том числе по развертыванию, восстановлению, наращиванию системы, перераспределению каналов связи и потоков информации и т.п.). К задачам технологического

управления относятся сбор и первичная обработка информации о задержанных сообщениях, состоянии линий, каналов и средств связи, доведения и реализации управляющих воздействий на средства связи.

Деятельность должностных лиц АСУС непосредственным образом связана: с накоплением и обработкой информации о системе и средствах противодействия; с распределением материальных и интеллектуальных ресурсов; с анализом (прогнозом) состояния и принятием решений по изменению (синтезу) структуры и параметров системы и ее элементов; с оценкой свойств системы с заданными параметрами в условиях прогнозируемых или фактических воздействий оружия, систем радиоразведки и РЭП, а также отказов технических средств. Эти задачи не могут быть решены только на основе методов формальных рассуждений.

Однако в настоящее время на разработку и применение информационных технологий в АСУС ВМФ негативно влияет ряд факторов. Во-первых, это недостаточный уровень автоматизации процессов сбора, передачи, преобразования и обработки информации, а также поддержки принятия решений в системе управления связью, что не позволяет обеспечить возрастающие требования к связи при управлении силами и оружием в современной войне. Во-вторых, имеет место определенная дезинтеграция функциональных подсистем и сетей АСУС ВМФ как в организационном, так и в системно-техническом плане (по видам передаваемой информации, предназначению и т.д.). В-третьих, не полностью решены вопросы сопряжения, взаимодействия и поэтапной интеграции с АСУ силами ВМФ, АСУС ВС РФ, системой управления взаимоувязанной сетью связи РФ, системами и сетями связи других министерств и ведомств в интересах создания единого информационного пространства России. В-четвертых, принципы организации, технические и программные средства автоматизации управления связью, используемые в системах связи ВМФ, не унифицированы, что создает угрозу разрыва циклов управления. В-пятых, в повседневной деятельности должностных лиц органов управления связью различного уровня практически отсутствуют или внедрены в недостаточных объемах современные средства автоматизации управления связью. В-шестых, предметная область АСУС ВМФ как сфера военной деятельности плохо обеспечена адекватными методами и средствами инженерии знаний [72] (2004).

4.1.5.2. Автоматизированная система управления кораблем

боевая информационно-управляющая система — автоматизированная система управления, реализующая ограниченный круг функций управления, и обеспечивающая решение задач анализа обстановки, навигационного счисления, маневрирования, боевого применения оружия и средств гидроакустического противодействия [202] (2001).

единая автоматизированная система управления кораблем — автоматизированная система управления, связывающая все крупные технические системы и административную систему управления.

Создание такой системы позволит оптимизировать состав технических и программных средств, а, следовательно, сократить их номенклатуру, повысить ремонтопригодность и модернизационные возможности системы, упростить ее обслуживание.

Разработка единой АСУ для такой сложной организационно-технической системы, как современный корабль, требует продолжительного времени (не менее пяти лет) и значительных финансовых затрат. Устанавливать данную систему можно только на строящиеся корабли. Что касается кораблей боевого состава, то здесь модернизация практически невозможна из-за принципиальных расхождений в архитектуре единой АСУ и действующих систем [202] (2001).

интегрированная компьютерная информационная сеть корабля (ИКИС) — сеть, предполагающая подключение действующих и разрабатываемых автоматизированных систем управления крупными техническими системами при сохранении независимости функциональных систем от ее конкретной структуры; обеспечение, с одной стороны, «прозрачности» информационных ресурсов, а с другой — безопасности и надежности их хранения [202] (2001).

4.1.6. Автоматизированные системы обеспечения войск (сил)

4.1.6.1. Обеспечения войск цифровой информацией о местности

комплекс автоматизированной базы цифровых картографических данных (КАБЦКД) — комплекс средств автоматизации, предназначенный для создания, накопления, хранения и выдачи потребителям цифровых карт местности.

В нем удалось реализовать технологию создания цифровых карт местности по картографическим материалами (тиражные оттиски или диапозитивы постоянного хранения топографических карт отечественного издания и тиражные оттиски топографических карт зарубежного издания), а также с использованием аэрокосмических снимков.

КАБЦКД был принят на вооружение в 1984 году. За успешное решение проблемы создания цифровых карт местности в интересах картографического обеспечения высокоточного оружия ученым Е.И. Халугину и Е.А. Жалковскому была присуждена Государственная премия СССР [198] (2006).

комплекс автоматизированных рабочих мест создания, хранения и выдачи электронных карт и система электронных карт (АРМ-ЭК) — комплекс средств автоматизации, принятый на снабжение ВС РФ в 1999 году и предназначенный для создания электронных карт и планов городов, включенных в систему электронных карт, их накопления, учета, хранения и выдачи на машинных носителях, а также редактирования и изготовления их издательских оригиналов.

Комплексы АРМ-ЭК изготовлены, поставлены и успешно эксплуатируются в частях топографической службы ВС РФ. За разработку и внедрение этого комплекса и системы электронных карт сотрудникам 29 НИИ МО РФ Ш.А. Дивееву, С.А. Жаркову (посмертно), Н.А. Живичину, В.А. Леоньеву и А.И. Мартыненко в числе других была присуждена Государственная премия Российской Федерации в области науки и техники за 2002 год [198] (2006).

комплекс автоматизированных рабочих мест по созданию и подготовке к изданию авиационных (топографических) карт

(«Карта-А») — комплекс средств автоматизации, предназначенный для эксплуатации в стационарных условиях.

Был принят на снабжение ВС РФ в 2002 году [198] (2006).

банк картографических данных военного назначения — комплекс средств автоматизации, предназначенный для приема, накопления, хранения и выдачи цифровой информации о местности.

Был принят на снабжение ВС РФ в 2002 году [198] (2006).

аналитическо-цифровая фотограмметрическая станция (АЦФС) — комплекс средств автоматизации, предназначенный для создания и обновления электронных топографических карт, планов городов по одиночным космическим и аэрофотоснимкам.

Она функционально обеспечивает выполнение следующих операций:

прием, оценка и визуализация аналоговых и цифровых аэрокосмических и картографических изображений;

изготовление цифровых фотопланов с использованием информации о планово-высотном обеспечении и рельефе местности;

автоматизированное и оптико-визуальное дешифрирование аналоговых и цифровых панорамных, щелевых, радиолокационных и других фотоснимков, а также цифровых фотопланов;

создание (обновление) электронных топографических карт, планов городов по результатам дешифрирования;

создание цифровых пространственных моделей местности; выдача по запросам потребителей созданной цифровой информации о местности.

Наиболее важной особенностью функционального предназначения АЦФС является создание высокоточной информации в виде цифровых моделей местности.

В настоящее время серийные образцы АЦФС поставлены в части топографической службы ВС РФ и введены в эксплуатацию для выполнения заданий по созданию и обновлению цифровой информации о местности.

Особенно важно то, что применение АЦФС позволяет отказаться от технологий и аппаратно-программных средств создания электронных карт путем цифрования достаточно устаревших по содержанию картографических материалов и изготавливать эти карты и планы городов на основе аэрокосмических материалов.

За разработку и серийное внедрение аналитическо-цифровой фотограмметрической станции и технологии создания высокоточной информации о местности коллективу авторов, в который входили сотрудники 29 НИИ МО РФ (Л.И. Яблонский, Г.В. Барабин, В.Г. Елюшкин, Н.И. Конон, Р.С. Мухудинов, И.В. Сидоров, В.В. Скрипнюк), была присуждена премия Правительства Российской Федерации в области науки и техники за 2004 год [198] (2006).

унифицированная система авиационных карт — система карт, принятая на обеспечение ВС РФ в 1995 году.

Активное участие в решении этой задачи принимали А.А. Кузнецов, В.М. Фонарев, С.П. Малинин, А.К. Соловьев, А.Б. Кезлинг, В.П. Тюрютиков, Г.Б. Воронов и др. За разработку новой системы авиационных карт коллективу авторов в 1999 году была присуждена премия им. Ф.Н. Красовского [198] (2006).

единая система карт военного назначения (ЕСК ВН) — система карт, предназначенная для замены основных карт, стоящих на обеспечении ВС РФ в настоящее время: топографических, обзорно-географических, аэронавигационных.

При этом сохраняется возможность решения всех задач пользователей исходя из предназначения этих видов карт. В состав единой системы карт военного назначения входят: подсистема крупномасштабных карт (1:25 000, 1:50 000, 1:100 000) и подсистема мелкомасштабных карт (1:500 000, 1:1 000 000, 1:2 000 000, 1:4 000 000, 1:8 000 000, 1:16 000 000, 1:32 000 000). В качестве связующего звена двух названных подсистем выступает карта 1:250 000. Следует отметить, что разработанная ранее система авиационных карт вошла составной частью в единую систему карт военного назначения как подсистема мелкомасштабных карт.

Система была разработана сотрудниками 29 НИИ МО РФ (В.М. Фонаревым, А.А. Кузнецовым, В.П. Тюрютиковым и др.) в 2005 году в рамках исследований по стандартизации и унификации карт в целях оптимизации условий создания и применения картографической информации в существующих и перспективных системах управления войсками [198] (2006).

4.1.6.2. Информационные и коммуникационные технологии в деятельности военно-медицинской службы ВС РФ

информационная система оперативного и непрерывного наблюдения (мониторинга) за состоянием здоровья прикрепленного контингента — информационная система, предназначенная для автоматизации процесса своевременного распознавания преморбидных состояний и заболеваний прикрепленного контингента 2 ЦВКГ им. Мандрыка, а также деятельности семейного врача.

Информационная система разрабатывалась в 2005—2008 годы в соответствии с Решением Минэкономразвития России в рамках ОКР «Кладезь». Разработанный опытный образец системы прошел государственные и межведомственные испытания в составе: информационно-аналитическая подсистема обеспечения качества медицинского обслуживания прикрепленного контингента; мобильные телемедицинские комплексы пациентов и врачей; носимые АРМы врачей; фактографическая медицинская книжка; носимый комплекс мониторинга кардиологического больного; центр хранения результатов диагностических исследований; программно-технические средства сопряжения с медицинским оборудованием.

Мобильные телемедицинские комплексы пациентов и носимый комплекс мониторинга кардиологического больного зарегистрированы и лицензированы в Федеральной службе по надзору в сфере здравоохранения и социального развития РФ.

Применение разработанной информационной системы оперативного и непрерывного наблюдения (мониторинга) за состоянием здоровья прикрепленного контингента является эффективным средством в работе по своевременному распознаванию преморбидных состояний и заболеваний и коррекции самых ранних нарушений, по восстановлению функционального состояния организма и работоспособности пациента. Ее внедрение в медицинскую практику позволит повысить качество профилактической и лечебно-диагностической работы в лечебно-профилактических учреждениях: заблаговременно обнаружить медицинские проблемы в состоянии здоровья прикрепленного контингента, оказать своевременную медицинскую помощь, передать врачу по каналам связи информацию о пациенте, дать возможность пациенту получить своевременные рекомендации. Это снизит трудовые и экономические потери, обусловленные преждевременной смертностью

лиц трудоспособного возраста, инвалидностью, временной и стойкой нетрудоспособностью от болезней системы кровообращения [62] (2011).

мобильный телемедицинский диагностический комплекс пациента (МТМДКП) — комплекс средств автоматизации, предназначенный для получения, обработки, хранения и передачи по каналу связи объективных клинических показателей удаленных пациентов (военнослужащих и членов их семей), ввода и вывода аудио- и видеоинформации, оперативного дистанционного взаимодействия с мобильным телемедицинским комплексом врача (МТМКВ) и стационарным телемедицинским комплексом медицинских специалистов.

Пациент с помощью своего мобильного комплекса имеет возможность: получать информацию о своем функциональном состоянии (исходя из методик, входящих в комплекс); связаться с семейным врачом (консультантом) для решения вопросов в возникшей ситуации, уточнения ранее данных рекомендаций; по рекомендации врача (консультанта) провести исследования с использованием встроенной аппаратуры; получать указания по выполнению плана профилактических и лечебных мероприятий [62] (2011).

носимое автоматизированное рабочее место лечащего врача (НАРМ ЛВ) — переносной (карманный) компьютер с соответствующим программным обеспечением, с помощью которого врач, беседующий с пациентом, получает данные о больном из базы данных, корректирует его схему лечения и план обследования, заносит в базу данных результаты своего анализа текущего состояния больного и назначения по дальнейшим лечебно-диагностическим процедурам.

Он обеспечивает беспроводный доступ к локальной БД ЛВС в оговариваемых зонах в помещениях лечебного учреждения, а также на его территории [62] (2011).

носимый комплекс мониторинга кардиологических больных (НКМКБ) — комплекс средств автоматизации для осуществления непрерывного круглосуточного наблюдения за пациентами с нестабильным состоянием в остром периоде заболевания.

Комплекс НКМКБ с помощью наклеиваемого на поверхность грудной клетки пациента датчика надежно вырабатывает сигнал тревоги при существенных отклонениях от нормы показателей сердечной деятельности. Данное устройство позволяет надежнее контролировать

жизненно важные функции больного (частоту и ритмичность сердечных сокращений, частоту дыхания) в условиях изменения режима больного.

Главное назначение такого варианта НКМКБ — выдавать постовой медицинской сестре на экран ее АРМа, а лечащему врачу на его носимый АРМ данные о критических изменениях в состоянии больного, о местонахождении пациента для принятия (при необходимости) срочных мер по оказанию помощи [62] (2011).

фактографическая медицинская книжка (ФМК) — устройство, расширяющее возможности медицинского персонала по изучению, хранению или передаче информации о пациенте, предоставляющее врачу возможности нового, основанного на современных информационных технологиях взгляда на динамику показателей состояния здоровья и течение заболеваний.

В ФМК хранится не только информация, записанная медицинскими специалистами во всех медицинских книжках пациента, но и результаты диагностических исследований (лабораторных, рентгенологических, функционально-диагностических, ультразвуковых и др.) в любой форме представления. Объем флэш-памяти позволяет хранить даже аудио- и видеоданные результатов исследований [62] (2011).

4.1.6.3. Автоматизированные рабочие места органов военной юстиции

автоматизированное рабочее место следователя (дознавателя) — совокупность технических и программных средств, обеспечивающих решение стоящих перед военными следственными органами задач [2] (2014).

алгоритм деятельности по раскрытию и расследованию преступлений — комплекс взаимосвязанных между собой следственных, оперативно-розыскных и иных действий, а также их совокупностей, выстроенных в оптимальной последовательности и направленных на получение предопределенного результата — установление обстоятельств содеянного и доказывание виновности преступника.

Он представляет собой зависимые от следственной ситуации и взаимосвязанные совокупности следственных, организационных и

иных действий, а также их комплексов, выстроенных в оптимальной последовательности на основе приоритетов [2] (2014).

раскрытие и расследование преступлений — процесс собирания, исследования и использования криминалистически значимой информации (розыскной и доказательственной), содержащейся как в материальных, так и в идеальных следах преступлений.

Вместе с тем в ходе раскрытия и расследования преступлений также используется информация, не содержащаяся в материальных и идеальных следах преступлений и не имеющая непосредственного отношения к расследуемому преступлению, например, различного рода справочная информация.

Кроме того, при раскрытии и расследовании преступлений также может потребоваться информация, содержащаяся в различных нормативных правовых актах [2] (2014).

носимые хранилища информации — эталоны, определители и справочники, служащие целям выделения значимых объектов из окружающей среды, их определения, классификации, а также для получения представления об их свойствах и признаках в целях правильного обращения с ними, надлежащей их упаковки, хранения и транспортировки [2] (2014).

правовые информационные системы (справочные правовые системы, справочно-правовые системы) (СПС) — специальные компьютерные программы, предназначенные для работы с базами данных, содержащими тексты нормативных правовых актов, решений различных государственных органов, комментарии и консультации специалистов из различных отраслей юридической науки, а также другую правовую информацию.

Компьютерные технологии, к которым относятся СПС, имеют ряд уникальных достоинств и возможностей. В первую очередь это компактное хранение больших объемов информации, быстрый поиск нужных документов и высокоскоростная передача информации средствами связи на любые расстояния. Они способны оказать существенную помощь при решении правовых вопросов.

Сегодня на российском рынке представлено значительное количество компаний — разработчиков справочно-правовых систем, а также сервисных центров, осуществляющих их поставку и обслуживание. Наиболее востребованными и распространенными из них являются

СПС «КонсультантПлюс» и «Гарант». Однако вышеупомянутые СПС в большей степени ориентированы на коммерческие организации. Специфика деятельности органов следствия и дознания ими не учитываются. Об этом свидетельствует и тематика информационных банков данных систем. Вместе с тем возможно использование адаптированной версии данных продуктов при соответствующих госзаказах [2] (2014).

прикладные программы автоматизированного рабочего места следователя (дознавателя) — программные продукты, как, например, «Аргус-Следователь 5.0» (Центр правовой информатизации Министерства юстиции по Воронежской области), «Автоматизированное рабочее место следователя (дознавателя)» (TechnicalSofvtGroup), «Автоматизированный Кабинет Следователя» (SLIDSTWO), АРМ «Следователь» («Овионт Информ») и др.

Данные программы обеспечивают удобство работы с файлами документов, отрабатываемых на компьютере, а также их систематизацию. В отрабатываемые бланки процессуальных документов автоматически вставляется статическая информация, предварительно внесенная в базу данных программ (справочников). В некоторых программах реализована функция вставки информации из других документов, выполненных по данному делу (например, обстоятельства дела, которые кратко повторяются в разных документах).

По сведениям производителей, данные программы экономят 30—50% рабочего времени. Следует отметить, что в настоящее время разработки подобных программ носят разрозненный характер и, как следствие, продукта, отвечающего всем требованиям, еще не получено. Указанные программы находятся в стадии развития и апробации. Представляется, что необходима координация данных разработок правоохранительными органами с целью создания единого универсального продукта. Положительное влияние на этот процесс окажет и конкуренция разработок [2] (2014).

требования к автоматизированному рабочему месту следователя (дознавателя) — в целях совершенствования информационного обеспечения раскрытия и расследования преступлений АРМ следователя (дознавателя) должно быть способно обеспечить выполнение широкого круга ранее в полном объеме не использовавшихся возможностей по следующим направлениям:

обеспечение использования как в стационарных, так и в полевых условиях;

программная алгоритмизация раскрытия и расследования преступлений, предусматривающая вариативность предлагаемых дознавателю решений с учетом конкретных условий обстановки, складывающейся на момент их принятия, а также ожидаемых результатов предложенных решений (в том числе негативных последствий, так называемые риски);

автоматизация деятельности дознавателя по раскрытию и расследованию преступлений;

доступ к криминалистическим учетам, сформированным на основе автоматизированных информационных систем;

доступ к локальным периодически обновляемым информационным системам;

внедрение коммуникационных возможностей (электронный документооборот, возможность работы в режиме видеоконференции и др.) [2] (2014).

4.1.6.4. Другие автоматизированные системы

Информационная система ведения метеоинформации — обеспечивала автоматизированное сшивание метеосводок и их рассылку пользователям. В ее создании участвовали А.А. Симонян, О.А. Кокурин, В.С. Леляева и др. [99] (2009).

Информационно-расчетная система АСУ Тылом ВС — была разработана в 1981 году под руководством В.И. Воробьева. Разработке системы предшествовала большая работа по созданию системы классификации и кодирования тыловой информации, формализации и переизданию табеля срочных донесений штаба Тыла ВС. Успех этой работы был предопределен тем, что она осуществлялась под руководством и при непосредственном участии генералов и офицеров штаба Тыла ВС. Активное участие в разработке этой системы принимали Ю.С. Тислин, Л.В. Андреев, А.И. Боков, О.В. Масленников и многие другие.

При этом впервые в практике создания ИС классификаторы рассматривались как элемент ее базы и использовались при организации ведения и обработки информации. Описание структур входных и выходных данных (документов) осуществлялось с помощью таблиц-описателей. Для описания алгоритмов обработки информации был разработан специальный язык SUPER, с помощью которого могли за-

даваться условия поиска и выборки данных и правила их обобщения. Сбор информации осуществлялся по телеграфным каналам, корректировка информационной базы — по изменениям [99] (2009).

Автоматизированная система информационного обеспечения (АСИО) — создана во второй половине 1980-х годов для формирования информации при вводе ее для хранения на объектах АСУ. В создании АСИО под руководством А.А. Симоняна принимали участие Е.И. Якутин, В.Ф. Денисов, Н.Н. Штыков, В.И. Котляров, А.С. Демьяненко, В.Н. Филиппова, С.П. Данилочкин и др. АСИО постоянно развивается, совершенствуется и находится в эксплуатации на объекте АСУ по настоящее время [99] (2009).

4.1.7. Автоматизированные системы организационно-мобилизационных органов ВС РФ

организационно-мобилизационные органы ВС РФ (ОМО) — органы военного управления, решающие задачи организационного строительства, подготовки и мобилизационного развертывания Вооруженных Сил.

Функционирование ОМО четко регламентировано. Все они объединены в систему управления, для которой характерны: широкая номенклатура органов управления со сложной организационной структурой; значительный территориальный размах (органы управления расположены по всей стране); взаимодействие ОМО с большим числом органов военного и государственного управления, включая гражданские министерства, ведомства, предприятия и учреждения; передача между ОМО больших объемов оперативной информации, классификаторов и нормативно-справочной информации [26] (1999).

автоматизация организационно-мобилизационных органов — работы по автоматизации ОМО развернулись достаточно давно, с конца 60-х годов. Они начались с формализации оргмобинформации (разработки классификаторов и номенклаторов) и автоматизации ее сбора и обработки. На этом этапе автоматизация охватила прежде всего ОМО высших уровней управления. Так, в интересах организационно-мобилизационных органов стратегического звена управления создан огромный программно-информационный фонд, включающий базы данных оперативной информации и комплексы информационных и

расчетных задач. В настоящее время разработанные средства внедрены на больших ЭВМ, что позволило сократить время подготовки документов по организационному строительству и мобилизационному развертыванию ВС и одновременно существенно уменьшить число ошибок в документах организационно-мобилизационной отчетности. В ОМО низших уровней управления автоматизация носила практически «кустарный» характер, когда энтузиасты из числа должностных лиц ОМО занимались разработкой автономных информационно-расчетных задач.

Необходимость разработки единой автоматизированной системы, которая охватывала бы ОМО всех уровней управления, стала особенно остро ощущаться в 80-е годы, когда для этого появились и реальные предпосылки: в практику работы штабов начали внедряться ПЭВМ, повысилась компьютерная грамотность должностных лиц ОМО. Поэтому в конце 80-х годов были развернуты работы по автоматизации ОМО военных округов, в ходе которых выявился ряд узких мест, в частности информационно-техническая несовместимость средств автоматизации, эксплуатирующийся в ОМО [26] (1999).

объектовый подход — основные положения его заключаются в следующем: орган управления представляет собой цельный организм, функционирующий по единому алгоритму и оснащаемый типовым КСА; компоненты КСА объединяются между собой вычислительными сетями; обеспечение целостности и непротиворечивости информации достигается использованием единой системы ее классификации и кодирования в АС и клиент-серверной архитектуры при построении КСА; однократность ввода-вывода данных в КСА при организации межобъектового обмена позволяет повысить достоверность и безопасность передаваемой информации [26] (1999).

Автоматизированная система мобилизационного развертывания войск военного округа — разработка первой и второй очереди этой системы завершилась в основном, в конце 1980 и начале 90-х годов соответственно. Комплексы средств автоматизации из состава этой системы поставлены на тысячи объектов по всей стране. При их создании и внедрении впервые для систем такого масштаба решены сложнейшие вопросы организации взаимодействия объектов различного уровня, вопросы перевода существующих информационных фондов на бумажных носителях в электронные базы данных, вопросы обучения личного состава, а также вопросы постоянной модернизации техничес-

ких и программных средств без снижения характеристик функционирования системы в целом.

В 2004 году за создание и внедрение на объекты Министерства обороны автоматизированной системы мобилизационного развертывания войск военного округа Х.И. Сайфетдинову в составе авторского коллектива была присуждена Государственная премия Российской Федерации в области науки и техники [99] (2009).

4.1.8. Автоматизированные системы организаций ВС РФ

автоматизированная система поддержки принятия решений обоснования перспектив развития ВВТ — функционирование разработанной автоматизированной системы предполагает участие в процессе подготовки и принятия решений органов государственного и военного управления, а также научно-исследовательских организаций Министерства обороны и оборонной промышленности.

Автоматизированная система состоит подсистем — автоматизированных рабочих мест (АРМ). Структура АРМ обусловлена, во-первых, спецификой методического аппарата, используемого в каждом из них, во-вторых, необходимостью разграничения доступа к информации, в-третьих, целесообразностью уменьшения громоздкости интерфейса и упрощения работы операторов (пользователей). Все АРМ имеют аналогичную архитектуру, различаясь только по составу используемых исходных данных и набору программно реализованных методик — модулей расчетов. Многие модули используются одновременно в нескольких АРМ.

В целом система позволяет автоматизировать процесс разработки ГПВ и ГОЗ, начиная с момента ввода исходных данных и заканчивая выдачей проекта планового документа на бумажном носителе. Дальнейшее ее совершенствование видится в подключении к информационному обмену других организаций, в том числе структурных подразделений аппарата Совета Безопасности РФ, Генерального штаба и военных округов. Дополнение автоматизированной системы соответствующими модулями обработки данных в итоге должно обеспечить автоматизацию всего процесса программного планирования развития ВВТ: от анализа военно-политической обстановки и определения целей развития системы вооружения до подготовки совокупности плановых документов [30] (2002).

Центр моделирования ВС РФ (ЦМ) — центр, предназначенный для систематизации и обобщения перспективных разработок в области автоматизации и информатизации процессов управления войсками (силами); выработки единой методологии математического моделирования вооруженного противоборства; развития научно-методического аппарата поддержки принятия решений; проведения моделирования операций (боевых действий, других процессов функционирования ВС) и оперативно-стратегических (оперативно-тактических) расчетов; осуществления информационной и интеллектуальной поддержки решений должностных лиц ОВУ; освоения и экспертной оценки программной продукции военного назначения, разрабатываемой организациями промышленности.

Цель создания ЦМ — развитие теории и практики математического моделирования вооруженного противоборства и поддержки принятия решений, оценка состояния разработки и внедрения в автоматизированные системы информационных технологий и программной продукции военного назначения, координация деятельности НИО МО по созданию математических моделей и информационно-расчетных задач, определение направлений, методов и объектов моделирования в интересах повышения обоснованности решений, вырабатываемых органами государственного и военного управления.

Создание ЦМ, по нашему мнению, обеспечит ускоренное развитие научно-методического аппарата поддержки принятия решений ОВУ высшего, стратегического и оперативного звеньев, его внедрение в управленческую деятельность за счет усиления организационно-распорядительных и координирующих функций в системе моделирования вооруженного противоборства, концентрацию всех ресурсов (материальных, технических, людских) на приоритетном научно-практическом направлении, а также приведет к сокращению затрат на создание и эксплуатацию моделирующих систем и комплексов за счет многоцелевого применения составляющих их моделей и задач [47] (2014).

Центр оперативной подготовки Военной академии Генерального штаба (ЦОП ВАГШ) — в конце 1980 — начале 90-х годов функциональные возможности информационных систем военного назначения стали расширяться за счет включения в их состав появившихся к этому времени новых программно-информационных технологий, обеспечивающих прежде всего обработку графической информации, электронных карт и обмен информацией в региональных телекоммуникаци-

онных сетях. Такой разработкой явился ЦОП ВАГШ, предназначенный для обеспечения учебного процесса академии, проведения занятий со слушателями и других оперативных мероприятий. Разработка ЦОП ВАГШ осуществлялась под руководством Х.И. Сайфетдинова и В.П. Тарана при активном участии К.В. Кошкина, В.П. Селезнева, С.Г. Воронкина, П.С. Лукьянова, П.И. Бобнева, В.Д. Антонова, Л.В. Тришиной, Е.А. Неумоина и др.

ЦОП ВАГШ, введенный в эксплуатацию в 1988 году, представлял собой аппаратно-программный комплекс, реализованный на основе IBM-совместимых персональных компьютеров, телевизионных средств индивидуального и коллективного пользования (телевизоры, телекамеры, телепроекторы и видеомагнитофоны), а также средств связи и коммутации, объединенных в локальную вычислительную сеть. Центр размещался в Военной академии Генерального штаба и обеспечивал проведение занятий с несколькими группами слушателей одновременно. Для обеспечения учебного процесса в составе центра реализованы автоматизированные рабочие места руководства, штаба руководства, руководителя занятий, помощника руководителя занятий, групп слушателей, а также обеспечивающих служб.

В состав информационного обеспечения ЦОП ВАГШ впервые были введены электронные карты, соответствующие бумажным обзорно-географическим картам блока «Европа» масштаба 1:1 000 000, и программные средства создания и ведения оперативной обстановки на них. Принципы создания и образцы первых электронных карт также были разработаны в институте [99] (2009).

4.1.9. Автоматизированные системы в военном образовании

автоматизированная система военного образования (АСВО) — организационно-техническая система, в которой на основе современных информационных технологий в автоматизированном и (или) автоматическом режимах реализуются информационные процессы в интересах своевременного и полного обеспечения пользователей необходимой информацией.

Учитывая тесную взаимосвязь военного образования и военной науки, целесообразно в контур АСВО включить подсистему управления научной работой [149] (2006).

4.1.9.1. Компьютерные формы оперативной подготовки

оперативные основы создания компьютерных форм обучения — совокупность положений и соответствующих требований оперативного характера, определяющих основные направления решения научно-технических задач по реализации компьютерных технологий обучения в системе оперативной подготовки в ВС РФ [146] (2016).

оперативные основы создания и внедрения компьютерных форм оперативной подготовки — совокупность положений и требований, вытекающих из системы взглядов военно-политического руководства сторон на возможный характер вооруженной борьбы, формы и способы ведения военных действий во всех видах войн и вооруженных конфликтах.

К оперативным основам также можно отнести содержание и последовательность работы должностных лиц (обучаемых) при выполнении своих функций, а также требования руководящих документов, регламентирующих организацию подготовки и ведения операций (боевых действий) [146] (2016).

компьютерные формы оперативной подготовки[1] (КФОП) — формы обучения должностных лиц, в которых организация и методы проведения мероприятий оперативной подготовки основываются на информационных и компьютерных технологиях обучения.

К компьютерным формам оперативной подготовки можно отнести: компьютерные командно-штабные учения, компьютерные военные игры, компьютерные командно-штабные тренировки.

Центральной компонентой в КФОП будут являться математические модели операций, соответствующие системе операций, принятой в настоящее время в Вооруженных Силах [146] (2016).

компьютерные формы оперативной подготовки[2] (КФОП) — формы обучения органов военного управления и профессионально-должностной подготовки генералов, адмиралов и офицеров, в которых организация и методы проведения мероприятий оперативной подготовки основываются на компьютерных технологиях обучения.

Иначе говоря, КФОП — это такие формы обучения, в которых обучаемые вырабатывают и принимают решения на основе моделирования боевых действий противоборствующих сторон, а руководство

оценивает действия обучаемых путем прогнозирования хода и исхода операций (боевых действий) методом их моделирования по реально принятым сторонами решениям. Именно это и обеспечивает объективность оценки действий обучаемых [189] (2004).

компьютерная форма оперативной подготовки — форма обучения органов управления руководству войсками (силами), где имитация действий войск (сил) сторон, а также оценка работы обучаемых в ходе подготовки и ведения операций (боевых действий) осуществляются на основе системы моделирования боевых и информационных процессов и реализованного в ее составе соответствующего специального математического и программного обеспечения.

Актуальность развития компьютерных форм оперативной подготовки обусловлена, во-первых, повышением требований к уровню подготовленности руководящего состава и должностных лиц органов управления и, во-вторых, сокращением интенсивности традиционных мероприятий в условиях ограничения оборонных расходов, когда практически невозможно проведение полномасштабных войсковых учений [142] (1997).

компьютерные формы боевой подготовки в тактическом звене — командно-штабные учения, военные и командно-штабные военные игры, командно-штабные и штабные тренировки, командирские и тактические занятия (специальные сборы), групповые занятия.

Методы обучения при этом различны: практические занятия по выработке решений на основе моделирования боевых действий сторон, розыгрыш боевых действий методом «свободной игры», компьютерные и телеконференции, компьютерные методы разбора учения (игры) [190] (1998).

компьютерные технологии обучения — совокупность средств и методов обучения на основе применения программно-аппаратных комплексов, обеспечивающих виртуальное отражение реальной обстановки в пространственно-временных показателях проводимого мероприятия оперативной подготовки посредством применения в процессе обучения расчетных методик и методов математического моделирования [146, 189] (2004, 2016).

компьютерные военные игры (КВИ) — форма оперативной подготовки, при которой ЭВМ используются в целях разработки и

обоснования замысла игры, осуществления расчетов для поддержки принятия решений обучаемыми.

При этом одним из основных аспектов использования ЭВМ в компьютерных военных играх является имитация действий войск и розыгрыш операций (сражений, боевых и обеспечивающих действий, ударов) по результатам принятых обучаемыми решений.

Суть игр, на наш взгляд, должна заключаться в следующем. В ходе проведения учения обучаемые принимают соответствующие решения на предстоящие действия, опираясь на данные о поставленной задаче (замысел старшего начальника, свои задачи) и о сложившейся обстановке (противник, свои войска, соседи, местность и др.). Для оценки степени соответствия принятого решения складывающейся ситуации необходимо иметь достаточно достоверные данные прогноза хода и исхода действий при тех или иных вариантах принятых решений. Получить их можно с использованием аналитических методов либо имитационного моделирования, ориентированных прежде всего на оценку эффективности действий войск. Для ее нахождения (вычисления) разрабатываются на основе имеющихся закономерностей математические модели операций (боевых действий). Именно здесь необходимо использование таких качеств современных ЭВМ, как быстродействие и возможность оперировать большими массивами данных, формализующих различного рода случайности и неопределенности, возникающие в ходе подготовки и ведения действий, а также прогнозировать их ход и исход. Таким образом, принятые командирами решения формализуются и с помощью операторов вводятся в ЭВМ. С учетом этих решений и данных по исходной обстановке руководитель учения (штаб руководства) осуществляет розыгрыш операции (боевых действий) с использованием определенной модели операции. В ходе разбора учений (игры) или непосредственно при их проведении имеется возможность показать обучаемым, как принятые ими решения влияют на результаты выполнения поставленной задачи [142] (1997).

математическая модель операции (ММО) — система математических зависимостей и логических правил, позволяющая с необходимой полнотой и в определенной зависимости представить наиболее существенные стороны процесса вооруженной борьбы и с заданной степенью точности определить искомые выходные величины по известным входным данным [146] (2016).

оперативные требования к математическим моделям операций — количественно-качественные показатели, реализация которых с помощью математических и логических зависимостей обеспечит адекватное воспроизведение на средствах отображения процессов двусторонних боевых действий в различных формах и способах их ведения [146] (2016).

4.1.9.2. Информационно-технологическое обеспечение учебного процесса в высшей военной школе

информационно-технологическое обеспечение учебного процесса в военном вузе — система, представляющая собой целостное единство функционально и структурно связанных между собой информационной и технологической составляющих, использование которых в педагогической практике позволяет военному преподавателю в условиях информатизации обучения решать дидактические задачи на технологической основе, т.е. с гарантированным качеством.

Информационную составляющую, обеспечивающую содержательный аспект подготовки военного специалиста в вузе, следует рассматривать в контексте решения задачи полного и адекватного предоставления обучающимся и педагогу учебной и другого рода информации, способствующей гарантированному достижению поставленных дидактических целей. В качестве такой составляющей может, на наш взгляд, выступать дидактический комплекс информационного обеспечения учебной дисциплины. Названный комплекс представляет собой дидактическую систему, в которую в целях создания условий для педагогически активного информационного взаимодействия между преподавателем и обучающимися интегрируются прикладные педагогические программные продукты, базы данных, а также совокупность других дидактических средств и методических материалов, обеспечивающих и поддерживающих учебный процесс.

В качестве технологической составляющей, обеспечивающей процессуальную сторону подготовки специалиста в военном вузе, предлагается рассматривать технологическое обеспечение, которое реализуется на основе применения в учебном процессе современной информационной технологии обучения [158] (2003).

дидактический комплекс учебной дисциплины — дидактическая система, позволяющая военному педагогу реализовать через информационную составляющую процесса обучения целостную информационную технологию обучения.

Этим решается задача гарантированного достижения целей профессиональной подготовки курсантов и слушателей военного вуза. Каждый элемент дидактического комплекса является не просто носителем соответствующей информации, но и выполняет специфические функции, определенные замыслом педагога. Таким образом, комплекс представляет собой постоянно развивающуюся базу знаний в одной из предметных областей, изучающихся в военном вузе.

Для использования дидактических комплексов в высшей военной школе характерно следующее. Во-первых, они проектируются и создаются как целостные системы педагогических программных средств, интегрированных в целях сбора, организации, хранения, обработки, передачи и представления учебной информации их пользователям. Во-вторых, все элементы комплексов взаимосвязаны между собой, имеют единую информационную основу и программно-аппаратную среду. В-третьих, изначально при их проектировании предусматривается возможность использования комплексов как в локальных и распределенных компьютерных сетях военного вуза, так и при дистанционной форме обучения курсантов и слушателей. Этим решается вопрос об их поддержке имеющимися в учебном заведении информационными и телекоммуникационными средствами, а также средствами связи [158] (2003).

информационная технология обучения — 1) дидактический процесс, организованный с применением совокупности внедряемых (встраиваемых) в педагогическую систему принципиально новых средств и методов обработки учебной информации;

2) техническая среда обучения, в которой ключевое место занимают используемые информационные технологии.

В первом случае речь идет о самом процессе обучения, а во втором — о применении в этом процессе специфических программно-технических средств [158] (2003).

4.1.9.3. Информационно-коммуникационные технологии в военном образовании

декларативный способ получения знаний — способ, ориентированный на последовательное предъявление порций учебной информации и контроль ее усвоения (электронные учебники, тестовые и контролирующие программы, справочники и учебные базы данных, учебные видеофильмы) [168] (2009).

процедурный способ получения знаний — способ, строящийся на основе моделей изучаемых объектов, процессов и явлений (имитационные модели, предметно-ориентированные среды и разрабатываемые на их основе лабораторные практикумы, тренажеры, игровые программы) [168] (2009).

система дистанционного обучения — комплекс образовательных услуг, предоставляемых с помощью специализированной информационно-образовательной среды на любом расстоянии от образовательных учреждений [168] (2009).

информационно-коммуникационные технологии в военном образовании — практический опыт внедрения информационно-коммуникационных технологий в образовательный процесс высших военно-учебных заведений свидетельствует, что фундамент образовательных информационно-коммуникационных технологий составляют учебные электронные издания (электронные учебники, учебные пособия, справочники, энциклопедии, тестирующие системы, автоматизированные обучающие курсы), которые позволяют качественно подготовить конкурентоспособных специалистов для рынка труда, способных к профессиональному росту и профессиональной мобильности в условиях информатизации российского общества и развития новых наукоемких технологий [168] (2009).

4.1.9.4. Автоматизированная система планирования и контроля мероприятий боевой подготовки

эффективность функционирования автоматизированной системы планирования и контроля мероприятий боевой подготовки — возможности системы по формированию последовательности про-

ведения спланированных мероприятий боевой подготовки по созданию (формированию, оформлению, представлению) требуемых документов по боевой подготовке по установленному перечню [225] (2017).

эффективность применения автоматизированной системы планирования и контроля мероприятий боевой подготовки — эффективность ее функционирования в требуемых (заданных) условиях и сроках применения. В этой связи эффективность применения автоматизированной системы планирования и контроля мероприятий боевой подготовки характеризуется полнотой реализуемости и объективностью контроля выполнения спланированных мероприятий боевой подготовки (перечня мероприятий боевой подготовки) [225] (2017).

требования к автоматизированной системе планирования и контроля мероприятий боевой подготовки — совокупность качественно-количественных характеристик, определяющих особенности ее построения, функциональную и системную архитектуры, эффективность применения и функционирования [225] (2017).

4.1.9.5. Информационно-аналитическая система для углубленной экспертизы диссертационных работ

информационно-аналитическая система для углубленной экспертизы диссертационных работ — специальная, ориентированная на информационную поддержку экспертизы диссертационных работ, информационно-аналитическая система с развитыми поисковыми и аналитическими функциями, предназначенная для поддержки аналитической работы эксперта [1] (2016).

неструктурированные текстовые данные — набор документов, представляющих собой логически объединенный текст без каких-либо ограничений на его структуру (тексты диссертаций и авторефератов, сообщения средств массовой информации и электронной почты, статьи в книгах и журналах, блоги в социальных сетях, отчеты и нормативные акты) [1] (2016).

система «Антиплагиат» — система, позволяющая быстро провести анализ стиля автора, сравнить предложенный текст с опубликованными в Интернете.

Так могут быть отсеяны откровенно списанные и купленные научные работы.

Наиболее часто используются следующие способы обойти «Антиплагиат»:

1) рерайтинг;

2) использование синонимайзеров;

3) замена определительной придаточной части сложноподчиненного предложения синонимичным ему причастным оборотом;

4) замена обстоятельственной части сложноподчиненного предложения синонимичным ему деепричастным оборотом;

5) использование «черных» методов снижения процента плагиата, добавляя дополнительные невидимые невооруженным глазом символы (после каждого слова или меняя некоторые на латинские) [1] (2016).

рерайтинг — переписывание текста другими словами с сохранением смысла, излагаемого в диссертации.

Приемы рерайтинга: использование синонимичных слов; перевод прямой речи в косвенную; перемещение абзацев; упрощение текста за счет удаления слов и словосочетаний, не несущих смысловой нагрузки, изменения грамматического строя предложений и т.п. Переписанный текст должен обладать тем же или меньшим объемом информации оригинальной статьи при условии сохранения соответствия смысловому содержанию оригинала.

В этом процессе участвует профессиональный коллектив рерайтеров, многие имеют профильное филологические образование и ученую степень [1] (2016).

синонимайзер — программа, заменяющая слова синонимами там, где это возможно.

Для подбора качественных синонимов используются бесплатные или платные онлайн-синонимайзеры.

Разновидностью этого подхода является замена словосочетаний на синонимичные. Некоторые словосочетания можно построить другим способом подчинительной связи, и перед вами будет то же словосочетание, но в иной форме [1] (2016).

система «Антиплагиат.ру» — система, позволяющая бесплатно в отдельном окне сервиса многократно протестировать текст онлайн (до 3000 символов) на уникальность контента [1] (2016).

система «Антиплагиат.ВАК» — система, позволяющая экспертным советам проводить анализ самостоятельности автора при подготовке диссертации, а также повысить эффективность и объективность экспертизы [1] (2016).

система «Антиплагиат.РГБ» — система, обеспечивающая проведение проверки текстовых документов на наличие заимствований или совпадений по полнотекстовой базе электронной библиотеки диссертаций Российской государственной библиотеки (РГБ) и подготовку заключения эксперта РГБ по результату проверки.

Система имеет надежную защиту от простых средств «обхода» проверки и распознает: замены русских букв латинскими; изменения формы слов; замены слов синонимами; изменения порядка слов; перестановки страниц, абзацев, предложений [1] (2016).

4.2. Сетецентрические системы управления в Вооруженных Силах

управление войсками (силами) — теория управления определяет, что наиболее эффективные действия можно организовать только при **централизованном управлении** всеми силами и средствами из одного пункта.

Поэтому для управления сетецентрическими действиями группировок войск (сил) система пунктов управления, входящих в группировку воинских формирований и боевых систем, должна быть иерархической, с передачей функций управления верхнему звену. Это возможно при выполнении следующих условий:

1) наличие на пункте управления достоверной информации о составе, местоположении, состоянии, обеспеченности и действиях противника и своих войск (сил);

2) возможность с помощью КСА верхнего звена формировать эффективные способы действий каждым боевым формированием и средством и доводить до них боевые задачи;

3) возможность реализовать цикл управления, меньший, чем у противника [139] (2011).

управление войсками в условиях автоматизации — рассматривая подготовку и ведение военных действий со времен Великой Отечественной войны (1940—1945) по настоящее время, следует отме-

тить, что организация управления войсками кардинально не изменилась. В частности, по-прежнему остается огромное количество целей действий, задач, алгоритмов и планов для их решения. И это при том, что современные информационные технологии позволяют существенно сократить их.

В решении этой проблемы западные специалисты делают ставку на использование моделирования и имитации для поддержки принятия решений, определения развития событий, планирования выполнения задач на тренировках и в ходе операций (боевых операций).

Подобные подходы к подготовке и ведению боевых действий на базе ЕСУ ТЗ апробируются Главным командованием Сухопутных войск ВС РФ в ходе боевой подготовки 5 омсбр.

Результаты апробации показывают, что применение технологий моделирования потребует обоснованности и высокой степени формализации работы органов управления. Необходимо уточнить содержание и алгоритмы выполнения задач управления, посредством которых будут достигаться цели действий группировок войск, с учетом возможностей средств автоматизации. Поиск, обобщение, анализ информации целесообразно осуществлять при решении любой управленческой задачи.

На основе моделей действий возможно автоматическое формирование планирующих и директивных документов. При этом изменения данных обстановки могут потребовать уточнения соответствующих показателей содержания разделов планирующих документов на основе ситуационной модели действий группировки войск.

Однако научные основы управления войсками, которые сформировались в 80-х годах двадцатого столетия, не отражают в настоящее время возросшего влияния современных информационных технологий на подготовку и ведение военных действий.

В основу технологий реализации интеллектуальной системы поддержки военных действий целесообразно положить современный концептуальный подход к автоматизированному управлению, практический опыт реализации сетецентрических технологий, внедрения существующих отечественных и зарубежных систем автоматизированного управления, разработки перспективных архитектурных решений в ведущихся опытно-конструкторских работах [199] (2011).

советский подход создания сетецентрических систем управления — в последние годы американские военные специалисты стали

трансформировать свои взгляды в сторону российского подхода, который был реализован в СССР еще в 80-х годах прошлого столетия в АСУ тактического звена «Маневр».

Суть его заключалась в следующем. Замысел на применение сил и средств вырабатывается командиром верхнего уровня с участием предложений командиров нижнего уровня. Решения на применение ударных средств и задачу целераспределения на поле боя решает каждый командир нижнего уровня, начиная с командира бригады, полка, батальона, роты, взвода в пределах поставленной ему задачи. Командиры верхних уровней управления решают задачи распределений зон ответственности, усилий, привлечения дополнительных частей и подразделений, либо сил и средств резервов, приданных верхним начальникам.

С учетом вышеизложенного, для создания сетецентрических систем управления для ВС РФ представляется целесообразным использовать подход, в основу которого положены предшествующие отечественные разработки по данному направлению [182] (2011).

недостатки Вооруженных Сил Российской Федерации — по мнению зарубежных аналитиков, при проведении в августе 2008 года операции по принуждению Грузии к миру в ВС РФ в очередной раз вскрылись следующие основные недостатки:

боевые комплексы технически и морально устарели, средства разведки не имели возможности быстро передавать собранную информацию;

устаревшие системы связи и передачи данных не позволяли эффективно управлять подчиненными формированиями, приходилось пользоваться сотовыми и спутниковыми телефонами, имевшимися у корреспондентов;

какая-либо координация и взаимодействие между подразделениями ВВС и СВ отсутствовала, что не позволяло сформировать действительно объединенную группировку войск;

средства высокоточного поражения имелись в единичных экземплярах, носителей, способных применять такое оружие, было недостаточно, на самолетах, вертолетах и танках порой не было ни инфракрасных камер, ни приборов ночного видения, ни систем распознавания «свой—чужой», ни навигационной аппаратуры;

теория оперативного искусства, до сих пор базирующаяся на старых принципах проведения традиционных крупномасштабных назем-

ных операций, не соответствует реалиям современных концепций, предусматривающих массированное применение высокоточных средств вооруженной борьбы [5] (2014).

реализация сетецентрической концепции в ВС РФ — комплексная задача, решение которой предлагает поиск новых технологий, перевод оборонно-промышленного комплекса на инновационный путь развития, уточнение уставов и наставлений, разработку новых форм и способов применения группировок войск, обучение личного состава работе с современными аппаратными и программными средствами [5] (2014).

объединенный орган управления — в первую очередь целесообразно уделить внимание созданию действительно объединенных органов управления, разработке современных алгоритмов их работы при решении различных боевых задач, формированию перечня средств, которые планируется связать в сеть. При этом необходимо понимать, почему и для чего это нужно, иначе на «модное направление» будут израсходованы значительные средства и, кроме того, «неожиданно» возникнет неразрешимая проблема объединения этих разрозненных автономных сетей и сеточек. К сожалению, данные опасения уже сбываются, они нашли отражение в докладе генерал-полковника А.В. Бахина «Организация управления войсками (силами) военного округа новой организации», прозвучавшем на общем собрании Академии военных наук (АВН) РФ 28 января 2012 года. По словам докладчика, на КП Объединенного стратегического командования развернута аппаратура 12 АСУ, элементы которой никак не сопряжены между собой [5] (2014).

основные принципы автоматизации в автоматизированной системе управления округом — в качестве основы для решения проблемы сокращения времени на разработку замысла и доведение распоряжения на применение войск командующим региональной группировкой, которое может составлять до суток и более, может быть взята апробированная на практике и внедренная в Московском военном округе автоматизированная система управления округом, где время от получения боевой задачи до выдачи приказов на применение войск удалось сократить до 1,5—2 часов, что соответствует лучшим зарубежным достижениям.

Этого удалось добиться за счет внедрения следующих основных принципов автоматизации:

1) параллельной работы в автоматизированном режиме всех командиров и штабов с использованием цифровых карт местности и геоинформационных систем для разработки замыслов и решений на применение войск;

2) заблаговременной подготовки, ввода и отображения на цифровых картах исходного положения сил и средств противника, своих сил и средств, возможных сценариев боевых действий, моделей оценки эффективности боевого применения войск;

3) возможности контроля и оперативного участия командиров высшего иерархического уровня в процессе разработки замысла и формирования решения на применение сил и средств подчиненных командиров и штабов;

4) заблаговременной отработки, обучения и слаживания действий командиров и штабов в ходе полевых и командно-штабных учений, компьютерных игр;

5) формирования технических заданий, реализации и военно-научного сопровождения, непосредственного участия в разработке и принятии на снабжение войск АСУ автоматизации округа (АСУ театра военных действий) командиров и штабов всех уровней [182] (2011).

учения по сетецентрической войне — в сентябре 2009 года на территории России и Белоруссии были проведены оперативно-стратегические учения «Запад-2009». В интервью телеканалу «Звезда» бывший тогда начальником Генерального штаба ВС РФ генерал армии Николай Макаров сказал, что в ходе учений отрабатывается концепция сетецентрических войн. В ходе подготовки и проведения учений для топогеодезического обеспечения войск, ведения дежурных карт, 3D-моделирования оперативной обстановки активно применялась принятая на снабжение ВС РФ геоинформационная система (ГИС) «Карта-2005», разработанная КБ «Панорама». 3D-моделирование оперативной обстановки осуществлялось с использованием библиотеки трехмерных условных знаков, разработанной Центром геоинформационного обеспечения топографической службы ВС РФ [27] (2014).

4.2.1. Корпоративные автоматизированные информационные системы военного назначения

корпоративные автоматизированные информационные системы военного назначения (КАИС ВН) — глобальные, территориально распределенные, масштабируемые системы, предназначенные для комплексной автоматизации всех видов систем управления межвидовыми и межведомственными группировками войск (сил) и оружием, систем разведки, наблюдения, навигации, опознавания, целеуказания, наведения, боевых платформ и систем боевого управления в условиях единого информационного пространства.

Основу таких систем составляет совокупность определенным образом организованных во времени и пространстве информационных, вычислительных и телекоммуникационных ресурсов [106] (2015).

сервис-ориентированная архитектура (СОА) — модульная реализация прикладных систем и «открытие» отдельных функций, реализуемых этими системами, в виде сервисов (услуг), доступных другим информационным системам. Технологической основой такого взаимодействия между системами по принципу предоставления услуг друг другу является технология web-сервисов [106] (2015).

сервисы — отдельные законченные функции программного обеспечения, приложений и систем.

Сервисы могут быть доступны из любой точки информационной сети независимо от ее расположения, достаточно иметь лишь физический доступ к сети [106] (2015).

информационный портал (от англ. portal — главный вход; ворота) — общедоступный узел в компьютерной сети или отдельном се сегменте.

На информационном портале размещаются для общего доступа (с учетом полномочий пользователей) информационные ресурсы органа управления, взятые из различных источников [106] (2015).

портлеты — процедурные компоненты портальных технологий, обеспечивающие связи между соответствующими фрагментами визуального интерфейса и функционалом портала [106] (2015).

виртуализация в вычислениях — процесс набора (логического объединения) вычислительных ресурсов, дающий какие-либо преимущества перед оригинальной конфигурацией.

Это новый «виртуализированный» взгляд на ресурсы, не ограниченный их реализацией, географическим положением или физической конфигурацией составных частей. Обычно виртуализированные ресурсы включают вычислительные мощности и хранилище данных [106] (2015).

виртуальная машина — окружение, которое представляется для «гостевой» операционной системы как аппаратное. Однако на самом деле это программное окружение, которое эмулируется программным обеспечением хостовой системы [106] (2015).

центр обработки данных (ЦОД) — объединение большого количества программных и аппаратных платформ различного типа (таких как серверы, дисковые массивы, ленточные библиотеки, средства резервирования и репликации данных, средства обеспечения надежного функционирования).

Центры обработки данных призваны на новом качественном и архитектурно-техническом уровне возродить культуру организации информационно-вычислительного процесса, присущую традиционным вычислительным центрам (ВЦ), размешавшимся на пунктах управления [106] (2015).

базовая операционная система — операционная система, управляющая аппаратным обеспечением центра обработки данных и предоставляющая унифицированную среду программным комплексам [106] (2015).

гипервизор — операционная система, обеспечивающая виртуализацию аппаратных ресурсов и управления виртуальными машинами [106] (2015).

4.2.2. Сетецентрические технологии

модель сетецентрического управления групповым движением объектов через конфигурирование квазисиловых полей[1] — модель, разработанная специалистами Института проблем управления РАН имени В.А. Трапезникова.

Модель направлена на обоснование возможностей автономизации управления групповым движением БЛА или других видов мобильных объектов, подразумевает переход от дистанционного управления к автоматическому выполнению миссий посредством сетецентрической самоорганизации всех аппаратов в условиях сложной и быстро меняющейся обстановки с учетом активного противодействия как со стороны традиционных средств ПВО, так и групп БЛА противника.

Подобное применение БЛА или других роботизированных средств вооруженной борьбы в едином пространстве сетецентрического управления, по мнению специалистов института, обеспечивает следующие преимущества:

— распределенное размещение на средствах вооруженной борьбы большего количества разнообразных средств многоканального сбора информации, противодействия и поражения;

— существенное повышение точности определения координат подвижных целей, достигаемое путем множественного их определения отдаленными друг от друга летательными аппаратами (роботизированными средствами) и последующей обработкой сведений в едином алгоритмическом пространстве — эффект зондирования с большой базой;

— возможность концентрации распределенных многоканальных средств обнаружения, высокоточного наведения и поражения посредством динамически самоорганизующейся их аккумуляции в определенном месте и в определенный момент времени — эффект «флешмоба»;

— кардинальное повышение вероятности успешного выполнения миссии при минимизации расхода боезапаса, собственных потерь и непланируемого ущерба, достигаемого за счет высокого качества управления и максимальной координации боевых возможностей средств вооруженной борьбы, направляемых на наиболее уязвимые места с высокой точностью и синхронностью [5] (2014).

модель сетецентрического управления групповым движением объектов через конфигурирование квазисиловых полей[2] — модель, разработанная специалистами одного из институтов РАН, которая обосновывает возможности перехода от дистанционного управления к автоматическому выполнению миссий посредством сетецентрической самоорганизации всех аппаратов в условиях сложной и быстроменяю-

щейся обстановки (с учетом активного противодействия как со стороны традиционных средств ПВО, так и групп БПЛА противника).

У специалистов института имеются решения, связанные с разработкой новой элементной базы и ее архитектуры, обеспечивающей качественно новые возможности полномасштабного решения задач сетецентрического управления в ресурсах глобально связанных сетей. Такие решения, по заверениям ученых, не требуют новых технологий проектирования и изготовления сверхбольших интегральных схем (СБИС). По их словам, опытная партия прототипа элементной базы с принципиально новой архитектурой «управляющий компьютер на кристалле», поддерживающей единое пространство сетецентрического управления, может быть реализована на доступных технологиях проектирования и изготовления СБИС с проектными нормами 65—45 нм в течение двух-трех лет при относительно малых затратах [27] (2014).

геоинформационная система «Карта-2011» — комплект программ, разработанных ЗАО КБ «Панорама», способствующий организации топогеодезического обеспечения войск на основе принципов сетецентрического управления в перспективных АСУ войсками и оружием.

Она содержит:

— средства обработки данных с навигационных приборов GPS и ГЛОНАСС (наиболее современное и высокоточное оборудование российской разработки может быть подключено с применением комплекса GEO-RTK, разработанного Российским институтом радионавигации и времени);

— средства обработки данных с БПЛА (первичная обработка данных выполняется в комплексе «Фотомод», разработанном компанией «Ракурс»);

— данные с геодезических приборов различного назначения;

— цифровые карты, снимки Земли, матрицы высот, размешенные на удаленных серверах пространственных данных под управлением ГИС «Сервер» (разработка КБ «Панорама»);

— интернет-ресурсы карт, снимков, матриц, публикуемые на сайтах Google, Yandex, Digital Globe, OpenStreet по специализированным http-протоколам;

— цифровые карты, снимки Земли, матрицы высот, доступные через web-сервисы по стандартам OGC WMS, WFS, IVCS.

Сетецентрический подход построения информационной системы основан на создании равноправных территориально распределенных узлов, выполняющих различные функции и предоставляющих пользователям возможность работы с приложениями и базами данных с помощью браузера из любого места и с любого устройства, подключенного к Интернету. Узлы сети могут передавать данные, подготавливаемые различными службами и подразделениями: разведкой, РЭБ, инженерным обеспечением, топогеодезическим обеспечением, техническим и тыловым обеспечением и т.д. ГИС «Сервер» не только предоставляет доступ к данным, но и выполняет функции защиты данных. Операторы, работающие с ГИС «Карта-2011», могут одновременно подключаться к нескольким ГИС-серверам с разными правами на просмотр, редактирование и копирование данных.

ГИС «Карта-2011» обеспечивает автоматизированную обработку всех видов пространственных данных, в частности:

— векторных карт и планов в различных проекциях и системах координат, включая морские карты, радионавигационные (воздушные), навигационные и другие;

— данных дистанционного зондирования Земли (космические снимки в оптическом диапазоне), мультиспектральных снимков, данных лазерного сканирования, эхолокации и др.;

— регулярных матриц высот, матриц качественных характеристик (покрытия), TIN-моделей;

— 3D-моделей [27] (2014).

математические модели интеллектуальной поддержки принимаемых решений — одной из наиболее сложных задач, требующих применения моделей, является формирование группировки войск для проведения современных операций (боевых действий). Данная проблема, по мнению авторов, включает в себя определение: состава группировки, а для каждого ее компонента — его элементов; перечня и объема функций (задач), выполняемых каждым компонентом (элементом); структуры функционального и информационного взаимодействия между всеми звеньями группировки.

При разработке моделей по формированию группировок войск необходимо выполнить ряд основных условий:

1) Адекватный учет и формализация в модели воспроизводимых процессов управления войсками и оружием.

2) Декомпозиция и агрегирование в модели функций (задач) составных частей группировки войск с требуемой степенью их детализации в целом и реализация для каждого уровня своей структуры логических отношений между компонентами (элементами).

3) Адаптивное и оперативное изменение функциональных возможностей модели в соответствии со складывающимися как оперативно-тактической обстановкой и условиями ведения боевых действий, так и с необходимыми потребностями органов управления войсками и оружием.

4) Обеспечение для должностных лиц органов управления войсками и оружием ясности и понятности методологии моделирования, прозрачности используемых математических методов, отсутствия существенных ограничений на размерность модели, простоты управления процессом моделирования и оперативности получения результатов, наглядности представления и интерпретации результатов моделирования, дружественного пользовательского интерфейса.

5) Единый методологический подход к моделированию функций (задач) компонентов (элементов) группировки войск при подготовке и проведении операций (боевых действий), а также организации реализующих их информационно-вычислительных процессов на комплексах средств автоматизации пунктов управления и автоматизированных рабочих местах должностных лиц в составе автоматизированных систем управления войсками [214] (2012).

4.2.3. Разработанные автоматизированные системы управления сетецентрического типа

автоматизированная система управления войсками «Маневр» — единая автоматизированная система управления общевойскового соединения, объединявшая все его части (полки и отдельные подразделения) с использованием центральной ЭВМ дивизии («Бэта-3») и бортовых ЭВМ дивизионного звена для решения боевых задач начиная со сбора информации, ее обработки и обмена, уяснения задачи, принятия решения, планирования боя дивизии, ее частей и подразделений, постановки им боевых задач, управления ходом боя и контроля за его результатами.

Парадигмой этой разработки была позиция, что не могут существовать отдельно система управления войсками, система автоматизации и система связи, что это единая динамичная сложная система, направ-

ленная на достижение превосходства над системой управления противника и победы в бою. Есть либо автоматизированная, либо неавтоматизированная системы управления. Третьего не дано [186] (2010).

автоматизированная система управления Воздушно-десантными войсками «Полет-К» — работы по ее созданию начались в 1993 году. «К» означало космическую компоненту АСУ. «Полет-К» должен был стать технической основой собственной идеологии управления сетецентрическими действиями ВДВ. АСУ ВДВ была в целом спроектирована к началу 2000 года, отдельные ее элементы прошли успешные полигонные испытания, которые показали, что эта система пригодна и для управления формированиями Сухопутных войск. «Полет-К» нельзя было подавить никакими радиоэлектронными средствами, нейтрализовать компьютерным вирусом. Было реализовано множество уникальных технических решений, к которым в то время в США только подступались. В «Полете-К» новейшая идея управления сетецентрическими действиями была реализована наиболее оптимальным образом. Однако тема была закрыта [179] (2012).

автоматизированная система управления Северо-Кавказского региона (АСУ «Акация») — базовые программно-технические средства автоматизации для обеспечения автоматизированного управления войсками (силами) Северо-Кавказского военного округа, объединениями, соединениями и частями видов Вооруженных Сил РФ, дислоцированных в регионе, а также обеспечения автоматизированного взаимодействия с воинскими формированиями других министерств и ведомств, государственными органами власти субъектов РФ на территории региона.

АСУ Северо-Кавказского региона (СКР) должна была состоять из двух частей: стационарной и мобильной.

Предполагалось, что основой АСУ СКР должна была стать стационарная часть, состоящая из унифицированных комплексов средств автоматизации, предназначенных для оснащения штабов повседневных пунктов управления оперативно-стратегического, оперативного и тактического звеньев управления, а также защищенных стационарных пунктов управления оперативно-стратегического и оперативного звеньев.

Мобильная часть должна была наращивать стационарную часть до структуры АСУ СКР в целом и состоять из КСА подвижных пунктов управления объединений, соединений и частей и подразделений

всех видов ВС РФ и других ведомств, имеющих войсковые формирования на территории Северо-Кавказского региона.

Однако в ходе работы по результатам выполнения эскизно-технического проекта ОКР «Акация» (ноябрь 1997 года) в связи с ограниченным финансированием было принято решение о создании только стационарной части АСУ СКР. В результате коллективу ФГУП «Концерн «Системпром» за относительно короткое время (три года) удалось разработать опытный образец стационарной части АСУ СКР, включивший в себя:

унифицированные комплексы средств автоматизации (УКСА) штаба военного округа (региона), штаба тыла военного округа, штаба вооружения военного округа, защищенного (запасного) командного пункта (КП) округа (региона), штаба армии (армейского корпуса), штаба (защищенного КП) армии (армейского корпуса), штаба военно-морской базы (ВМБ), штаба флотилии, штаба дивизии (отдельной бригады);

автоматизированное рабочее место удаленного объекта (АРМ-У), предназначенное для установки во взаимодействующих органах управления, в том числе в органах управления других силовых министерств и ведомств для формирования единого контура автоматизированного управления;

автоматизированное рабочее место удаленное переносное (АРМ-УП), предназначенное для работы должностных лиц оперативного состава вне мест постоянной дислокации (в составе оперативных групп и т.д.).

Для применения в органах управления высшего звена управления Вооруженных Сил Российской Федерации был разработан информационно-коммуникационный программно-технический комплекс (ИКПТК).

Государственные испытания стационарной части АСУ СКР проходили в 2001 году при проведении на Северном Кавказе контртеррористических операций. В течение последующих лет доработанная по результатам государственных испытаний стационарная АСУ СКР прошла опытную эксплуатацию. В настоящее время стационарная АСУ «Акация» принята на снабжение (вооружение) ВС РФ.

Все перспективные системные, технические, программные и другие базовые решения, положенные в основу создания стационарной АСУ «Акация», были в последующем развиты и реализованы в разработанной ФГУП «Концерн «Системпром» мобильной части автомати-

зированной системы управления войсками (силами) региона, которая с положительными результатами прошла государственные испытания.

Были разработаны комплексы средств автоматизации (КСА) для формирования полевых подвижных пунктов управления (ППУ) фронта, армии (армейского корпуса).

Мобильные комплексы средств автоматизации обеспечивают:

повышение эффективности боевого управления на основе комплексной автоматизации процессов планирования, организации и управления войсками и силами в регионе;

повышение устойчивости, непрерывности, оперативности и скрытности боевого управления;

сокращение продолжительности циклов и основных процессов боевого управления во всех видах деятельности органов управления ППУ;

комплексную автоматизацию на единых для всех элементов системы управления системотехнических, программных и информационно-лингвистических средствах.

Основой мобильной части автоматизированной системы управления войсками (силами) региона является ряд автоматизированных подвижных единиц (АПЕ), предназначенных для работы должностных лиц органов управления, позволяющих сформировать в настоящее время комплексы средств автоматизации полевых подвижных пунктов управления объединенного стратегического и оперативных командований любого формата [191] (2011).

автоматизированная система управления оперативно-стратегического звена «Акация» — идеи сетецентрического управления войсками планируется реализовать и в этой системе. К концу 2012 года российская армия при достаточном финансировании может быть полностью оснащена мобильным вариантом системы «Акация-М» — военным аналогом Интернета.

Вместе с тем очевидно, что без системы управления тактическим звеном, т.е. уровнем «бригада — батальон — рота — солдат», автоматизация управления оперативно-стратегического уровня большого смысла не имеет [179] (2012).

Единая система управления тактического звена[1] (ЕСУ ТЗ) — задачу по созданию этой системы решает с 2000 года концерн «Созвез-

дие», ведущее предприятие радиоэлектронной промышленности по созданию АСУ, средств связи для ВС РФ и силовых структур.

Ее принятие на вооружение может стать революцией в области военного управления. Например, ЕСУ ТЗ позволяет расширить район ведения боевых действий бригады вдвое при двукратном сокращении времени цикла боевого управления. При этом возможно непрерывное ведение боевых действий и их обеспечение, что позволяет максимально использовать боевой потенциал тактических формирований. Испытания показали — отдельные нормативы военнослужащими выполняются в 40 раз быстрее, чем раньше. В системе используется не просто компьютер, а коммуникатор, который в режиме IP-телефонии позволит выйти на отдельного военнослужащего простыми набором номера. Вес аппаратуры с WiFi-связью, GSM-модулем, ГЛОНАСС и радиостанцией шестого поколения — полкилограмма. Основу комплекса составляет ПЭВМ отечественного производства. Единая цифровая защищенная полевая сеть связи создается с использованием мэдж-технологий на базе станций Wi-Fi. Для обеспечения оперативных контуров управления в составе оперативного командования (армии) требования по взаимодействию заданы в обеих системах. Более того, ЕСУ ТЗ должна взаимодействовать не только с «Акацией», но и с другими АСУ видов и родов войск на основе интеграции их ресурсов.

Вместе с тем, создание ЕСУ ТЗ и ее сопряжение с АСУВ «Акция» затягивается. Все упирается в надежность оборудования, устойчивость каналов связи и производство комплектующих. Имеются сложности и в создании программного обеспечения ЕСУ ТЗ. Интерфейс программных комплексов остается очень сложным, не всегда отвечающим логике боя и алгоритмам действий военнослужащих. Проблема здесь кроется в том, что в условиях принижения значимости военно-научного сопровождения разработки ЕСУ ТЗ со стороны НИУ МО РФ программисты концерна «Созвездие» при создании программного обеспечения использовали идеологию и принципы, не предназначенные для решения военных задач. В Министерстве обороны признают, и это очевидно, что ЕСУ ТЗ сейчас требует значительной переработки [179] (2012).

Единая система управления тактического звена[2] (ЕСУ ТЗ) — был одобрен весьма спорный вариант этой системы, суть которого сводилась к разделению ЕСУ ТЗ на 11 независимых друг от друга вертикалей. При этом каждая из них возглавлялась своим заказчиком,

своим главным конструктором, своим органом военно-научного сопровождения, да еще и собственным военачальником. В итоге не были выполнены ни по срокам, ни по содержанию требования концепции 2002 года о создании единой системы управления войсками (силами) и оружием в тактическом звене на период до 2010 года, основными принципами которой являлись: руководящая роль общевойскового командира, единая информационно-техническая основа, координация систем информационного обеспечения, огневого поражения, РЭБ и связи в единые автоматизированные боевые системы, интегрирующие функции управления, разведки, связи, РЭБ, навигации, опознавания, максимально эффективное осуществление управление.

Система связи — это органичная и очень важная составляющая автоматизированной системы управления (а не функциональная и самодостаточная структура и часть ЕСУ ТЗ), она ее нерв. А командование и штаб — не подсистема, а мозг АСУ. И нельзя мозг ограничивать только постановкой и решением информационных и расчетных задач. Как минимум без комплексного моделирования боя в помощь интеллекту и воле общевойскового командира не обойтись [186] (2010).

недостатки разрабатываемых программно-аппаратных средств — в настоящее время предприятия военной промышленности в целях автоматизации процессов управления в ВС РФ в условиях жесткой конкуренции создают определенные программно-аппаратные средства. Однако по своим параметрам они зачастую несовместимы.

Кроме того, промышленные разработки должны обеспечивать реальную автоматизацию процессов управления, а не обозначение возможностей. Для этого необходимо сформировать общее понимание конечного результата автоматизации управления у представителей военной промышленности, повысить роль военно-научного сопровождения.

В первую очередь требует пересмотра организация разработки и внедрения специального программного обеспечения. Большое количество разработанных расчетных и информационных задач (иногда однотипных) сложны в применении. Поэтому в работе органов управления войсками они не применяются.

Так, в ходе отработки учебных вопросов на опытном батальонном тактическом учении с применением программно-технических средств единой системы управления тактическим звеном (ЕСУ ТЗ) со 2 мсб 5 омсбр командир и штаб батальона, командиры рот и взводов

отработали и передали 1018 документов, 4609 команд и сигналов управления, взаимодействия и оповещения. Документы и команды управления создавались вручную, на электронной карте и в виде текстов. Почти половину времени (около 40%) цикла управления затрачивалось на обработку информации [199] (2011).

4.2.4. Перспективы реализации сетецентрических концепций

автоматизированная система управления — единая (т.е. вневидовая и вневедомственная) или не единая (только, например, соединений и частей Сухопутных войск) — это чрезвычайно сложная, динамичная, человеко-машинная система, нацеленная на победу над подобной же системой противника в интеллектуально-информационно-разведывательно-навигационно-электронно-огневом противоборстве [186] (2010).

информационно-управляющая система военного назначения (ИУС ВН) — автоматизированная система, которая должна обеспечивать реализацию эффективных способов оперативного (боевого) управления при подготовке и ведении войсками (силами) операций (боевых действий) с использованием самого современного вооружения и военной техники и в любых условиях обстановки, что в настоящее время подразумевает применение сетецентрического принципа в построении такой системы [28] (2009).

4.2.4.1. Перспективный облик системы управления Вооруженными Силами Российской Федерации

оперативные основы создания перспективного облика системы управления Вооруженными Силами — совокупность положений и требований, вытекающих из системы взглядов военно-политического руководства сторон на возможный характер вооруженной борьбы, формы и способы ведения военных действий во всех видах войн и вооруженных конфликтов, а также положения и требования, вытекающие из руководящих документов и нормативно-правовых актов, регламентирующих работу ОВУ при подготовке и ведении операций (боевых действий) и развитии системы управления [147] (2015).

оперативные требования к системе управления Вооруженными Силами Российской Федерации — количественно-качественные показатели ее функционирования, которые будут определять ее перспективный облик на заданный период развития [147] (2015).

перспективный облик системы управления Вооруженными Силами — состояние, при котором количественно-качественные показатели ее функционирования обеспечат решение задач управления войсками (силами) при применении различных форм и способов ведения военных действий с заданной (требуемой) эффективностью [147] (2015).

оперативные исходные данные (оперативные постановки задач) — сведения, которые невозможно изложить в ТТЗ на ОКР, но они необходимы генеральным конструкторам.

Например, функции должностных лиц органов военного управления и алгоритмы их работы при управлении войсками (силами) при подготовке и входе ведения операций (боевых действий) [147] (2015).

4.2.4.2. Единая (общевойсковая) автоматизированная система управления

единая (общевойсковая) автоматизированная система управления для ВС государства — должна быть централизованной, иерархической и территориальной, обладать развитыми горизонтальными связями, иметь «вертикальные стволы» управления отдельными системами и видами ВС. Модульное и сетевое построение КСА органов управления и АСУ в целом, наличие гибкой структуры и алгоритмов функционирования сделают такую систему адаптивной, способной адекватно реагировать на изменение средств и способов ведения военных действий.

Можно определить следующие принципы построения перспективных АСУ группировками ВС:

— объединение в единую глобальную информационно-управляющую сеть всех органов управления, а также сил и средств разведки и РЭБ;

— организация эффективных вертикальных и горизонтальных связей в структуре системы;

— автоматизированные поддержка принятия решений и обеспечение планирования операций (боевых действий) на основе комплексных математических моделей (экспертных систем);

— оперативное получение необходимых (санкционированных) данных любым органом управления;

— гибкая структура АСУ и способность к непрерывному развитию;

— модульное построение глобальной информационно-управляющей сети;

— использование единых стандартов и форматов документов;

— полная совместимость применяемых программных и аппаратных средств;

— гарантированная защита информации от несанкционированного доступа [18] (1999).

единая автоматизированная система управления — автоматизированная система, предназначенная для обеспечения руководства всеми войсками (силами), размещенными или действующими в конкретном регионе (на стратегическом направлении), независимо от их принадлежности.

Начинать ее создание целесообразно с автоматизации управления повседневной деятельностью штабов всех уровней, так как это позволит быстро и при минимуме затрат повысить эффективность управления войсками. Причем в первую очередь необходимо автоматизировать процессы, связанные с организацией боевой, оперативной и мобилизационной подготовки войск, планированием их применения, оценкой обстановки. Наиболее перспективными средствами для этого являются персональные ЭВМ и новейшие информационные технологии. Их использование в совокупности с электронными картами, макетами местности и имитаторами позволяет проводить компьютерные военные игры различного масштаба [84] (2005).

система информационного обеспечения деятельности штабов и войск — система, которая обеспечивала бы своевременность сбора и обработки информации, поступающей от различных источников, постоянное знание штабами обстановки и быстрое принятие обоснованных решений на выполнение различных мероприятий, сокращение времени на доведение данных обстановки до подчиненных инстанций.

Повышение эффективности деятельности штаба во многом зависит от сокращения сроков сбора и обобщения данных обстановки. Как

показывает опыт учений, сбор информации занимает большую часть рабочего времени основных должностных лиц органов управления. Сокращение интервала времени от момента начала событий до получения о них сведений командующим и штабом — одна из серьезных проблем управления. Она может быть решена, прежде всего, путем улучшения организации работы по сбору информации, упорядочению потока данных и сокращению его объема. Суть проблемы сбора и обработки информации заключается еще и в том, что в разных областях деятельности одни и те же данные обстановки интерпретируются поразному. Поэтому главное внимание следует обратить на целенаправленность сбора и обработки информации. Информационные материалы в совокупности должны содержать все количественные и качественные характеристики основных факторов, влияющих на выполнение задачи.

При наличии системы информационного обеспечения деятельности штабов и войск появится возможность оперативно влиять на ход событий, сокращать время на постановку задач подчиненным войскам, более рационально использовать имеющиеся силы и средства, своевременно предвидеть возможные изменения обстановки, четко координировать деятельность подчиненных штабов, обеспечивать непосредственное руководство подготовкой и практическим осуществлением мероприятий. Создание эффективной системы информационного обеспечения возможно на базе существующих средств автоматизированного управления путем объединения пользователей в локальные сети [84] (2005).

4.2.4.3. Создание единой стационарно-мобильной автоматизированной системы управления войсками и оружием объединенного стратегического командования

единая стационарно-мобильная автоматизированная система управления войсками (силами) и оружием объединенного стратегического командования (ЕАСУ ОСК) — автоматизированная система, создаваемая с применением передовых информационных и телекоммуникационных технологий и обеспечивающая в различных условиях обстановки централизованное и децентрализованное автоматизированное управление дислоцированными в зоне ответственности объединенного стратегического командования войсками (силами)

(независимо от видовой и ведомственной принадлежности) во всех звеньях управления на основе взаимоувязки подсистем разведки, связи, навигации, опознавания, огневых и ударных средств в единую автоматизированную систему [152] (2013).

унифицированные программно-технические комплексы (УПТК) — информационно-техническая основа создания единой стационарно-мобильной автоматизированной системы управления войсками (силами) и оружием объединенного стратегического командования, включающая средства автоматизации, связи и обмена данными, навигации, разведки и опознавания различного исполнения и предназначения, разработанные на единых нормативно-технических и методических документах с применением новейшей элементной базы отвечающие требованиям информационной безопасности и технологической независимости, позволяющие (в том числе) формировать пункты управления (ПУ) различного уровня (по модульному принципу) и обеспечивающие возможность должностным лицам органов управления выполнять свои обязанности как на месте, так и в движении.

Рациональная структура данной автоматизированной системы может быть сформирована на основе взаимоувязанных: стационарных УПТК органов и ПУ; мобильных УПТК подвижных ПУ; переносных УПТК мобильных ПУ; носимых УПТК [152] (2013).

переносные унифицированные программно-технические комплексы — комплексы, используемые для развертывания мобильных пунктов управления в палатках, во временных укрытиях (например, в блиндажах, окопах) [152] (2013).

мобильные унифицированные программно-технические комплексы — комплексы, устанавливаемые в базовые платформы боевых и обеспечивающих машин с одновременной интеграцией с их управляющими системами [152] (2013).

носимые унифицированные программно-технические комплексы — комплексы, имеющие в своем составе автономные средства автоматизации и связи, минимально необходимые должностному лицу при его нахождении вне автоматизированной подвижной единицы применительно к уровню управления с обеспечением возможности подключения дополнительного оборудования (ведения разведки, в том

числе радиационной и химической, видеонаблюдения, определения координат целей, жизнеобеспечения и др.) [152] (2013).

интеграция информационных ресурсов — один из важных вопросов при создании единой стационарно-мобильной автоматизированной системы управления войсками (силами) и оружием объединенного стратегического командования, решаемый для вышестоящих, взаимодействующих, подчиненных (приданных) объектов управления (в том числе систем разведки, оружия и т.д.), расположенных в зоне ответственности объединенного стратегического командования.

Принципиальная особенность подхода к созданию данной автоматизированной системы заключается в переходе от документального к фактографическому обмену данными в интересах повышения оперативности управления через комплексную автоматизацию всего информационно-вычислительного процесса (в первую очередь процесса разработки оперативных (боевых) документов) в реальном масштабе времени или близком к нему с широким использованием различных систем поддержки принятия решений, ориентированных на непрерывный мониторинг обстановки [152] (2013).

единая визуализация данных обстановки, ее изменений и решаемых задач — такая визуализация на основе цифровых карт местности обеспечит автоматизированную поддержку процессов комплексного планирования, координации, контроля и применения различных средств поражения (артиллерии, ракетных войск, авиации и т.д.). В реальном масштабе времени будет обеспечено комплексное представление разнородной информации, привязанной к пространству и ко времени (т.е. географически достоверной), что позволит существенно повысить степень восприятия географической и оперативно-тактической информации должностными лицами органов управления и операторами огневых и ударных систем, оперативность выработки решений и их качество с одновременным снижением нагрузки на людей за счет высвобождения от нетворческой, рутинной работы [152] (2013).

инфраструктурная система топографического обеспечения — система, позволяющая получать и обрабатывать информацию из различных источников (например, фото- и видеоизображений местности) с целью создания актуальных цифровых карт местности, на основе которых формируется **единая картина оперативно-тактической об-**

становки для обеспечения эффективного функционирования автоматизированных подсистем [152] (2013).

4.2.4.4. Автоматизированная система управления войсками сетецентрического типа

автоматизированная система управления войсками сетецентрического типа — композиция единого информационного пространства, единого функционального пространства, единого исполнительного пространства и единого коммуникационного пространства [214] (2012).

единое информационное пространство[6] (ЕИнП) — предоставляет возможность для создания и поддержания в актуальном состоянии общей «языковой» среды, в которой все компоненты (элементы) группировки войск могут общаться на едином информационном языке и однозначно интерпретировать факты и события предметной области: интегрированного хранилища информации, из которого все компоненты (элементы) группировки войск могут брать необходимые им для выполнения своих функций (задач) данные [214] (2012).

единое функциональное пространство (ЕФП) — позволяет: создавать и поддерживать в актуальном состоянии интегрированный банк (хранилище) функций, обеспечивающих реализацию потребностей и возможностей компонентов (элементов) группировки войск по выполнению возлагаемых на них боевых задач; осуществлять адаптивное формирование структуры группировки войск и ее компонентов (элементов) под цели и задачи операции (боя); взаимосогласовывать по целям, задачам и информации выполнение функций (задач) всеми компонентами (элементами) группировки войск [214] (2012).

единое исполнительное пространство (ЕИсП) — должно обеспечивать создание и поддержание в актуальном состоянии интегрированного банка (хранилища) исполнительных компонентов (элементов), обеспечивающих адаптивное формирование структуры группировки войск как по намеченным целям, так и по поставленным боевым задачам операции (боя) [214] (2012).

единое коммуникационное пространство (ЕКП) — обеспечивается: применением на объектах автоматизации компонентов (эле-

ментов) группировки войск программно-аппаратных средств цифровой передачи, приема и обработки информации, основанных преимущественно на принципах программно-определяемого радио; использованием унифицированных протоколов информационного обмена; созданием тактического Интернета [214] (2012).

4.2.4.5. Универсальная автоматизированная система управления войсками

единое информационно-коммуникационное пространство[4] — совокупность высокотехнологичных коммуникационных средств и необходимых информационных ресурсов (данных), обеспечивающих своевременное решение управленческих задач в целях эффективного воздействия на противника в реальном масштабе времени.

По-нашему мнению, понятие «единое информационно-коммуникационное пространство» в более полной мере, чем относительно узкое по смыслу понятие «единое информационное пространство», соответствует реально происходящим изменениям в военной и смежных с ней науках в области управления войсками и оружием. По сути, отражаемое данным понятием явление представляет собой материальный объект в виде высокотехнологичной глобальной информационно-коммуникационной сети, что, кстати, соответствует сущности понятия «сеть» в теории сетецентрической войны.

Вряд ли нужно доказывать, что «единое информационно-коммуникационное пространство» не является пространством как таковым, а представляет собой совокупность современных средств (в самом широком смысле), которая позволяет существенно повысить возможности управления, в частности, войсками и оружием.

Несмотря на условность понятия «Единое информационно-коммуникационное пространство», этой условностью можно пренебречь, так как в конечном счете данное понятие трансформируется в понятие «Универсальная автоматизированная система управления войсками» [165] (2012).

универсальная автоматизированная система управления войсками (УАСУВ) — организационно, функционально и технологически интегрированная (объединенная) совокупность средств, органов и функций, обеспечивающая в реальном масштабе времени требуемый уровень программно-информационного обеспечения командных ин-

станций и осуществление ими всей совокупности информационных процессов, направленных на максимально эффективное поражение противника и защиту своих войск [165] (2012).

4.2.4.6. Автоматизированная система управления подготовкой и ведением военных действий

система управления подготовкой и ведением военных действий — совокупность функционально взаимоувязанных органов военного управления, объединенных общей управленческой деятельностью, информационная связность которых реализуется ресурсами обеспечивающих автоматизированное управление систем [199] (2011).

система обеспечения автоматизированного управления — система, создающаяся на основе автоматизации основных информационных процессов.

Она включает: интеллектуальную систему поддержки военных действий, информационно-телекоммуникационную систему, систему поиска (добывания) информации [199] (2011).

интеллектуальная система поддержки военных действий (ИСПВД) — система с соответствующим специальным программным обеспечением, позволяющая адаптировать автоматизацию управления войсками к целям и задачам действий войск.

При этом наряду с задачами оптимизации действий войск должны применяться многоуровневые системы комплексного моделирования противоборства сторон, включающие моделирование систем всестороннего обеспечения и обслуживания.

Составной частью ИСПВД может рассматриваться база знаний, которая должна непрерывно пополняться за счет поступления информации от всех компонентов системы автоматизированного управления подготовкой и ведением военных действий [199] (2011).

4.2.4.7. Автоматизированная система управления авиацией

многофункциональность — в последнее время начали разрабатываться и уже ставятся на вооружение новые многоцелевые авиационные средства (комплексы), способные комплексно решать весь

спектр задач, стоящих перед авиацией (ударные, истребительные, разведывательные, специальные и др.) и обладающие возможностью перенацеливания уже в ходе выполнения боевой задачи. Необходима новая технология создания комплексов средств автоматизации, обеспечивающая возможность (причем не только методологически, но и инструментально) выделения полного набора частных задач и функций управления, характерных для каждого конкретного органа военного управления, и последующего синтеза КСА, обладающего необходимой функциональностью, универсальностью, возможностью наращивания и адаптации (реконфигурации) при изменении условий применения (в том числе в процессе эксплуатации) [29] (2008).

интеллектуализация комплекса средств автоматизации — осуществляемая за счет разработки и внедрения в них комплексных, математических моделей и экспертных систем, адекватно отражающих реальные условия, средства вооруженной борьбы и учитывающих закономерности функционирования и взаимные связи между ними. Моделирование вариантов развития событий с помощью комплексных моделей позволит прогнозировать действия по выполнению задач, стоящих перед авиацией, и оценивать полученные результаты по выбранным показателям и критериям. В основу новой технологии должно быть положено создание имитационно-аналитических моделей сил и средств вооруженной борьбы с применением принципа объектно-ориентированного анализа сложных систем. При этом создаются модели средств вооруженной борьбы и геофизических условий [29] (2008).

открытая архитектура — построенная на принципах открытых сетевых архитектур, с помощью которых создаются вертикальные и горизонтальные связи, обеспечивающие возможность взаимодействия между собой любых органов и пунктов управления, объединения их в региональные сети управления соединений родов войск (видов ВС) и в глобальные сети управления объединений и ВС в целом. При этом обеспечивается построение территориально распределенных, интегрированных и адаптивных вычислительных сетей военного назначения с единым информационным пространством. Это позволит интегрировать видовые и иные специальные системы управления не только в информационно-управляющие сети отдельных группировок войск, но и в единую глобальную информационно-управляющую сеть ВС РФ [29] (2008).

модульность — средства автоматизации должны строиться по блочно-модульному принципу и иметь архитектуру, позволяющую наращивать (изменять) состав технических средств для использования на всех пунктах управления. Модульное построение КСА создаст гибкую структуру АСУ и способность к ее непрерывному развитию без особых финансовых затрат [29] (2008).

сетевые принципы построения — позволять реализовать концепцию распределенного пункта управления, при которой отдельные функциональные группы органа или пункта управления могут находиться рассредоточенно (в разных машинах или укрытиях) и перемещаться независимо друг от друга. В этом случае выход из строя одной или нескольких отдельных функциональных групп органа или пункта управления не приведет к потере управления группировкой войск и сил в целом [29] (2008).

использование сертифицированных отечественных базовых информационных защищенных компьютерных технологий (БИЗКТ) — обеспечивает унификацию базовых элементов для построения КСА, беспроблемное наращивание и реконфигурацию стоящих на вооружении средств автоматизации [29] (2008).

4.2.4.8. Разведывательно-поражающая система

разведывательно-поражающая система (РПС) — совокупность сил и средств разведки, поражения и обеспечения видов и родов войск ВС, интегрированных в единый контур управления боевыми средствами (оружием) объединения (соединения), в рамках которого осуществляется их совместное боевое применение с целью поражения группировок войск и объектов противника высокоточным оружием (в перспективе — оружием на новых физических принципах) с требуемой эффективностью.

Отметим, что интеграция сил и средств видов ВС и родов войск в РПС общевойскового объединения может осуществляться как по горизонтали (в одной командной инстанции управления), так и по вертикали (между различными командными инстанциями управления), что обеспечивает при необходимости включение в состав РПС оперативно-стратегического уровня нижестоящих РПС оперативного (оперативных командований) и тактического (бригад и батальонов) звеньев.

Другими словами, РПС следует рассматривать как иерархически сложную, многоуровневую систему, функционально объединяющую на основе автоматизированного управления разнородные силы и средства разведки, поражения и обеспечения в качестве соответствующих элементов и подсистем [45] (2009).

подсистема автоматизированного управления оружием — стержневой интегрирующий компонент разведывательно-поражающей системы, совместимый на каждом уровне руководства (стратегическом, оперативно-стратегическом, оперативном и тактическом) с комплексами средств автоматизации соответствующих органов управления войсками (силами).

Исследования показывают, что подсистема автоматизированного управления разведывательно-поражающей системы (при условии создания единого информационного пространства на стратегическом направлении) вносит решающий вклад в решение задач поражения противника (порядка 43%) по сравнению с подсистемами высокоточного оружия (около 37%) и всестороннего обеспечения (в пределах 20%) [45] (2009).

подсистема разведки разведывательно-поражающей системы объединения (соединения) — штатные и временно подчиненные (на время выполнения боевых задач) силы и средства.

При этом активно используются космические системы видовой, радиотехнической, радиоэлектронной разведки, стратегические и тактические разведывательные самолеты, авиационные комплексы радиолокационного дозора и наведения, беспилотные летательные аппараты, а также широкий спектр наземных систем радиолокационной, радио- и радиотехнической разведки. Подсистема поражения разведывательно-поражающей системы объединения (соединения) также может включать штатные и приданные силы и средства, что позволяет гибко реагировать на изменения оперативной (боевой) обстановки [45] (2009).

средства поражения разведывательно-поражающей системы — в состав таких средств оперативного звена могут входить самолеты бомбардировочной и истребительно-бомбардировочной авиации с управляемым и неуправляемым оружием, вертолеты армейской авиации, силы и средства ПВО, оперативно-тактические и тактические ракетные комплексы с управляемыми ракетами, дальнобойные реактив-

ные системы залпового огня (РСЗО), силы и средства радиоэлектронной борьбы (РЭБ).

В состав средств поражения разведывательно-поражающей системы тактического звена могут входить самолеты штурмовой авиации, вертолеты армейской авиации, тактические ракетные комплексы, РСЗО, артиллерийские комплексы, применяющие высокоточные боеприпасы (ВТБ), силы и средства войсковой ПВО и РЭБ [45] (2009).

4.2.4.9. Автоматизированная система поддержки принятия решений

автоматизированная система поддержки принятия решений (АСППР) — автоматизированная система, позволяющая проводить сбор и анализ исходной информации, осуществлять синтез решений и оценку их влияния на развитие процессов в военной и примыкающих к ней областях [30] (2002).

система поддержки принятия решений (СППР) — человеко-машинная система, обеспечивающая решение слабоструктурированных задач.

В настоящее время в отечественной практике не существует единого подхода к описанию СППР, нет закрепленного стандартами их определения. Западные специалисты к данному виду объектов относят несколько типов программно-технических систем: системы информационной поддержки принятия решения руководителями (Management Information System, MIS) и (Executive Information System, EIS), модель-ориентированные системы (Model-oriented Decision Support Systems, DSS) и системы формирования управленческих решений (Management Decision Systems, MDS) [210] (2012).

требования к автоматизированной системе поддержки принятия решений — при построении такой системы необходимо:

1) Нельзя требовать от нижестоящих организаций как можно больше информации (так сказать, на всякий случай). Запрашиваться должны только действительно необходимые данные. Примером не совсем удачного информационного обмена могут служить некоторые табели срочных донесений, где количество и детальность информации таковы, что полное и корректное заполнение всех позиций затрудни-

тельно. Кроме того, составить их могут только высококвалифицированные и опытные специалисты, которые в условиях существующего кадрового дефицита являются редкостью. В результате табели заполняются некачественно, а при перекрестной их проверке выявляются существенные противоречия, что вынуждает организацию, отвечающую за их обработку и обобщение, повторно запрашивать недостающие данные, а значит, дополнительно тратить время и ресурсы.

2) Информация нижестоящей организации должна быть структурирована таким образом, чтобы при ее передаче в базу данных автоматизированной системы вышестоящей организации исключить процедуры преобразования структуры и форматов, при выполнении которых возможно искажение информации.

3) Общее и специальное программное обеспечение автоматизированной системе поддержки принятия решений нижестоящей и вышестоящей организаций должны быть совместимы. Требование очевидное, но в современных условиях трудно реализуемое из-за существенных различий в техническом оснащении организаций. Быстро провести унификацию технических и программных средств в условиях недостатка ассигнований невозможно, но необходимо хотя бы поэтапное движение в этом направлении, начиная с ключевых звеньев планирования и управления развитием ВВТ.

4) Система обмена данными должна быть нормативно утверждена и находиться под жестким административным контролем в целях полного, своевременного и корректного представления данных (упомянутые табели срочных донесений, вводимые в действие приказом министра обороны, в целом являются важнейшей основой нормативного обеспечения информационного обмена).

5) Система обмена информацией должна быть управляемой, т.е. работать в режиме двустороннего обмена [30] (2002).

интеллектуальная система поддержки принятия решения (ИСППР) — система поддержки принятия решений, имеющая средства работы со знаниями [210] (2012).

система поддержки принятия решений по управлению войсками (силами) и оружием — взаимосвязанный набор компонентов специального программного обеспечения, общесистемного программного обеспечения и информационно-лингвистического обеспечения

постоянной или временной структуры, функционирующих под единым управлением, организованным так, чтобы обеспечить в условиях неполной информации автоматизированный анализ обстановки, прогноз ее развития и разработку предложений по достижению поставленных целей, формулируемых на языке, близком к естественному.

В соответствии с назначением в состав АСУВ могут входить относительно автономные целевые системы поддержки принятия решений, такие как:

информационная — для административного управления войсками (силами) в мирное время;

интеллектуальная — для управления группировками войск (сил) при организации и ведении военных действий [210] (2012).

система поддержки принятия решений при управлении войсками (силами) — человеко-машинная система, которая позволяет лицам, принимающим решения, использовать данные, знания, объективные и субъективные модели для анализа и решения слабоструктурированных проблем.

Системы поддержки принятия решений призваны на основе накопленного опыта применения автоматизированных систем управления обеспечивать потребности в решении задач организационного управления лицам, принимающим решения.

Системы поддержки принятия решений включают процедуры и методы, позволяющие сформулировать поставленную проблему, проанализировать возможности ее решения с помощью баз данных, баз моделей, баз знаний и получить результат.

В рамках информационного подхода системы поддержки принятия решений относят к классу автоматизированных информационных систем, основное назначение которых — улучшить деятельность работников умственного труда (knowledge workers) в организациях путем применения информационной технологии.

Важно при этом подчеркнуть, что они только помогают принимать лучшие решения. Существуют некоторые принципиальные границы — система поддержки принятия решений сама по себе не сможет выдать качественно новый вариант решения. Новые средства могут помочь разобраться в ситуации, но они не заменяют и не смогут заменить творчески мыслящего руководителя [71] (2014).

4.3. Создание автоматизированных систем военного назначения

научно-техническое сопровождение АСУВ — процесс планирования и выполнения заказчиком в тесном взаимодействии с пользователем и разработчиком системы комплекса научных, технических и организационных мероприятий, которые направлены на своевременное обоснование требований к ней, эффективные разработку, испытания, эксплуатацию, выявление направлений совершенствования и модернизации АСУВ [108] (2004).

4.3.1. Противоборство в сфере управления

информация при принятии решения на операцию (бой) — требуется определенное количество информации о войсках (силах) другой стороны, а, следовательно, время на ее добывание, обработку, накопление. Отсюда понятно стремление каждой из противоборствующих сторон обладать ею значительно раньше и в большем, чем у противника, объеме. И это можно считать одним из направлений противоборства в информационной сфере.

Однако при реализации его необходимо учитывать ряд моментов:

1) всякая попытка увеличить имеющийся объем информации может привести к удлинению сроков на организацию и подготовку к боевым действиям и в конечном итоге — к упреждению их начала противником;

2) одновременно с увеличением объема информации возрастает вероятность ее старения.

Значит, нужны дополнительные затраты, в том числе и временные, на ее перепроверку, обновление и повторный анализ. Поэтому от командующего (командира) требуется умение своевременно принимать решение, имея необходимый минимум данных, не позволяя противнику упредить себя в этом [33] (1990).

интеллектуальное противоборство — противоборство разума, идей и решений.

Исключительно важная роль в процессе управления принадлежит интеллектуальному, эмоционально-волевому потенциалу командующих (командиров). Известно, что наиболее ответственным актом управленческой деятельности является принятие решения на операцию

(бой). Неудачное решение неизбежно снижает реализацию возможностей, заложенных в средствах борьбы, и наоборот, оптимальное — предпосылка наиболее полного и эффективного их применения. Причем в стремлении «переиграть» противника интеллектуальное противоборство проявляется двояко: во-первых, в оптимизации своих решений и действий, а во-вторых, в использовании приемов военной хитрости, в обмане противника.

Качество решения на операцию (бой), как уже подчеркивалось выше, во многом определяется уровнем информационного обеспечения, а стало быть, успех интеллектуальной борьбы находится в прямой зависимости от него. Но зависимость эта проявляется только в сочетании с такими факторами, имеющими преимущественное значение, как личностные качества и уровень подготовки командующих (командиров), офицеров штабов. Ибо глубоко ошибочно даже в эпоху высоких научно-технических достижений в области управления войсками (силами) преуменьшать значение субъективного элемента в интеллектуальном противоборстве. Вместе с тем здесь неизбежно возрастает роль объективных факторов, связанных с кардинальными изменениями материальной базы вооруженной борьбы, и прежде всего на направлениях, тесно связанных со сферой управления (компьютеризация, приближение исследовательских работ в области искусственного интеллекта к практическим результатам) [33] (1990).

прогнозирование (предвидение) — решение командующего (командира) устремлено в будущее. Данные, полученные в их результате, лежат в основе любого решения. Не случайно утверждение, что эффективно управлять — значит предвидеть.

Долгое время прогнозирование строилось в основном на интуиции. Со временем на помощь ей пришли методы научного прогнозирования. Познание объективных закономерностей в военном деле, несмотря на множество разного рода случайностей, делает необходимым и возможным научный прогноз на базе количественных методов. Их применение знаменует более высокий этап развития любой, в том числе и военной, науки [33] (1990).

единовластие в военном деле — говоря о достижении интеллектуального превосходства в управлении, следует иметь в виду не только решение командующего (командира), а всю совокупность действий в управляющем звене. В многозвенной системе управления войсками

(силами) единовластие всегда оказывается как бы замаскированным многосубъективным руководством.

Поэтому успех в противоборстве в сфере управления неотделим от постоянной заботы о поддержании высокого интеллектуального потенциала, скрупулезной работы по подбору, расстановке и подготовке управленческих кадров во всех звеньях [33] (1990).

технологическое противоборство — фактор, обеспечивающий достижение интеллектуального и информационного превосходства, ибо успешное управление войсками неразрывно связано с качеством принятых и реализуемых в данной системе методов управления.

Содержание и уровень технологии управления обусловлены многими факторами: организационной структурой, оснащением систем управления, условиями обстановки и др. [33] (1990).

технология совокупного решения в системе (органе) управления — взаимодействие между организационными структурами, участвующими в выработке решения.

Число параметров, определяющих качество решения, достаточно велико. Между ними существуют многочисленные сложные связи. Их можно разделить на две группы. К первой отнесем параметры условий, в которых осуществляется управленческий процесс. Они характеризуются величинами, которые в данной конкретной обстановке не зависят от принимаемого решения. Ко второй — параметры, определяющие то, как намерен действовать командующий (командир). Назовем их параметрами управления. Ясно, что, чем больше параметров управления имеется в руках командира, тем он свободнее в выборе, но тем сложнее ему принять оптимальное решение, и наоборот.

В зависимости от условий обстановки старший начальник волен определять многие параметры управления для себя и подчиненных, чтобы с учетом обстановки и уровня подготовки подчиненных командиров, их личных качеств добиваться принятия эффективного совокупного решения в кратчайшие сроки. Если подчиненному командиру оставляется незначительное количество параметров управления, то этим объективно ускоряется и упрощается его работа, но вместе с тем сокращается свобода выбора, сужается инициатива. Следовательно, оценивая обстановку, условия управления, варьируя указанными параметрами, определяя методы работы, можно активно влиять на функционирование всей системы управления в ходе противоборства с противником.

Требование о сокращении времени на процессы управления объективно входит в противоречие со стремлением принять оптимальное решение. Один из путей решения проблемы — выбор отвечающего условиям метода работы (параллельного или последовательного, либо их сочетания). Вместе с тем нужен настойчивый поиск новых методов в работе и совершенствование уже известных. Например, рост объема и сложность управленческой деятельности вызывают необходимость совершенствования информационной технологии, важными составляющими которой являются использование компьютеров в коммуникационных системах и моделировании [33] (1990).

4.3.2. Свойства АСУВ

эргатическая система — сложная система управления объектами технических, технологических, организационных и экономических комплексов, в которой управляющая система содержит человека-оператора или группу операторов как главный компонент, характеризующийся функциональной активностью в условиях динамически изменяющейся внешней среды.

Поэтому можно сделать вывод, что составные элементы Вооруженных Сил РФ, военно-промышленного комплекса, имеющие в своем составе достаточно большое многообразие социально-технических структур, относятся к эргатическим системам[42] [206] (2007).

устойчивость автоматизированного управления — свойство системы, обеспечивающее своевременную выработку необходимых управляющих воздействий в условиях активного огневого (ударного) и радиоэлектронного противодействия противника.

Использование категории «устойчивость» при анализе этапов жизненного цикла АСУ можно предусматривать уже при проектировании конкретных мероприятий по обеспечению устойчивости автоматизированного управления. Прогнозирование же условий функционирования АСУ позволяет тщательно подготовить к ее эксплуатации органы управления, технические и программные средства, информационные ресурсы АСУ. Характерно, что при этом появляется реальная воз-

[42] В теории и практике военного дела главенствующая роль отводится двум крупным классам эргатических систем. Это системы управления оружием (с доминированием «машинного» фактора) и системы управления войсками (силами), где доминирует «человеческий» фактор. — *Прим. редактора журнала «Военная мысль».*

можность заранее рассчитать силы и средства для нейтрализации возмущающих воздействий. К типичным мероприятиям подобного рода относится обоснование необходимых резервов сил и средств (пунктов управления, каналов связи, технических и программных средств и т.д.) для обеспечения устойчивости автоматизированного управления. Данная категория является обязательной при проведении комплексного анализа эффективности процессов управления войсками и боевыми средствами, а также при планировании и осуществлении практических мероприятий [227] (1990).

количественная мера свойств АСУ войсками в целом — взаимоувязанная совокупность показателей качества, построение которой должно осуществляться с учетом основного предназначения данной системы — качественное обеспечение поддержки принятия решений командиром (начальником) в процессе управления войсками (силами) [64] (2006).

4.3.3. Информационное моделирование

4.3.3.1. Информационное моделирование ВС РФ

информационная модель Вооруженных Сил Российской Федерации — модель, при разработке которой предполагается использование комплекса научных дисциплин, применение широкого спектра научных теорий и методов.

При выработке концептуального подхода к решению проблем информатизации, на наш взгляд, целесообразно избежать междисциплинарного деления и обособления, которые накладывают соответствующие ограничения как на предмет исследования, так и на используемые методы. Кроме того, управление Вооруженными Силами основывается и реализуется исключительно информационными методами как по форме, так и по содержанию. Штабы всех уровней имеют четко выраженную особенность, которая определяется информационным характером их деятельности, и содержат все необходимые атрибуты, свойственные информационным органам. Следовательно, в силу природы управленческих процессов, протекающих в органах управления войсками, основой управления функционированием всей системы являются полнота и качество циркулирующей информации. Поэтому систематизация, классификация и стандартизация информации, а так-

же описание и формализация способов и методов ее обработки будут представлять собой не что иное, как информационное моделирование.

Сформулируем основные представления об информационной модели Вооруженных Сил. С организационной точки зрения ее разработка является крупной научно-технической задачей, а практическая реализация требует значительных капиталовложений. Построение информационной модели Вооруженных Сил исходит прежде всего из необходимости реализации автоматизированной человеко-машинной системы и имеет следующие особенности.

Во-первых, иерархическая организация Вооруженных Сил будет определять соответствующую архитектуру уровней моделирования и отображение их в структуре информационного и программного обеспечения. Следует особо подчеркнуть необходимость обеспечения комплексного, всестороннего охвата всего уровня управления (органа или процесса управления), так как информатизация (автоматизация) на одном из уровней (при сохранении прежних форм и методов обработки документов и данных на соседних уровнях) оказывается малоэффективной и не даст, как правило, никаких результатов, кроме разгрузки машинописных бюро.

Во-вторых, модель должна быть адекватна существующим организационно-штатным структурам своих войск и войск противника (в том числе по личному составу, вооружению и военной технике), сценарий моделирования с которым будет отрабатываться и исследоваться.

В-третьих, необходимо учитывать, что Вооруженные Силы вынуждено будут вступать в войну (боевые действия) в существующих организационно-штатных структурах с табельным вооружением и военной техникой, а также со сложившимися представлениями и образом мышления командующих и командиров всех уровней, основанными на базе руководящих документов по подготовке и ведению операций и закрепленными в процессе боевой и оперативной подготовки. В отображении состава войск и заключается, по нашему мнению, подготовка фактографического содержания банка данных информационной модели.

Наиболее важным вопросом в построении модели и автоматизированной системы управления Вооруженными Силами является необходимость учета ее функционирования в мирное и военное время.

Поскольку все процессы, в том числе и жизнедеятельности Вооруженных Сил, протекают во времени и физическом пространстве,

информация в модели должна быть систематизирована относительно этих понятий (времени и пространства) [21] (1994).

информационная единица — совокупность объектов и их характеристик, отнесенная к единице физического пространства и достаточная для решения всего перечня задач, стоящих перед органом управления.

При этом подразумевается согласование во времени значений характеристик объектов. Согласование во времени определяет также и последовательность решения (выполнения) задач, входящих в указанный перечень. Предлагаемая постановка вопроса о необходимости систематизации информации относительно времени и пространства носит принципиальный характер, так как при таком подходе определяются конкретные параметры, относительно которых может быть осуществлен контроль целостности данных информационной системы с помощью формальных методов [21] (1994).

4.3.3.2. Вербальная модель инфосферы управления войсками (силами)

инфосфера управления войсками (силами) — среда, представляющая собой совокупность определенным образом организованных в пространстве и времени информационных, вычислительных и коммуникационных ресурсов, которые предназначены для обеспечения поддержки принятия решений в ходе управления войсками (силами).

К **вычислительным ресурсам** инфосферы управления войсками (силами) можно отнести средства вычислительной техники, обеспечивающей обработку информации в интересах должностных лиц органов военного управления (ОВУ). В состав вычислительных ресурсов могут входить компьютеры, оперативная память, магнитные и магнитооптические носители (магнитная лента, магнитные диски и дискеты, жесткие диски), устройства отображения (табло для алфавитно-цифровой информации, экраны, самописцы и другие технические (программно-технические) устройства и комплексы).

Коммуникационные ресурсы инфосферы управления войсками (силами) представляют собой совокупность технических (программно-технических) средств, обеспечивающих передачу информации между должностными лицами ОВУ в ходе управления войсками (силами). К

коммуникационным ресурсам в первую очередь можно отнести линии и средства связи, а также пользовательское оборудование.

Очевидно, что основным (базовым) элементом инфосферы управления войсками (силами) являются **информационные ресурсы**, основным содержанием которых является информация, используемая при принятии решений по управлению войсками (силами) [63] (2008).

формализованные информационные ресурсы[1] — ресурсы, которые содержат определенным образом формализованную информацию (знания) о предметной области (в нашем случае это управление войсками (силами)), зафиксированную на так называемых машиночитаемых носителях (т.е. носителях, с которых можно прочитать информацию с использованием средств вычислительной техники) [63] (2008).

формализованные информационные ресурсы[2] — ресурсы, которые содержат определенным образом формализованную (приспособленную для компьютерной обработки) информацию (знания) о предметной области (в нашем случае — это управление войсками (силами)), зафиксированную на материальных носителях.

Важнейшая составная часть формализованных информационных ресурсов — интеллектуальные информационные ресурсы [52] (2014).

неформализованные информационные ресурсы — ресурсы, информация в которых зафиксирована на материальных носителях, не относящихся к машиночитаемым, а также в памяти человека, обладающего знаниями и квалификацией в рассматриваемой предметной области.

На последней части определения есть смысл остановиться более подробно. В качестве носителя информации человек может выступать одновременно как ее создатель, потребитель и интерпретатор. Важно подчеркнуть, что как интерпретатор информации человек (в нашем случае должностное лицо ОВУ) может принципиально изменить отношение к любой информации, включаемой в подготавливаемый документ, не меняя самой информации, что может привести к абсолютно непредсказуемым решениям [63] (2008).

функциональные информационные ресурсы — знания, рациональное использование которых косвенно способствует повышению

качества управленческих решений, например, за счет повышения скорости обмена или наглядности представления информации.

К функциональным информационным ресурсам можно отнести справочные информационные ресурсы, общесистемные программные компоненты, программные компоненты общего назначения и электронные словари.

К группе справочных информационных ресурсов относятся документы, зафиксированные на машиночитаемом носителе, которые используются должностными лицами в их повседневной деятельности. В первую очередь к ним можно отнести классификаторы военной информации, унифицированные формы военных документов, нормативно-справочную информацию, электронные условные знаки, документы в области стандартизации оборонной продукции, словари военных терминов и соответствующих им определений и другие документы.

Программные компоненты общего назначения предназначены для управления средствами коммуникаций, средствами коллективного пользования, обеспечения поддержки сетевых служб системного и пользовательского уровней, протоколов локальных вычислительных и территориально-распределенных сетей, формирования и обработки документов и команд (сигналов).

Состав, структура и степень детализации общесистемных программных компонентов определяется задачами должностных лиц ОВУ и организацией взаимодействия с другими информационными ресурсами, а также требованиями по защите информации от несанкционированного доступа [63] (2008).

интеллектуальные информационные ресурсы[1] — знания, используемые должностными лицами ОВУ при выполнении ими конкретных задач по управлению войсками (силами) с применением средств автоматизации.

Интеллектуальные информационные ресурсы включают в свой состав математические методы, расчетные методики, алгоритмы, математические модели и т.п. (назовем эту группу справочными интеллектуальными информационными ресурсами), а также программную реализацию вышеупомянутых расчетных методик, алгоритмов, математических моделей и т.п. Эта группа информационных ресурсов занимает особое место в инфосфере управления войсками (силами), так как на основе использования именно этого вида информационных ресурсов обеспечивается поддержка информационной, расчетно-анали-

тической, прогнозно-моделирующей деятельности должностных лиц ОВУ, а также выработка решений и планирование боевых действий [63] (2008).

интеллектуальные информационные ресурсы[2] — математические методы, расчетные методики, алгоритмы, математические модели и т.п. (группа справочных интеллектуальных информационных ресурсов), а также программная реализация вышеупомянутых расчетных методик, алгоритмов и математических моделей, взаимоувязанных в структуры любой степени сложности. Эта группа информационных ресурсов занимает особое место в области управления войсками (силами), так как на основе использования именно этого вида информационных ресурсов обеспечивается поддержка информационной, расчетно-аналитической, прогнозно-моделирующей деятельности должностных лиц ОВУ, включая выработку решений и планирование боевых действий.

Предлагается рассматривать следующие свойства формализованных информационных ресурсов: интеллектуальная согласованность, полнота, своевременность, достоверность, конфиденциальность, актуальность, точность [52] (2014).

инструментальные информационные ресурсы — знания, обеспечивающие создание и сопровождение формализованных информационных ресурсов.

Состав инструментальных информационных ресурсов определяется требованиями к характеристикам программных компонентов общего назначения, общесистемных программных компонентов и других программ, зафиксированных на машиночитаемом носителе. В общем случае в состав инструментальных информационных ресурсов могут входить программные компоненты разработки и отладки программ, а также программные компоненты тестирования [63] (2008).

свойства информационного ресурса — если подходить к информационному ресурсу управления вооруженными силами государства как к продукции, то можно выделить такие ее свойства, как функциональность, удобство использования, безопасность, актуальность, трудоемкость, доступность, размерность, надежность, мобильность и сопровождаемость. Есть смысл более подробно остановиться на содержании каждого из перечисленных выше свойств.

Функциональность — возможность выполнения функциональных обязанностей должностным лицом органа военного управления при использовании информационного ресурса.

Удобство использования — способность информационного ресурса при его использовании обеспечить условия для выполнения должностным лицом ОВУ своих функциональных обязанностей.

Безопасность — состояние защищенности информационного ресурса от воздействия различных деструктивных воздействий на информацию, в результате которого может быть нанесен материальный урон (ущерб) личному составу и боевой технике при использовании данного ресурса должностным лицом ОВУ при выполнении своих функциональных обязанностей.

Актуальность — соответствие сведений, зафиксированных на носителе информационного ресурса, решаемым задачам должностного лица ОВУ.

Трудоемкость — диапазон величины трудовых и временных затрат, использованных на создание информационного ресурса.

Доступность — возможность обращения к информационному ресурсу в заданные сроки и на доступном для должностного лица ОВУ языке запросов.

Размерность — диапазон величины объема (размера) информационного ресурса в заданных единицах измерения.

Надежность — способность функционирования информационного ресурса без отказов на заданном интервале времени.

Мобильность — способность информационного ресурса быть перенесенным из одной вычислительной среды в другую.

Сопровождаемость — возможность информационного ресурса к проведению его модификации (корректировки) [63] (2008).

4.3.3.2.1. Свойства формализованных информационных ресурсов

интеллектуальная согласованность — свойство, определяющее результат интеллектуальной деятельности людей по формированию согласованных по целям и средствам их достижения формализованных информационных ресурсов [52] (2014).

полнота — объем содержащихся в информационном ресурсе данных, которые могут быть использованы при принятии решений [52] (2014).

своевременность — свойство, определяющее временные параметры получения информационного ресурса.

Своевременный — такой ресурс, информация в котором может быть учтена при разработке решения без нарушения установленной процедуры, т.е. поступающая на тот или иной уровень управления не позже заранее определенного момента времени, согласованного со временем принятия решений в ОВУ [52] (2014).

достоверность — свойство, определяемое адекватностью отражения объективно существующих явлений, событий и процессов.

Данное свойство характеризуется отсутствием вирусных искажений, а также умышленных искажений и случайных ошибок в информационном ресурсе при его изготовлении и хранении. Следует уточнить, что достоверность следует трактовать с учетом актуальности информационного ресурса, т.е. сохранения с течением времени достаточного соответствия реальному состоянию объектов и явлений на момент использования этого ресурса [52] (2014).

конфиденциальность — свойство, характеризующее состояние информационного ресурса, доступ к которому ограничен в соответствии с законодательством Российской Федерации [52] (2014).

актуальность — свойство, характеризующее допустимые пределы актуальности отраженных в информационном ресурсе процессов и явлений, состояния объектов учета, времени доведения информации от первоисточников до хранилища, а также наличие соответствующей технологии обновления информационного ресурса [52] (2014).

точность — свойство, определяющее степень соответствия представленных в информационном ресурсе значений параметров объекта (процесса) их истинным значениям [52] (2014).

4.3.3.3. Информационная инфраструктура системы управления войсками (силами)

системная модель информационной инфраструктуры системы управления войсками (силами) — набор графических и текстовых представлений, обеспечивающих описание общего представления данной инфраструктуры и взаимосвязи между составляющими ее компонентами.

Системная модель идентифицирует системные возможности и различного вида ресурсы [51] (2010).

функциональная модель информационной инфраструктуры системы управления войсками (силами) — набор описаний (в виде диаграмм) процессов взаимодействия между элементами инфраструктуры по обеспечению необходимыми информационными ресурсами органов военного управления (ОВУ) в ходе решения задач по управлению войсками (силами) [51] (2010).

технологическая модель информационной инфраструктуры системы управления войсками (силами) — взаимосвязанная совокупность артефактов, содержащих сведения о нормативных требованиях к работе, документированию и взаимодействию элементов функциональной архитектуры, а также о требованиях к унификации данных элементов.

Она разрабатывается на основе *функциональной модели*.

Разработка технологической модели позволит оценить возможности использования существующей нормативной базы и необходимость разработки новых нормативных документов по стандартизации в процессе создания данной инфраструктуры [51] (2010).

модель терминологической системы информационной инфраструктуры системы управления войсками (силами) — описание упорядоченной совокупности взаимосвязанных терминов, соответствующих системе понятий рассматриваемой предметной области.

Данная модель может служить терминологической основой формирования исходных данных для разработки электронного словаря, который позволит проводить качественную терминологическую экспертизу всех видов документов, разрабатываемых в процессе создания и эксплуатации информационной инфраструктуры системы управления войсками (силами). Можно выделить три аспекта в проблеме со-

здания модели терминологической системы: синтаксический, семантический и прагматический.

Синтаксический аспект предполагает разработку системы понятий рассматриваемой предметной области, определение совокупности признаков понятий, отношения между понятиями, а также описание объема понятий, представляющие собой комплекс всех объектов предметной области, имеющих все признаки этого понятия.

Семантический аспект учитывает смысловое содержание терминов, принципы построения определений, признаки, отражаемые в определении (чтобы термины были правильно поняты пользователями, в определение целесообразно включать только существенные признаки данного понятия).

Прагматический аспект рассматривает и учитывает ценность, полезность разрабатываемой терминологии, т.е. изучаются потребительские свойства терминов, входящих в состав ее системы. При этом ценность терминологии во многом зависит от качества и способности, готовности потребителя правильно ею воспользоваться. Прагматический аспект непосредственно связан с практическим использованием системы терминов [51] (2010).

информационная модель объекта автоматизации информационной инфраструктуры системы управления войсками (силами) — следующий уровень детализации функциональной модели рассматриваемой инфраструктуры, ее описание осуществляют в виде диаграмм [51] (2010).

модель жизненного цикла информационной инфраструктуры системы управления войсками (силами) — обобщенная совокупность мероприятий и работ по созданию информационной инфраструктуры системы управления войсками (силами) на заданном временном интервале. Модель жизненного цикла является методической основой построения жизненного цикла информационной инфраструктуры системы управления войсками (силами), определенного требованиями нормативных документов по стандартизации с учетом выполнения конкретных ОКР по формированию данной инфраструктуры [51] (2010).

4.3.3.4. Оценка информации

репрезентативность информации — качество информации, связанное с правильностью отбора информации для адекватного отображения свойств объекта, ситуации, состояния.

От репрезентативности данных о признаках варианта действий средств воздушного нападения зависит правильность вскрытия этого варианта и, как следствие, правильность выбора варианта действий своих войск (сил) [159] (2006).

своевременность информации — качество информации, связанное с поступлением ее не позже заранее назначенного момента времени, согласованного с временем решения поставленной задачи.

Например, информация для принятия решения о подъеме в воздух истребителей ПВО должна поступить в орган управления своевременно («не позже», но и «не раньше»), так как, если истребители будут подняты раньше, они израсходуют свой запас горючего к моменту начала воздушного боя, а если позже, то могут не успеть встретить противника на заданном рубеже [159] (2006).

избирательность информации — способность информационной системы выбирать из массивов данных именно ту информацию, которая актуальна в данный момент времени.

Временна́я избирательность выражает привязку к оси времени, на которой обозначаются характерные по своему содержанию периоды развития обстановки и соответствующие этапы деятельности органов управления ПВО.

Действия средств воздушного нападения в пределах зоны границ ответственности противовоздушной обороны могут иметь различную интенсивность и отличаться по своему характеру на различных направлениях, в районах, участках, что потребует представления информации, отображающей особенности складывающейся обстановки. В связи с этим возникает необходимость **пространственной избирательности**.

С началом боевых действий задача органов управления ПВО заключается в том, чтобы своевременно вскрыть вариант действий противника и ввести в действие вариант действий своих войск. При этом вариант действий противника выявляется по характерным признакам, на определении которых сосредоточивается внимание. Чем точнее будут установлены такие признаки и сопоставлены с признаками ранее

разработанных вариантов, тем обоснованнее будет решение на ввод в действие соответствующего варианта ответных действий. В этой связи можно вести речь о **признаковой** и **ситуационной избирательности**, которые неизбежно должны быть связаны с временной и пространственной избирательностью.

Реальные действия противника в воздушном (воздушно-космическом) пространстве могут и не иметь достаточно полных совпадений с заранее проработанными вариантами, поэтому возникает потребность альтернативного выбора наиболее близких по содержанию вариантов (**альтернативная избирательность**).

Наконец, как и в любых военных действиях, необходимо предвидение дальнейшего развития обстановки, для чего в базе данных закладывается информация прогнозного характера. Это предполагает наличие **прогностической избирательности** [159] (2006).

мера информации — определенные затруднения вызывает и выбор наиболее подходящей для оценки достаточности информации в системах управления ПВО меры информации.

Существует мнение, поддерживаемое некоторыми специалистами в области информационных подходов к решению прикладных задач ПВО, о том, что наиболее универсальной мерой информации следует считать синтаксическую меру.

Предпочтение здесь, безусловно, должно быть отдано семантической и прагматической мерам информации [159] (2006).

синтаксическая мера информации — энтропия системы как мера недостающей информации.

Однако синтаксическая адекватность уже по определению отображает формально структурные характеристики информации и не затрагивает ее смыслового содержания, т.е. синтаксическая мера количества информации оперирует с обезличенной информацией [159] (2006).

тезаурусная мера информации — мера информации на семантическом уровне, которая связывает семантические свойства информации со способностью пользователя принимать поступившее сообщение.

Одно и то же сообщение может иметь смысловое содержание для компетентного пользователя и быть бессмысленным (семантический шум) для пользователя некомпетентного. Для систем управления ПВО принципиально важно наполнение базы данных с учетом особенностей

разнообразных динамично изменяющихся ситуаций. Необходимо добиваться, чтобы коэффициент содержательности, который определяется как отношение количества семантической информации к ее объему, приближался к единице [159] (2006).

прагматическая мера информации — полезность (ценность) информации для достижения пользователем поставленной цели.

Ценность информации измеряется, как правило, в тех же самых единицах (или близких к ним), что и целевая функция [159] (2006).

4.3.4. Математическое обеспечение

математическое обеспечение АСУВ — совокупность математических методов, моделей и алгоритмов для решения задач и обработки информации с применением вычислительной техники в автоматизированных системах управления [102] (1998).

специальное математическое обеспечение[1] (СМО) — совокупность описаний и алгоритмов информационных и расчетных задач, математических моделей операций (боевых действий), необходимых в процессе управления войсками (силами) [102] (1998).

специальное математическое обеспечение[2] — взаимодействующая совокупность алгоритмов, моделей и задач, которые могут использоваться в качестве функциональных требований и исходных данных при программной реализации информационных технологий поддержки управленческих решений [55] (2005).

специальное математическое и программное обеспечение[1] (СМПО) — вся совокупность методов, алгоритмов, программ, применяемых для решения управленческих задач с помощью компьютерной техники.

Использование компьютеров, снабженных соответствующими средствами СМПО, не только повышает качественную сторону процесса управления, но и вносит немало нового в работу управленческих органов. Ныне предпринимаются попытки внедрения принципиально новых средств СМПО на основе теории искусственного интеллекта с

использованием ЭВМ пятого поколения. Например, программно-информационные комплексы для выработки и оценки возможных вариантов действий определенных, потребных для выполнения задач сил и средств, их оптимальное распределение с учетом обстановки и др.

В зависимости от условий применяются те или иные средства СМПО, в том числе универсальные и специализированные (нацеленные на определенное звено управления, вид боевых действий) общевойсковые модели операции (боя), которые способствуют выработке оптимального решения в сроки, позволяющие опережать противника. Однако опыт показывает, что мало иметь добротные модели и средства их реализации. Важно, чтобы все должностные лица по роду своей деятельности мастерски владели ими [33] (1990).

специальное математическое и программное обеспечение[2] (СМПО) — обеспечение автоматизированной системы управления войсками (силами), в котором разрабатываются математические модели операций (боевых действий) и информационно-расчетные задачи, содержащие количественные методы анализа оптимальных (рациональных) вариантов применения оружия[43] [174] (2014).

специальное математическое и программное обеспечение АСУВ (СМПО АСУВ) — совокупность математических методов, моделей, алгоритмов и программ, разрабатываемых и применяемых для обеспечения непосредственного выполнения должностными лицами органов (пунктов) управления специфических функций по управлению войсками (силами) [59, 60] (2002).

---

[43] С позиции современных системологии и программной инженерии обращение к категории СМПО кажется анахронизмом. Например, в ГОСТ РВ 1210—003—2007 требования к математическому и программному обеспечению формулируются как к самостоятельным структурным элементам АСУВ (что совершенно правильно). Однако в конкретно-исторических условиях середины прошлого века, когда теория и практика автоматизации программирования делала только первые шаги, именно такой подход (информационно-расчетные задачи и модели СМПО) специалистов 27 ЦНИИ МО (ВЦ №1), позволяющий напрямую внедрять компьютерные технологии в практику работы органов военного управления, в значительной мере обеспечил успех решения актуальнейшей государственной задачи стратегического паритета с вероятным противником. — *Прим. редактора журнала «Военная мысль».*

4.3.4.1. Математическое моделирование

моделирование в военном деле[1] — расчеты с применением компьютерной техники, используемые при принятии решений, планировании боевых действий.

Своевременно полученные данные расчетов, компьютерного моделирования придают замыслу, построенному на интуиции, практическую основу с внесением в него необходимых коррективов [33] (1990).

моделирование в военном деле[2] — метод исследования объектов военно-научного познания с помощью моделей функционирования этих объектов.

Различают как **аналитически агрегированные модели**, описывающие изменения исследуемых показателей для оценок, позволяющих видеть допустимые границы возможностей систем или процессов, а также тенденции их развития, так и **имитационные модели**, которые связаны не с аналитическими представлениями, а с принципом имитации с помощью информационных и программных средств, процессов и систем в самом сложном аспекте — динамическом [32] (2015).

операция войск (сил) как объект моделирования — базируется на рассмотрении происходящего во времени и пространстве противоборства двух сложных иерархических систем.

Операция не относится к аддитивным процессам, т.е. ее нельзя свести к простой сумме множества составляющих ее боевых действий. Совокупное действие, порождаемое взаимодействием всех элементов противоборствующих группировок войск, обусловливает новое качество, выражающееся в текущих интегральных показателях состояния и боевых возможностей войск (сил) сторон в операции. Очевидно, что математическая модель должна учитывать эту важнейшую черту моделируемого процесса.

Военной операции присуще и такое системное свойство, как бесконечность, под которым понимается невозможность ее полного познания и всестороннего представления конечным множеством описаний. Вооруженная борьба отличается бесчисленным разнообразием сторон. Описание каждой из них с различной степенью подробности будет по-своему отражать структуру и механизм противоборства. Поэтому чрезвычайно важен выбор рационального содержательного и формального представления его в модели.

Операции, как сложному социальному явлению, присущи и другие системные свойства — способность к саморазвитию, многообразие, управляемость, самоорганизация, адаптация к изменениям условий деятельности, стремление к сохранению сторонами качественной определенности (боеспособности войск). Они реализуются через механизмы управления группировками войск.

По отношению к внешней среде операция является открытой системой, т.е. она связана с внешним миром, зависит от него и, в свою очередь, влияет на него. Однако при анализе и особенно при моделировании операцию удобнее рассматривать как изолированную или закрытую систему, характеризующуюся борьбой двух подсистем (систем более низкого уровня) с заранее заданными ресурсами [219] (1997).

информационные технологии принятия решения на операцию — совокупность информационных технологий, применяемых командующим и штабом на отдельных этапах принятия решения с использованием соответствующих средств автоматизации [157] (1999).

информационно-моделирующая среда (ИМС) — совокупность моделирующей системы и решаемых на ее основе информационно-расчетных задач, связанных с одной базой данных и обеспечивающих формирование военной обстановки любого масштаба, проведение расчетов, разработку способов действий для всех сил и средств вооруженной борьбы и моделирование военных и других действий во всех их проявлениях [139] (2011).

информационно-моделирующая среда ВС РФ (ИМС ВС РФ) — система моделей объектов и процессов в сфере вооруженной борьбы, строительства Вооруженных Сил и военной экономики, включая средства разработки и интеграции моделей, предназначенная для информационно-расчетного обеспечения управления развитием системы вооружения, строительством, подготовкой и применением Вооруженных Сил Российской Федерации [32] (2015).

моделирующая система — ядро (программная основа) информационно-моделирующей среды, представляющее собой совокупность имитационных и аналитических моделей сил (средств) и среды вооруженной борьбы.

Основными из них являются модели: вооружения и военной техники, воинских формирований, систем управления и связи, геоинфор-

мационной системы (физико-географических условий) и инфраструктуры, способов военных действий, отображения обстановки. Моделирующая система позволяет создавать и отображать на средствах индивидуального и коллективного пользования в двух- и трехмерном (на тактическом уровне) виде адекватные модели любых условий боевых действий, любого состава и размещения сил и средств вооруженной борьбы. Для них возможно формирование любых способов действий в любых формах и получение на основе моделирования по выбранным показателям результатов действий, близких к ожидаемым реальным [139] (2011).

система моделирования — перечень моделей, соответствующих баз знаний об объекте моделирования и порядок их практического применения для решения задач военно-научных исследований [32] (2015).

расчетно-моделирующие комплексы (РМК) — системы штабных математических моделей операций (боевых действий), информационных и расчетных задач, логически и информационно увязанных между собой по предназначению, оперативным постановкам, входным и выходным данным и другим параметрам и позволяющих прогнозировать ход и исход операции при заданных группировках и вариантах решений сторон [157] (1999).

информационно-расчетные задачи (ИРЗ) — комплексы организации планирования, оценки обстановки, разработки способов действий противника и своих войск (сил), автоматизированной разработки вопросов управления, всех видов обеспечения и управления.

Информационно-расчетные задачи информационно-моделирующей среды в отличие от ИРЗ существующих КСА не автономны, а связаны с моделирующей системой, что позволяет получить два существенных преимущества.

Первое преимущество: большая часть исходных данных для ИРЗ, описывающих условия обстановки, автоматически формируется моделирующей системой в ходе моделирования развития обстановки. Это позволяет, например, автоматически формировать маршруты полета авиации к объектам удара с учетом ожидаемой динамики изменения в ходе операции радиолокационного поля и зон зенитного ракетного огня противника.

Второе преимущество: часть полученных при решении ИРЗ данных автоматически используется в моделирующей системе при моделировании. Например, после решения задач по формированию порядка огневого поражения противника ракетными войсками и артиллерией, авиацией и силами флота можно сразу запускать моделирование для определения его ожидаемых результатов [139] (2011).

система моделей — совокупность взаимно связанных математических моделей для описания сложных систем, которые невозможно воспроизвести в одной модели.

Для планирования и прогнозирования поведения крупных объектов разрабатываются системы моделей, построенные обычно по иерархическому принципу, в несколько уровней. Они называются многоуровневыми системами [48] (2009).

комплекс моделей — совокупность моделей, предназначенных для решения одной сложной задачи, каждая из которых описывает ту или иную сторону моделируемого объекта или процесса.

Если же модели связаны так, что результаты одних оказываются исходными данными для других до получения общего результата, то комплекс обращается в систему моделей [48] (2009).

математическая модель операции (боевых действий) — программно реализованная система математических зависимостей и логических правил, позволяющая с достаточной полнотой и точностью воспроизводить во времени наиболее существенные составляющие моделируемых процессов и рассчитывать на основе этого численные значения показателей прогнозируемого хода и исхода процессов [59] (2002).

математическая модель боевых действий — система математических зависимостей и логических правил, позволяющая описать процессы, присущие операции (бою), и с заданной степенью точности определить искомые выходные данные по известным входным данным [32] (2015).

модель фронтовой операции (МФО) — модель первой версии (середина 80-х годов XX века) имела уникальные характеристики: время моделирования фронтовой операции не превышало 20—30 минут; подготовка оперативной информации осуществлялась в нормативные сроки работы штабов, обеспечивала выработку замысла опера-

ции, наглядно демонстрировала преимущества средств автоматизации при решении поставленных задач.

В 90-е годы математический аппарат моделирования боевых действий был усовершенствован с учетом произошедших изменений в содержании и характере вооруженной борьбы. Эта математическая модель была верифицирована по данным операций Великой Отечественной войны и послевоенных военных конфликтов, апробирована на мероприятиях оперативной подготовки ВС РФ, внедрена в учебный процесс ВАГШ ВС РФ и ОВА ВС РФ. Она на многие годы (вплоть до настоящего времени) стала основным инструментом поддержки принимаемых органами военного управления (ОВУ) решений на боевое применение группировок войск (сил) общего назначения.

К концу 90-х годов была разработана новая версия МФО, в которой обеспечивались сведение вариантов решений противоборствующих сторон, обмен данными по боевому и численному составу войск (сил) с внешней специализированной базой данных, разработанной в 27 ЦНИИ МО РФ, визуализация пространственной динамики изменения линии боевого соприкосновения сторон на электронной карте путем переноса на нее выходных результатов моделирования. В модели также воспроизводились ситуации, связанные с обходом и окружением противостоящих войск. Все это расширило возможности ее применения на мероприятиях оперативной подготовки в качестве инструмента объективной оценки штабом руководства решений обучаемых органов управления.

В период с 2000 по 2014 год МФО непрерывно совершенствовалась в части более полного и всестороннего учета межвидового характера современных операций (боевых действий) и возможностей новых средств вооруженной борьбы. В существующей версии математической модели реализована методология моделирования глубокого бесконтактного дистанционного воздействия разнородными средствами поражения на группировки и объекты противника с применением геоинформационных систем для учета характеристик театра военных действий.

В модели определяются критические уровни боеспособности соединений 1-го эшелона по заданным критериям, осуществляется сравнительная оценка боеспособности формирований по различным вариантам действий войск с учетом возможностей восстановления вооружения и техники, реализовано представление результатов моделирова-

ния в графическом и табличном виде с возможностью их пошагового сравнения за прогнозируемый период [47] (2014).

алгоритмическая модель — сложная алгоритмически заданная функция многих переменных, где различные логические процедуры и условия сочетаются с традиционными формами математического описания.

Причем определенным наборам значений переменных соответствует свой вид функций, описывающих протекающие в операции процессы. Такая неопределенность и неоднозначность свойств моделей порождает ряд теоретических и практических проблем, касающихся, например, оптимизации управления войсками (силами). Отсюда наиболее рациональным явилось сочетание логических методов выбора значений управляющих параметров и частичной математической оптимизации. В процессе моделирования допускается прямое вмешательство лиц, принимающих решения, для корректировки выработанных моделью управляющих воздействий и даже их формирования. Модели этого класса, несмотря на указанный недостаток, могут с требуемой полнотой отражать все стороны моделируемого процесса. Они подтвердили на практике свою эффективность [219] (1997).

расчетная единица (РЕ) — наименьший элемент в информационных структурах противостоящих группировок войск (сил), внутреннее строение которого не рассматривается на принятом уровне описания операции.

Так, на стратегическом уровне в качестве РЕ принимается дивизия, а на оперативно-тактическом — батальон или рота. Наиболее важную часть информации, необходимой для моделирования, составляют характеристики РЕ.

Выбор РЕ диктуется требованиями к выходным результатам, объемам исходной информации и оперативности моделирования, зависит от возможности получения той или иной исходной информации и должен быть обоснован с позиций корректного отображения содержательного описания операции. Проблема выбора РЕ решается эвристически на основе анализа моделируемых процессов и задач, возлагаемых на модель.

Для получения характеристик РЕ модели стратегического уровня дополняются моделями тактического и оперативно-тактического уровня, каждая из которых отражает ту или иную сторону вооруженной борьбы с необходимой степенью подробности. Наличие такого комп-

лекса моделей позволяет построить достаточно надежную схему определения характеристик РЕ для агрегированных моделей вооруженной борьбы [219] (1997).

единичная операция (ЕО) — применительно к воздушной операции на ТВД — ракетно-артиллерийский удар, массированный авиационный удар, систематические боевые действия авиации на операционном направлении [156] (1999).

количественные результаты моделируемых и реальных боевых действий (операции) — величины показателей эффективности вариантов ведения боевых действий (операции).

Это математическое ожидание (оценка математического ожидания) величины ущерба, наносимого противнику, математическое ожидание (оценка математического ожидания) потерь своих войск (сил). Каждый из этих показателей напрямую зависит от эффективности случайных элементарных событий, связанных с обнаружением (разведкой), поражением воздушных целей, наземных объектов воюющих сторон и с другими вероятностными событиями [86] (2005).

4.3.4.2. Принципы моделирования операций (боевых действий)

принцип цели — операция как сложный системный объект должна рассматриваться только с точки зрения задач, решаемых исследователем или лицом, принимающим решение. Это означает целенаправленность описания операции. Цель определяет его содержание и форму, а также уровень обобщения (агрегирования). Последний фиксируется выбором элементов структурного описания операции, целостные свойства которых определяют границу его подробности [219] (1997).

принцип многоуровневого описания — означает, что операция, выступающая в качестве объекта исследования и моделирования, должна быть представлена, во-первых, как элемент более широкой системы, во-вторых, как целостное явление, в-третьих, как сложная структура, подробность строения которой определяется поставленными целями исследования. Число уровней описания может быть и больше, но не меньше трех упомянутых [219] (1997).

принцип информационного единства — каждое понятие в языке вышестоящего уровня есть результат обобщения понятий нижнего уровня. Принятые в модели критерии эффективности на разных уровнях управления группировками тоже должны быть согласованы в соответствии с данным принципом [219] (1997).

принцип классификации — для построения модели операции необходимо классифицировать процессы вооруженной борьбы в соответствии с принятыми уровнями описания операции. Перечисленные принципы позволяют решать наиболее сложную проблему моделирования операций — создание системы информационного обеспечения модели [219] (1997).

принцип соответствия сложности преобразования информации человеком его психофизиологическим возможностям — предполагает декомпозицию многомерной задачи управления на систему частных задач управления сравнительно невысокой размерности. По своему содержанию эта декомпозиция относится к системному анализу, направленному на выявление наиболее существенных закономерностей подготавливаемой операции как устойчивых каузальных связей между отдельными элементами обстановки, принимаемого решения и возможными результатами боевых действий [157] (1999).

принцип последовательного разрешения неопределенности[1] — процесс принятия решения — движение от обобщенного представления о целях, характере деятельности, об условиях функционирования, развития и показателях рационального поведения управляемой организации к детальному представлению задач, механизмов функционирования, условий и критериев деятельности ее структурных элементов [219] (1997).

принцип последовательного разрешения неопределенности[2] — в соответствии с ним элементы решения определяются последовательно от общих к частным [157] (1999).

каузальный принцип обоснования принимаемых решений — отражает механизм системного синтеза решений, построенный на основе альтернативного способа выбора. При этом предпочтения лица, принимающего решение, определяемые на множестве возможных исходов боевых действий, фактически переносятся на множество соот-

ветствующих им альтернативных значений элементов принимаемого решения [157] (1999).

принцип лингвистического детерминизма — предполагает использование в процессе декомпозиции нормативно закрепленной системы категорий и понятий с фиксированным смыслом и выражает требование глобальной согласованности частных задач, обеспечивающее их однозначное понимание и интерпретацию [157] (1999).

принцип единства и совместного действия закономерностей операции — принцип, распространяющий закономерности составных частей на операцию в целом.

В соответствии с ним модель системных закономерностей операции образуется в процессе последовательного построения иерархически вложенной системы моделей закономерностей частных операций и их координации (взаимного согласования) по цели, месту, времени, привлекаемым силам, средствам и др. Отсюда модель системных закономерностей операции представляет собой своего рода набор матрешек, начинающийся с наименьшей — модели структурно неделимой «единичной» операции и заканчивающийся моделью подготавливаемой операции в целом [156] (1999).

принцип единства и совместного действия закономерностей операции (боевых действий) — требует выявления достаточно полной системы закономерностей, обладающей свойством монотонности, для надежного прогнозирования возможных последствий принимаемых решений. Причем независимо от способов построения такая система закономерностей должна быть открытой (наращиваемой) [156] (1999).

принцип робастности — отражает особенность построения моделей закономерностей и предполагает использование в качестве его основы аппарата теории нечетких множеств. В соответствии с ней модель закономерности боевых действий можно определить как нечеткое отношение на заданных нечетких множествах, используемых для качественного описания элементов обстановки, принимаемого решения и возможных результатов боевых действий, с функцией принадлежности, характеризующей степень тесноты каузальных связей между ними. Данному нечеткому отношению отвечает робастная модель, раскрывающая механизм действия соответствующей закономерности при дос-

таточно высоком уровне значимости каузальных связей. Для качественного описания переменных робастной модели (элементов обстановки, принимаемого решения и возможных результатов боевых действий) используются лингвистические переменные [156] (1999).

принцип системного подхода к построению моделей системных закономерностей операции — принцип, в соответствии с которым формируется информационная модель замысла операции как результат оптимизации значений системных показателей [156] (1999).

принцип структурного полиморфизма — обеспечивает возможность совместного анализа (по совокупности системных показателей) альтернативных вариантов проведения операции в целях выбора наиболее рационального [156] (1999).

принцип транзитивной оптимальности — координация альтернативных вариантов действий войск (сил), осуществляемая для каждого варианта и на каждом уровне, вплоть до наивысшего, соответствующего операции в целом.

Выбор рационального варианта проведения операции осуществляется с использованием специальных методов многокритериальной оптимизации. Причем этот выбор одновременно определяет цепочку соответствующих ему иерархически вложенных вариантов, раскрывающих его содержание [156] (1999).

системные закономерности операции — закономерности развития (поведения) операции как системы частных операций [156] (1999).

модель системных закономерностей операции — качественная зависимость хода и исхода операции от системных показателей — важнейших характеристик внутренней организации (структуры) и наиболее существенных системообразующих связей между частными операциями [156] (1999).

4.3.4.3. Классификация математических моделей

классификация математических моделей — несмотря на множественность взглядов на способы моделирования, математические модели все же имеют некоторые сходные черты, которые позволяют

объединять их в отдельные классы. Существующая классификация математических моделей боевых действий (операций) объединения ВВС учитывает следующие признаки: целевую направленность; способ описания функциональных связей; характер зависимостей в целевой функции и ограничениях; фактор времени; способ учета случайных факторов.

В зависимости от целевой направленности математические модели боевых действий (операций) принято подразделять на «оценочные» и «оптимизационные».

Учитывая потребность командующих и штабов объединений ВВС в эффективном обеспечении поиска рациональных вариантов ведения боевых действий (операций), необходимо ввести новую классификацию оптимизационных моделей боевых действий (операций) объединения ВВС, которая предусматривает разделение моделей на комбинированные и субоптимизационные. Это может помочь пользователям значительно расширить представление об особенностях построения и функционирования моделей, предназначенных для поиска рациональных способов ведения боевых действий (операций).

Предлагаемый подход к построению математических моделей боевых действий (операций) объединения ВВС, предусматривающий применение метода детального воспроизведения иерархической сущности принятия решений на боевые действия (операцию), позволил ввести еще один признак классификации математических моделей по иерархической структуре. Согласно этому признаку математические модели могут классифицироваться на одноуровневые и многоуровневые.

В существующей классификации математических моделей боевых действий (операций) важное место занимает классификация по способу описания функциональных связей между параметрами (процессов функционирования элементов системы). В соответствии с этим признаком математические модели подразделяются на аналитические и имитационные.

В зависимости от учета фактора времени модели боевых действий (операций) подразделяются на статические, динамические, непрерывные и дискретные.

На развитие и исход боевых действий (операций) объединения ВВС влияет большое число факторов, имеющих в основном вероятностную природу. В зависимости от способа учета случайных факторов математические модели боевых действий (операций) принято

классифицировать на детерминированные, стохастические (вероятностные) и комбинированные.

С точки зрения учета нестохастических неопределенностей математические модели можно классифицировать на модели, построенные на методах теории игр, и ситуационные (военные игры). Их принципиальное отличие состоит в одном важном ограничении, а именно — предположении в моделях теории игр полной («идеальной») разумности противника. Расчет на разумного противника — лишь одна из возможных позиций в конфликте, но в теории игр именно она кладется в основу. В реальном конфликте зачастую выбор рационального способа применения войск (сил) состоит в том, чтобы угадать слабые стороны противника и своевременно воспользоваться ими.

Важной особенностью игровых и ситуационных моделей является стремление глубоко рассмотреть все возможные виды действий и противодействий, выявить и изучить возможные варианты применения войск (сил) под воздействием противника.

В зависимости от количества сторон, участвующих в моделировании боевых действий (операций), нестохастические модели можно подразделить на двусторонние («парные») и многосторонние («множественные»), сочетаний и типов которых существует множество, включая модели, связанные с участием большого количества игроков и многих посредников. Участниками «множественных» моделей могут быть не только непосредственные противники, но и представители войск (сил), взаимодействующих с объединением ВВС, посредники и т.д. В качестве посредников могут выступать независимые военные эксперты, имеющие возможность вмешиваться в необходимых случаях в ход моделирования боевых действий (операций).

С точки зрения учета стохастической (вероятностной) неопределенности математические модели боевых действий (операций) можно подразделить на вероятностные и статистические. Мотивацией такой классификации является различие задач математической статистики и теории вероятностей [85] (2004).

оценочные (описательные) модели — модели, в которых элементы замысла (решения, плана, варианта) предполагаемых действий сторон являются заданными, то есть входят в состав исходной информации.

Итогом моделирования являются расчетные результаты действий сторон в боевых действиях (операциях). Такие модели чаще всего

называют моделями оценки эффективности боевых действий (операций). Для них выработка рациональных способов применения сил и средств не является основной задачей [85] (2004).

оптимизационные (оптимизирующие, нормативные) модели — модели, цель которых состоит в определении оптимальных способов ведения боевых действий (операций).

Основу этих моделей составляют математические методы оптимизации. По сравнению с оценочными моделями оптимизационные представляют наибольший интерес для планирования боевых действий (операций), поскольку они позволяют не только провести количественную оценку эффективности вариантов ведения боевых действий (операций), но и осуществлять поиск наиболее эффективных вариантов для конкретной обстановки [85] (2004).

методы оптимизации — аналитические методы (метод Лагранжа, уравнения Ланчестера), итерационные (методы линейного, нелинейного, динамического программирования), неитерационные (методы случайного поиска, многофакторного анализа), а также методы последовательной оптимизации (ситуационный метод, методы покоординатного поиска и наискорейшего спуска) [85] (2004).

метод субоптимизации — предложенный новый метод построения моделей, обеспечивающий комплексную оптимизацию действий войск (сил) в каждом эпизоде моделируемых боевых действий (операций).

Он предусматривает поиск рациональных способов ведения боевых действий (операций) «сверху вниз» — последовательно на каждом из уровней управления, но в рамках общего замысла боевых действий (операций). Неоспоримым достоинством субоптимизации является то, что на каждом уровне управления более детально выявляются факторы и условия боевых действий соединений и частей и выбираются наиболее разумные способы их действий [85] (2004).

одноуровневые модели — модели прямого воспроизведения воздушных и противовоздушных боев.

Но поскольку в рамках тактического уровня («на поле» тактического уровня) решаются задачи и оперативного уровня, математическая модель становится громоздкой и неудобной для практического использования. Применение таких моделей сопряжено, во-первых, с

необходимостью подготовки большого объема исходных данных, во-вторых, со снижением оперативности непосредственного моделирования боевых действий (операций) и, в-третьих, со сложностью восприятия полученных результатов моделирования [85] (2004).

многоуровневые математические модели боевых действий (операций) — целостная система функционально взаимосвязанных подмоделей (агрегатов) различного уровня, которые взаимосвязаны не только горизонтальными отношениями между собой, но и отношениями подчиненности.

Композиционный подход в многоуровневых моделях можно рассматривать как один из перспективных путей их совершенствования с сохранением требуемой степени детализации моделирования боевых действий (операций). Система подмоделей различного уровня управления создает благоприятные условия для моделирования боевых действий (операций) при параллельном или комбинированном методах планирования боевых действий. Оперативность планирования повышается в основном за счет подмоделей тактического уровня. Подготовка исходных данных, моделирование и трактовка его результатов на подмоделях тактического звена осуществляются параллельно соответствующими командирами и их штабами [85] (2004).

аналитические модели — модели, в которых процессы функционирования элементов системы описываются в виде некоторых функциональных соотношений или логических условий.

Наиболее полно исследование процесса можно провести, если известны явные зависимости, связывающие выходные характеристики с начальными условиями и входными переменными системы. Однако такие зависимости удается получить только для сравнительно простых моделей или при весьма жестких ограничениях, накладываемых на условия моделирования, что является неприемлемым для моделирования боевых действий (операций) объединения ВВС.

Аналитические модели в зависимости от вида применяемых в них аналитических зависимостей (целевая функция и ограничения) принято классифицировать на линейные и нелинейные. Если целевая функция и ограничения линейные, то модель называют **линейной**. В противном случае — модель **нелинейная**. Например, модели, в основе которых лежит метод линейного программирования, являются линейными, а в моделях, построенных на основе методов максимального

элемента или динамического программирования, целевая функция и (или) ограничения нелинейны [85] (2004).

имитационные модели — модели, в которых имитируются (копируются) элементарные явления (бои, авиационные удары, специальные боевые полеты), составляющие основное содержание боевых действий (операций) с сохранением их логической структуры и последовательности протекания (во времени), что позволяет в определенные моменты времени оценить их характеристики.

Имитационные модели позволяют достаточно просто учитывать такие факторы, как наличие дискретных и непрерывных элементов, нелинейные характеристики элементов системы, многочисленные случайные воздействия и др. В настоящее время имитационное моделирование — наиболее эффективный и часто единственно доступный метод исследования таких сложных систем, как боевые действия (операции) объединения ВВС [85] (2004).

статические модели — модели, служащие для описания боевых действий (операций) в какой-либо момент времени.

Они отражают определенный «временной срез» боевых действий (операций). Поэтому статические модели применяются для исследования наиболее важных этапов боевых действий (операций). Как правило, это начальный этап, от исхода которого в значительной степени зависят дальнейший ход событий и конечный результат операции [85] (2004).

динамические модели — модели, описывающие боевые действия (операцию) в развитии.

Это позволяет выявлять тенденции развития боевых действий (операций), факторы и взаимосвязи, которые, на первый взгляд, не оказывают существенного влияния на моделируемый процесс, но могут стать важным предметом рассмотрения. Тенденция развития динамических моделей боевых действий (операций) явно направлена на усиление их роли в исследовании способов применения войск (сил) сторон. Благодаря способности отражать преемственность между отдельными эпизодами боевых действий (операций) динамические модели нашли достойное применение для решения задач долгосрочного планирования и прогнозирования применения войск (сил) [85] (2004).

непрерывные модели — математические модели боевых действий (операций) с непрерывным временем моделирования, характеризующиеся тем, что их переменные и выходные параметры изменяются непрерывно, без скачков и последовательно принимают все возможные вещественные значения на всем временном интервале.

В непрерывных моделях для нахождения промежуточных значений используют интерполяцию. Так как она предусматривает нахождение промежуточных значений функции, то в основе модели должен лежать аналитический метод, обеспечивающий функциональную зависимость исходных и конечных величин. Аналитические методы наименее подходят для описания всей совокупности факторов боевых действий (операций) объединения ВВС, поэтому непрерывные модели не нашли широкого применения для поиска способов применения войск (сил) [85] (2004).

дискретные модели — модели, необязательно имеющие аналитическую зависимость между входными и выходными величинами, а использующие имитационный метод моделирования.

В дискретных моделях все процессы (входные и внутренние) отличаются скачкообразной, резко выраженной сменой конечного числа состояний: входных, выходных и внутренних. Продвигаясь в дискретной модели боевых действий (операций) последовательно от эпизода к эпизоду с заданным временным шагом моделирования, командующий и его штаб получают комплексное, системное представление о процессах, происходящих в ходе боевых действий (операций). Величина шага моделирования варьируется и может выбираться исходя из требуемой глубины моделирования отдельных эпизодов. Если необходимо глубже изучить тот или иной момент операции, величина шага уменьшается [85] (2004).

детерминированные модели — модели боевых действий (операций), в которых для данной совокупности входных значений модели всегда получается единственный результат.

Каждый выбранный командующим объединения ВВС способ применения войск (сил) приводит к строго определенным последствиям, поскольку в ходе моделирования пренебрегают случайными, заранее непредвиденными воздействиями.

Детерминированные модели можно рассматривать как сознательное упрощение реальной действительности, носящей на самом деле неопределенный характер. До того времени, когда в штабах стали

применять мощные вычислительные средства, детерминированные модели были основным инструментом оценки эффективности боевых действий (операций). Вся стохастическая неопределенность «пряталась» в исходные данные, в частности в величины вероятностей поражения воздушных целей, наземных объектов, вследствие чего вероятностная задача становилась детерминированной и решалась обычными математическими методами.

Чтобы не усложнять учет неопределенностей, обусловленных слабо предсказуемыми действиями противника, в детерминированных моделях исследовались наиболее вероятные (как правило, типовые), по мнению военных экспертов, варианты применения противником своих войск (сил). Поэтому детерминированные модели можно считать лишь одним из этапов научного изучения вооруженного противоборства [85] (2004).

недетерминированные модели — модели, которые по сравнению с детерминированными позволяют исследовать большее количество возможных вариантов действий противника в ходе ведения боевых действий (операций) объединения ВВС.

Необходимо подчеркнуть, что именно недетерминированные, а не стохастические (вероятностные) модели, как это принято в практике моделирования боевых действий (операций). Данное уточнение является очень важным. Прежняя классификация моделей боевых действий (операций), по сути дела, игнорирует наличие другого типа неопределенностей — нестохастических (реальных). К этому типу неопределенности относят неопределенность природы, то есть внешней среды, неопределенность целей (степень соответствия желаемого результата реальным возможностям), неопределенность действий противника.

Нестохастические неопределенности вооруженного противоборства, особенно неопределенности действий противника, играют чуть ли не решающую роль в моделировании боевых действий (операций). Столкновение воюющих сторон, преследующих противоположные цели, оказывает существенное влияние на сценарий развития боевых действий (операций). Для каждого такого сценария командующий и его штаб и выбирают рациональный способ применения своих войск (сил). В какой-то степени нестохастическая неопределенность является первичной по отношению к другому роду неопределенности — стохастической, поскольку сторонами могут быть выбраны такие варианты

действий, которые снижают количество случайных элементарных событий.

В недетерминированных моделях реалистичнее по сравнению с детерминированными моделями отражается комплексное влияние на ход и исход боевых действий (операций) нестохастических и стохастических неопределенностей. Влияние этих неопределенностей в недетерминированных моделях оценивается с учетом наиболее существенных факторов, обусловливающих проявление этих неопределенностей. Так, для учета нестохастической неопределенности предусматривается, что противник практически не ограничен в выборе вариантов способов применения своих войск (сил). Для исследования стохастических неопределенностей случайные процессы, связанные с поражением (обнаружением, радиоэлектронным подавлением) воздушных целей, наземных объектов, воспроизводятся с учетом конструктивных ошибок средств поражения (обнаружения), дальности до цели и ее ракурса, возможности выполнения воздушной целью противоракетного маневра, маскировки наземных объектов поражения, электромагнитной обстановки и т.д. [85] (2004).

комбинированные модели — модели, в которых используются приемы учета неопределенностей, характерные как для детерминированных, так и недетерминированных моделей.

Среди комбинированных моделей можно выделить те, в которых наиболее глубоко исследуется влияние на результат моделирования боевых действий (операций) стохастической неопределенности, либо наоборот — оцениваются слабо предсказуемые действия противника, а вероятностная природа элементарных событий поражения (обнаружения) воздушных целей, наземных объектов учитывается в исходных данных в соответствующих величинах исходных вероятностей [85] (2004).

ситуационные модели (военные игры) — модели, в ход которых в любой момент может вмешаться человеческий фактор.

Причем игроки обеих сторон практически не ограничены в выборе стратегии своего поведения. Каждый из них, выбирая свой очередной ход, может в зависимости от сложившейся обстановки и в ответ на предпринятые оппонентом шаги принимать то или другое решение. Затем он приводит в действие математическую модель, которая показывает, какое ожидается изменение обстановки в ответ на это решение и к каким последствиям оно приведет спустя некоторое время. Пос-

ледствиями могут быть возможное количество потерь сторон, количество подавленных постановщиками помех средств ПВО, ударных средств, пунктов управления и связи и т.д. Следующее «текущее решение» принимается уже с учетом реальной новой обстановки. В результате рациональное решение выбирается после многократного повторения такой процедуры [85] (2004).

вероятностные модели — модели, в которых заданы вероятностные характеристики случайных событий поражения (обнаружения, радиоэлектронного подавления) воздушных целей, наземных объектов.

По заданным характеристикам рассчитываются эффективности боевых действий (операций), например, математическое ожидание числа сохраненных объектов, математическое ожидание числа пораженных воздушных целей и т.д. [85] (2004).

статистические модели — модели, в которых вероятностная модель не задана (или задана не полностью), а в результате машинного эксперимента стали известны реализации случайных событий.

На основе этих данных математическая статистика подбирает подходящую вероятностную модель для получения вывода о рассматриваемых явлениях, связанных с поражением (обнаружением, подавлением) воздушных целей, наземных объектов.

На ранних этапах математического моделирования, в том числе моделирования боевых действий (операций), вероятностный подход являлся наиболее популярным методом учета стохастической неопределенности. Это обусловлено тем, что объем вычислений статистических методов по сравнению с вероятностными методами чрезмерно велик. Для получения обоснованных результатов моделирования с помощью статистических методов требуются быстродействующие ЭВМ.

По мере развития вычислительной техники статистические методы получают все большее применение для учета стохастической неопределенностей боевых действий (операций). Статистика вычислительного эксперимента по поражению (обнаружению) воздушных целей, наземных объектов, полученная в ходе моделирования боевых действий (операций), содержит в себе информацию об условиях проведения эксперимента: конструктивные ошибки средств поражения (обнаружения); дальность до цели и ее ракурс; возможность выполнения воздушной целью противоракетного маневра; маскировка наземных объектов поражения; электромагнитная обстановка. В вероятностных моделях вероятностные характеристики случайных явлений пора-

жения (обнаружения, подавления) воздушных целей, наземных объектов должны быть заданы заранее, что является затруднительным, поскольку невозможно достаточно точно спрогнозировать те условия обстановки, в которых будет осуществляться поражение (обнаружение) воздушных целей, наземных объектов [85] (2004).

методы учета стохастической (вероятностной) неопределенности — методы математической статистики, в том числе метод отношения правдоподобия, метод последовательного анализа, метод Монте-Карло и др. [86] (2005).

4.3.4.4. Расчетно-моделирующие комплексы и системы

моделирующий стенд (МС) — предназначен для компьютерно-аппаратного моделирования процессов функционирования возможных вариантов АСУ для различных идеологических и даже конструкторско-технологических решений создания АСУ в ходе ее разработки.

Важнейшей частью и инструментом МС будет являться экспертно-аналитический аппарат, перечень информационно-расчетных и моделирующих методик которого должен быть не только разработан, но и соответствующим образом утвержден [187] (2009).

4.3.4.4.1. Единая информационно-моделирующая среда для систем военного назначения

единая информационно-моделирующая среда для систем военного назначения — совокупность электронных (виртуальных) моделей, обеспечивающих проведение расчетов и моделирование военных и других действий во всех их проявлениях.

Главная особенность информационно-моделирующей среды состоит в том, что она обеспечивает создание и отображение модели обстановки и вооруженного противоборства во всех сферах вооруженной борьбы (на земле, на море, в воздухе и космосе) на тактическом, оперативном и стратегическом уровнях, а также моделирование действий любых средств вооруженной борьбы и любых группировок войск (сил).

Информационно-моделирующая среда является результатом совместной работы более 30-ти научно-исследовательских учреждений Министерства обороны РФ и предприятий оборонно-промышленного комплекса. Головным исполнителем данных работ является ОАО «НПО РусБИТех» [138] (2015).

потенциальные модели — модели, построенные на аналитических расчетах определения и сопоставления различных потенциалов государств и группировок войск (сил) для оценки военно-политической, военно-экономической и военной обстановки [138] (2015).

экспресс-модели (штабные модели) — модели, построенные на аналитических расчетах определения возможностей противостоящих группировок войск (сил) по развертыванию, перегруппировкам и взаимному поражению для оперативной (быстрой) оценки различных вариантов замыслов операций и других форм военных действий [138] (2015).

имитационные модели (виртуальное поле боя) — модели средств, сил и процессов вооруженного противоборства во всех сферах для определения возможных результатов их действий [138] (2015).

виртуальное поле боя (боевое пространство) — обеспечивает: разработку модели любой обстановки противостояния группировок войск (сил); разработку любых способов ведения ими оборонительных и наступательных операций, боевых и других действий; имитационное моделирование разработанных способов действий; визуализацию обстановки и процессов вооруженной борьбы в двух- и трехмерном виде в стратегическом, оперативном и тактическом масштабе; получение необходимых показателей результатов действий. Виртуальное поле боя включает следующие модели: физико-географических условий выбранных районов военных действий; вооружения и военной техники; воинских формирований; систем управления и связи; средств и систем обеспечения группировок войск (сил); элементов инфраструктуры и оборонно-промышленного комплекса; элементов решений и боевых задач воинским формированиям (модели способов действий войск, сил и средств) [138] (2015).

комплексы информационно-расчетных задач — аналитические информационные и расчетные задачи, с помощью которых можно рассчитывать различные показатели состава и возможностей группи-

ровок войск (сил), оперативно получать ожидаемые результаты их действий, рассчитывать возможности управления, связи, видов обеспечения [138] (2015).

4.3.4.4.2. Планирование применения стратегических вооружений

планирование применения стратегических вооружений — важнейшая часть единого, централизованного, системно скоординированного процесса управления Вооруженными Силами в целом.

Цели, задачи и содержание планирования применения стратегического оружия рассматриваются в контексте более общего процесса планирования операций (военных действий) ВС в их взаимоувязке с мероприятиями по разработке замысла и планов боевого применения других войск и вооружений в составе сил общего назначения (СОН) ВС РФ [174] (2014).

стратегическое планирование — сложный многоэтапный процесс определения целей, масштабов, форм и способов боевого применения войск (сил), ударных средств, информационно-управляющих, оборонительных и обеспечивающих систем, отвечающих задачам применения ВС РФ в войне (вооруженном конфликте).

Сущность планирования применения стратегических вооружений заключается в их рациональном распределении по задачам операций (военных действий), стратегическим воздушно-космическим направлениям, районам сосредоточения усилий и объектам поражения, периодам военных действий и времени нанесения ударов с учетом всей совокупности факторов и условий прогнозируемой (сложившейся) обстановки, а также оперативных, технических и иных ограничений, определяемых свойствами оружия, масштабами и целями его боевого использования [174] (2014).

методическое обеспечение планирования — специальные методы количественного анализа, определяющие множество пространственно-временных характеристик (параметров) плана боевого применения оружия, являющихся главным в его содержательной части [174] (2014).

принципы и положения создания специального математического и программного обеспечения планирования применения

стратегических вооружений — в качестве основных выделяют следующие:

1) Системная ориентация разработок СМПО планирования на обеспечение функций конкретного органа управления (штаба).

2) Ориентация СМПО на решение конкретных практических задач.

3) Ориентация на организационный уровень управления войсками (силами).

4) Поэтапность создания СМПО.

5) Участие органов управления в создании СМПО на всех этапах разработок.

6) Обоснованность выбора системных и математических методов моделирования процессов боевого применения оружия, высокий уровень достоверности получаемых результатов решения информационно-расчетных задач.

7) Информационная обеспеченность моделей (методик, информационно-расчетных задач).

8) Оперативность проведения расчетов с использованием созданного СМПО.

9) Системная согласованность моделей (информационно-расчетных задач) [174] (2014).

4.3.4.4.3. Планирование огневого поражения противника

расчетно-моделирующий комплекс системы воздушных операций — расчетно-моделирующий комплекс (РМК), разработанный в целях обоснования решений на их проведение, а также нанесение массированных, групповых, одиночных авиационных и ракетных ударов.

Работа над созданием РМК началась в середине 90-х годов прошлого века и завершилась его программной реализацией в начале текущего столетия. К середине 2014 года РМК претерпел глубокую модернизацию. Были уточнены и модифицированы научно-методические подходы по моделированию боевого применения формирований ВВС и ПВО с учетом опыта локальных войн и вооруженных конфликтов, доработаны информационно-расчетные задачи по преодолению современных средств ПВО противника, определению потребных нарядов авиации и сил ПВО для нанесения заданного ущерба различным группировкам и объектам с учетом произошедших изменений в формах и

способах их боевого применения. Обновленная версия РМК позволяет определять цели, сроки, построение воздушных операций, привлекаемый состав сил и средств ВВС и ПВО, прогнозировать противоборство сторон в воздушной сфере, оценивать результаты их действий и соответствующие изменения обстановки в установленных зонах ответственности [47] (2014).

повышение эффективности огневого поражения противника — достижение в условиях быстрого роста объема информации необходимой результативности применения вооружения за счет улучшения качества управления на основе комплексирования средств поражения, разведки и управления войсками и оружием, обусловившего создание разведывательно-ударных (огневых) систем [102] (1998).

специальное математическое обеспечение планирования огневого поражения противника — сложная система математического обеспечения, предназначенная для количественного и качественного обоснования предложений по огневому поражению противника (ОПП) в соответствии со складывающейся боевой обстановкой, повышения обоснованности и оперативности планов ОПП, оценки его результатов и определения эффективности ударов сторон в ходе противоборства.

Модели боевых действий, используемые при планировании ОПП, классифицируются по масштабу воспроизводимых операций (боевых действий) — модели стратегического, оперативного и тактического уровня и по предназначению — штабные и исследовательские.

Штабные предназначаются для непосредственного использования в штабах в процессе управления ОПП, оценки его результатов в типовых боевых ситуациях (в огневых операциях, сражениях, ударах и т.д.) и прогноза возможного хода и исхода вооруженного противоборства. С их помощью могут быть получены ответы на главные вопросы, возникающие у командующих (начальников) и штабов при выработке планов ОПП и принятии решения на их реализацию. Исследовательские модели отличаются большей степенью детализации обстановки, многообразием исходных данных, значительными затратами времени и используются обычно в НИУ МО.

Кроме того, модели различаются по целевой направленности. Они бывают оценочными — в них элементы вариантов планов ОПП считаются заданными, а итогом моделирования являются ожидаемые результаты действий сторон или потребные наряды сил и средств по различным вариантам планов ОПП и оптимизирующими — позволяют

находить наилучший результат действий сил и средств по принятому критерию эффективности [102] (1998).

расчетно-моделирующий комплекс для обеспечения общего планирования огневого поражения противника в операциях — к концу 90-х годов были разработаны: теоретические основы планирования огневого поражения противника (ОПП) в общевойсковых операциях, оперативная постановка на расчетно-моделирующий комплекс (РМК), методики и алгоритмы решения информационно-расчетных задач (ИРЗ), архитектура построения и функционирования штабных математических моделей массированного огневого удара и систематического огневого воздействия. Полученная научно-методическая база позволила оперативно осуществить программную реализацию прототипа РМК и его апробацию на мероприятиях оперативной подготовки ВС РФ.

Фактически к середине 2000 года впервые не только была решена одна из ключевых научно-методических проблем, но и создан программный прототип, включающий более 20 ИРЗ, три математические модели и фрагмент системы поддержки принятия решений (СППР). Благодаря этому за время, отведенное на выработку замысла операции, стало возможным получение количественных характеристик по 3—4 вариантам осуществления ОПП, осуществление их сравнительного анализа по заданным критериям и выбора рационального варианта, в максимальной степени соответствующего складывающимся условиям обстановки.

В период с 2008 по 2014 годы РМК по планированию ОПП был доработан с учетом современных взглядов на проведение комплексного воздействия на противника различными средствами поражения, применение высокоточного оружия большой дальности по критически важным объектам противника, создание интеллектуальных СППР органов управления, а также реализован в составе специального программного обеспечения базовой автоматизированной системы управления войсками военного округа [47] (2014).

4.3.4.4.4. Моделирующий комплекс взаимодействия войск

моделирующий комплекс — аппаратно-программный комплекс, обеспечивающий сбор, накопление и визуализацию оперативно-

тактической информации для ее оценки, моделирования действий войск, выработки (уточнения) решений и постановки (уточнения) боевых задач подразделениям в интересах организации и поддержания взаимодействия войск [172] (2013).

подсистема сбора и ввода информации — аппаратно-программный блок, отвечающий за получение данных, источником которых могут быть объекты, включенные в автоматизированную систему управления (АСУ) войсками по каналам связи, а также электронные топографические карты, материалы дистанционного зондирования, различные текстовые документы, донесения, сводки и др. [172] (2013).

подсистема управления и хранения информации — реализует набор функций управления информационными ресурсами комплекса и взаимодействие с внешней средой через систему сбора и ввода оперативно-тактической информации со всех уровней управления, обеспечивает восстановление работы комплекса после проявления неисправностей в технических средствах, функционирование других программ и управление ими, а также организацию хранения и защиты оперативно-тактической информации [172] (2013).

подсистема моделирования — включает операции, обеспечивающие проведение всех аналитических действий, осуществляемых при организации взаимодействия [172] (2013).

подсистема пользователя — посредством библиотек специальных процедур позволяет создавать программные элементы задач, возникающих внезапно и не реализованных заранее [172] (2013).

подсистема вывода информации — предназначена для визуализации электронных топографических карт, информации, проходящей по каналам АСУ, результатов работы подсистемы моделирования, а также оформления и выдачи на печать боевых документов по организации взаимодействия или их фрагментов [172] (2013).

4.3.4.5. Субъективные аспекты применения математического моделирования

субъективный фактор лица, принимающего решения, в военном деле — не просто неизбежное, а и закономерное явление.

В условиях неполной информации опытные командиры (начальники) способны формулировать правильные решения на интуитивном уровне. При этом обычно они исходят из своих субъективных представлений о важности различных критериев оптимальности и эффективности возможных альтернатив принимаемых решений.

Именно это часто порождает субъективное неприятие результатов математического моделирования, что в конечном счете может приводить к серьезным ошибкам в планировании и боевом управлении [211] (2011).

субъективное неприятие применения математического моделирования должностными лицами органов военного управления — основными причинами неприятия любого новшества, как уверяют психологи, являются непонимание его сущности, незнание особенностей и неумение его применять.

Теоретически должностные лица ОВУ, применяющие компоненты специального программного обеспечения в своей практической деятельности, должны понять границы применимости математической модели.

Еще одна проблема — проблема разделения ответственности за принимаемые решения между пользователем модели и разработчиком ее математического аппарата.

Существенно влияет на внедрение математического моделирования в практику деятельности ОВУ нерациональность компоновки интерфейсов, создаваемых промышленностью математических моделей.

Немаловажно и личное отношение каждого должностного лица к результатам математического моделирования. Не секрет, что порой должностные лица ОВУ, не удовлетворенные результатами моделирования, пытаются различными способами их скорректировать. Хорошо знающий модель пользователь (оператор) может «сыграть» различными факторами так, чтобы повлиять на результаты в нужную сторону. Но вот подтасовать результаты, не меняя исходные данные, невозможно, особенно, если модель используется для сравнительного анализа вариантов применения войск (сил) при прочих равных условиях. Сами результаты могут меняться, а вот тенденцию изменения ситуации модель все равно покажет верную.

Подход к разрешению этой ситуации, на наш взгляд, тот же — привлечение должностных лиц к разработке математического аппара-

та, который закладывается в СМПО, создаваемое для автоматизации их деятельности.

Анализ субъективных факторов, мешающих применению математического моделирования в практической работе ОВУ, показывает, что имеющиеся недостатки являются системными. Для их устранения необходимо менять порядок как создания математических моделей, вводя обязательные этапы, предусматривающие участие будущих пользователей моделей в их разработке, так и порядок подготовки должностных лиц ОВУ к работе с ними.

В целях уменьшения негативного влияния субъективных факторов на применение математического моделирования в практике работы ОВУ необходимо повысить знания и умения пользователей СМПО и преодолеть нежелание разработчиков учесть их требования (преодолеть под твердым руководством заказчика АСУВ, при помощи ОВУ и организаций, осуществляющих военно-научное сопровождение работ). Для этого необходимо:

— совершенствование порядка разработки математических моделей, включение в процесс разработки обязательных этапов макетирования и апробации макетов в ОВУ; изменение отношения (повышенное внимание) к созданию программных интерфейсов математических моделей из состава СМПО АСУВ;

— корректировка руководящих документов, определяющих содержание этапов разработки математических моделей;

— оптимизация процесса подготовки должностных лиц, применяющих математические модели в составе специального программного обеспечения комплектов средств автоматизации пунктов управления [211] (2011).

4.3.5. Программное обеспечение

4.3.5.1. Географические информационные системы

геоинформация — 1) в широком понимании — совокупность сведений и описаний, характеризующих объекты и явления на земной поверхности, отражающая наличие пространственно-временных отношений между ними;

2) в прикладном значении — пространственно-временные данные, формализованные в виде совокупности информационных моде-

лей, предназначенных для обработки сведений об объектах, процессах и явлениях, происходящих на Земле, с использованием различных геоинформационных систем [178] (2016).

геоинформационные технологии — совокупность средств, способов и методов обработки данных, имеющих пространственный аспект и обеспечивающих получение информации в требуемом виде.

В геоинформационных технологиях выделяют две взаимосвязанные области: моделирование пространственных данных (определение координат и топологии реальных объектов, создание и обновление электронных карт) и использование последних в расчетно-аналитических задачах для количественного обоснования принимаемых решений.

Наиболее важными сферами их применения можно считать: навигацию; анализ влияния местности на боевую эффективность войск (сил) и оружия (определение зон видимости, оптимальных маршрутов, проходимости местности); планирование операций (моделирование боевых действий, оценка местности); разведку; картографирование (ввод данных наблюдений, составление обзорно-географических, топографических, специальных тематических карт, формирование картографических документов планирования) [90] (1999).

геоинформационная технология в АСУВ — технология получения качественно новой информации, необходимой для решения задач управления войсками на основе анализа соответствующим образом структурированной картографической информации.

Такая информация может включать данные об объектах, имеющих пространственную привязку (свои войска, противник, местность и др.) [67] (2004).

геоинформационная система[1] (ГИС) — система управления базами данных, предназначенная для работы (сбора, хранения, структурирования, анализа и вывода) с территориально ориентированной информацией.

Важнейшей особенностью ГИС является способность связывать картографические объекты с их свойствами (атрибутами). В простейшем случае каждому картографическому объекту ставится в соответствие строка таблицы (запись в базе данных) с атрибутивной информацией, что и определяет основные функциональные возможности ГИС [126] (2001).

геоинформационная система[2] (ГИС) — специализированная трехмерная информационная система, обеспечивающая сбор, обработку, формирование и визуализацию виртуальных и физических объектов, имеющих пространственную локализацию.

К числу разнообразных задач и функций управления и обеспечения, которые могут быть более эффективно решены и выполнены органами управления ВКО с помощью ГИС, относятся: сбор, обработка, хранение и отображение информации о всех элементах наземной и воздушно-космической обстановки с учетом их пространственного расположения и динамики изменения; формирование и отображение пространственных данных для принятия обоснованного решения на ведение операций (боевых действий) на основе более эффективной информационной поддержки (лучшая информированность помогает принять лучшее решение, так как ГИС обеспечивает представление исходных данных и получаемых результатов в наглядном и удобном для восприятия виде); совершенствование группировок войск и сил, боевых порядков частей и соединений, принятие решения на маневр и выполнение маневра силами и средствами с использованием цифровых карт местности; обеспечение безопасности полетов своей авиации путем отображения ситуации на местности с целью выявления объектов (гор, зданий, вышек, антенн и др.), которые могут оказать влияние на эту безопасность; организация и проведение мероприятий по всестороннему обеспечению боевых действий войск (сил); прогнозирование маршрутов полета нарушителей государственной границы и принятие необходимых мер против них; прогнозирование, контроль и принятие оперативных мер при аварии (разрушении) радиационно и химически опасных объектов; проведение восстановительных и спасательных работ, строительство новых сооружений, подъездных путей и других объектов; оценка проходимости местности; проведение мероприятий по оперативной и боевой подготовке органов управления (использование ГИС позволит максимально приблизить занятия к натурным тренировкам); разработка боевых (оперативных), отчетных и других графических документов [125] (2010).

интегрированная геоинформационная среда в едином информационном пространстве (ИГИС в ЕИП) — совокупность упорядоченных в заданной системе координат и предметно структурированных баз данных, относящихся к топографической, навигационной,

геофизической, гидрографической, геологической, гидрометеорологической и другим видам специализированной обстановки, отражающей состояние поверхности Земли и (или) околоземного, водного, подземного и подводного пространства, а также технологических и инфраструктурных средств, обеспечивающих работу с такими ресурсами [178] (2016).

электронная карта — цифровая картографическая модель, подготовленная для показа на экране средствами отображения информации в специальной системе условных знаков и соответствующая содержанию аналоговой (бумажной) карты определенного вида и масштаба[44] [172] (2013).

4.3.5.1.1. Классификаторы условных знаков

геоинформационная система «Интеграция» — геоинформационная система, применяемая в Военной академии Генерального штаба ВС РФ для нанесения и редактирования на электронной карте оперативной обстановки в ходе подготовки и проведения занятий и командно-штабных учений.

Система позволяет создавать векторные, растровые и матричные карты, а также оперативно обновлять различную информацию о местности, выполнять по карте расчеты (определять длины, площади, периметры, строить профили, зоны отсечения, вести статистику по характеристикам объектов), решать прикладные задачи (создавать тематические карты и диаграммы, обрабатывать GPS данные), выводить на внешние устройства печати изображение электронной карты с нанесенными на нее условными знаками. Слои векторной карты со всеми входящими в них объектами и их характеристиками описаны в цифровом классификаторе этой карты. ГИС «Интеграция» поддерживает стандартные системы классификации, кодирования объектов и их характеристик в соответствии с требованиями Роскартографии и топографической службы ВС РФ [170] (2010).

классификатор условных знаков обстановки — классификатор Violit ВАГШ для создания карт, на которые пользователи наносят обстановку.

---

[44] ГОСТ Р 52438—2005.

В классификаторе условные знаки обстановки объединены в слои, которые подразделяются по видам ВС и родам войск: Сухопутные войска, ВВС, ВМФ, ПВО, РВСН, инженерные войска, войска связи, РЭБ, РХБЗ и другие. Для удобства большинству слоев присвоены названия кафедр (учебных модулей) ВАГШ. Это означает, что каждая кафедра использует в основном характерный для нее определенный набор обозначений объектов. При этом каждый пользователь может независимо добавлять в классификатор новые слои и условные знаки и изменять их характеристики. В связи с этим у разных пользователей классификаторы могут иметь одинаковые названия, но разное количество объектов и слоев, разные характеристики одних и тех же объектов. Следовательно, уже нельзя говорить о том, что эти классификаторы являются одинаковыми [170] (2010).

объединение классификаторов — поскольку при создании карт с обстановкой в ВАГШ могут использоваться отличные друг от друга классификаторы, на практике часто возникает ситуация, когда пользователи создают на один район карты единого масштаба, но с разными классификаторами.

Но копировать объекты можно только на карту с идентичным классификатором, т.е. с классификатором, где объекты и семантики имеют те же классификационные коды. В связи с этим, прежде чем копировать объекты с одной карты на другую, необходимо убедиться, что данные объекты полностью идентичны тем, которые описаны в классификаторе карты, на которую они будут копироваться.

Если все же классификаторы оказались различными, то перед тем как произвести копирование объектов с нескольких карт на одну, необходимо сделать классификаторы карт идентичными. Если объекты будут копироваться на новую карту, то перед ее созданием следует предварительно создать новый классификатор, в который необходимо собрать из других классификаторов все нужные объекты. В случае, когда на карту с нанесенной обстановкой надо скопировать объекты с других карт, перед копированием необходимо перенести в классификатор этой карты все недостающие объекты [170] (2010).

групповые условные знаки — знаки, создающиеся из нескольких векторных объектов, которые располагаются друг над другом.

Пользователь устанавливает расстояния между соседними объектами и определяет, какой знак над каким будет находиться. Удобство создания группового условного знака состоит в том, что все входящие

в него объекты можно одновременно перемещать, копировать или удалять. При этом расстояния между объектами и их взаимное расположение друг относительно друга сохраняются.

Данный режим создания группового условного знака также позволяет выбрать из классификатора карты линейный или векторный объект и установить его как выноску условного знака [170] (2010).

4.3.5.2. Интеллектуальные информационные системы

интеллектуальная система — совокупность или множество субъектов и объектов, связанных между собой организационно, находящихся в состоянии активности, взаимодействия под воздействием единого для них внешнего мира [94] (2010).

интеллектуальные информационные системы — информационные системы, которые наряду с традиционными функциями сбора, хранения, накопления, поиска, обработки информации и передачи данных, включают средства автоматизации таких «семантических задач», как машинный перевод, смысловой поиск, обработка текстовых сообщений (для их реферирования, аннотирования, классификации), выделение фактографических данных из текста документа и т.п.

Их создание требует соответствующего методического аппарата формализации и распознавания текстовых сообщений на естественном языке (ограниченном естественном языке), а также построения соответствующих инструментальных средств смысловой обработки таких сообщений [107] (2004).

создание интеллектуальных АСУ — необходимый этап для практической реализации идеи «сетецентризма» в деятельности войск и сил.

Внедрение интеллектуальных технологий в АСУ войсками, сложными многозвенными комплексами вооружений (планирования, целеуказания, расчета полетных заданий) ведет к созданию человеко-машинных систем высокого уровня, предназначенных для реального управления и наработки новых знаний, алгоритмов, систем нечетких правил и моделирования.

Подходы к созданию интеллектуальной (интеллектуализированной) АСУ (ИАСУ) состоят в следующем:

1) Общие принципы построения ИАСУ: системный подход, централизация и эмерджентность, декомпозиция, адаптация (к изменению обстановки, целей управления и технологического процесса), развитие по горизонтали (расширение связей и круга задач) и по вертикали (развитие целей управления), живучесть в критических ситуациях (сохранение эффективности), стандартизация, унификация.

2) Одно из основных направлений создания ИАСУ — системотехническая, информационная интеграция в иерархическую сетевую организационно-техническую структуру средств автоматизации (планирования, командно-сигнальных, моделирования, разработки, расчета полетных заданий ударным, разведывательным комплексам, системам связи, РЭБ, оружию, информационного обеспечения) огневого, тактического, оперативного уровней.

Необходима проработка научно-методических, системотехнических, информационных основ создания и обеспечения ИАСУ, ее организационной, функциональной структур, в том числе при образовании «сетецентричных» систем. Затем следует осуществить системное проектирование, разработку технического облика и структуры, формирование интегрированных баз данных и знаний о противнике, условиях выполнения оперативных, боевых задач, порядке их ведения и т.д.

3) Условия создания и организации функционирования ИАСУ:

— тесное информационное взаимодействие ИАСУ с реальной обстановкой;

— сохранение функциональности при потере некоторых связей;

— наличие аппарата прогнозирования событий, изменений в обстановке и состояния собственных управляемых объектов;

— открытость ИАСУ для интеллектуализации и совершенствования на каждом новом уровне, при получении новых задач;

— построение ИАСУ в виде многоуровневой иерархической структуры.

4) Для согласованного комплексного решения информационно-расчетных задач, моделирования в режимах реального времени и его масштабирования при обосновании и выработке оперативных и тактических задач войскам, силам, замыслов и планов огневого поражения, ударов, взаимодействия, применения оружия, специальных систем, расчета полетных заданий, прицельных данных, подготовки документов, а также адаптации системы к изменяющейся обстановке необходимо в рамках ИАСУ реализовать информационно-техническое взаимодействие средств автоматизации.

5) Как специальное направление проектирования ИАСУ предлагается осуществлять создание методических основ ее интеллектуализации. Процесс «обучения, тренировки» на изменяющиеся параметры внешней среды, в том числе на субъективные особенности лиц, участвующих в управлении, должен быть непрерывным на всех этапах управления войсками, силами и оружием (в ходе оперативной, боевой подготовки и боевых действий) с использованием всех комплексов автоматизации (управления, планирования применения войск и оружия, подготовки полетных данных).

Интеллектуализация АСУ состоит в «наращивании объема знаний» об условиях, моделях функционирования объектов управления, систем автоматизации управления на «предыстории» планирования применения и управления автономным оружием как отправной базы сведений об условиях, алгоритмах и моделях решения совокупности частных задач.

6) Обеспечение повышения функциональности системы («обучение» и «тренировку»), что обусловлено содержанием, взаимосвязью, взаимным влиянием друг на друга процессов повышения квалификации и накопления опыта специалистами органов управления (знаний, алгоритмов решения задач).

7) Определить место интеллектуальных технологий в структуре АСУ на ближайшую перспективу в обеспечении решения частных информационных задач при планировании применения войск, оружия, подготовке заданий боевым системам.

8) Специальное программное обеспечение (СПО), созданное в промышленности, полагать исходным продуктом для «обучаемой» АСУ.

9) В «обучении» ИАСУ следует учитывать аспекты двусторонности процесса и результатов:

— Во-первых, органы управления и войска обеих сторон наращивают опыт, приобретая искусство ведения сражения и боя. Формируются образные представления боевых ситуаций, противника, вплоть до психологических оценок; командованием сторон вырабатываются идеи, замыслы, первоначально не имеющие материального воплощения; при их реализации проявляются объективно обнаруживаемые факты, планы вскрываются, командиры сторон приобретают знание и ощущение противника.

— Во-вторых, обучаются и персонал органа управления, и комплекс ИАСУ, что эмерджентно, по сути: система управления развива-

ется как человеко-машинная система, поэтапно приобретая качественно новые свойства.

10) Организационные, кадровые, системотехнические изменения фактически «обнуляют» предыдущие периоды «обучения». Переход к планированию следующей операции на прежнем операционном направлении также потребует нового цикла «обучения» системы. «Обученная» система несет проблемы сохранения функциональности, более сложные, чем просто восстановление выучки и слаженности реорганизованного штаба [94] (2010).

4.3.5.2.1. Интеллектуализация процессов управления

интеллектуализация — внедрение специально разработанных «интеллектуальных» систем в информационные процессы и процессы управления, позволяющих повышать их эффективность за счет использования в данных системах знаний специалистов (экспертов), определенным образом структурированных и хранящихся в специализированных базах знаний. При этом такие базы создаются заблаговременно применительно как к различным видам операций (боев) и к выполняемым в них задачам, так и к обеспечивающим их информационным процессам и процессам управления [80] (2008).

интеллектуализация в информационной сфере в операции (бою) — использование таких «интеллектуальных» систем, которые при обработке больших объемов данных в условиях определенного дефицита времени позволяют уже по отдельным элементам обстановки прогнозировать и упреждающе выдавать начальникам, командующим (командирам) обобщенную картину, складывающуюся к конкретному времени и в определенном районе или полосе боевых действий и требующую принятия соответствующего решения в целях ее изменения [80] (2008).

4.3.5.2.2. Принципы создания интеллектуальных информационных систем

принцип интеллектуальности — предполагает, что информационная система должна обеспечивать поиск как по библиографичес-

кому описанию документов (профилю), так и по контексту документов и степени их принадлежности к предметным рубрикам (смысловой поиск). Кроме того, данный принцип предусматривает возможность формирования и накопления различных знаний, выполнения проблемно-ориентированных запросов, уточняющего поиска и т.д. [107] (2004).

принцип открытости — означает, что должны поддерживаться стандартизованные интерфейсы для встраивания в существующие системы [107] (2004).

принцип наглядности — связан с наличием средств систематизации и упорядочения документов [107] (2004).

принцип адаптивности — возможность динамической настройки интеллектуальной информационной системы в процессе ее эксплуатации на обрабатываемую предметную область, информационные и эргономические потребности должностных лиц ОВУ.

Другими словами, принцип адаптивности предполагает устойчивую работу системы во многих предметных областях [107] (2004).

4.3.5.2.3. Технологии интеллектуализированного управления

нечеткие технологии (fuzzy-технологии) — совокупность математических методов, в которых используются нечеткие понятия, множества, знания, меры, логика, алгоритмы, интегральное исчисление, исчисление предикатов и др.

Основы «нечеткой технологии» — «нечеткие логика, алгоритмы, знания», нейросети, ассоциативная память, экспертные системы, широко функционирующие в системах управления специальных и боевых роботов.

Технология применена в автоматизированном комплексе оценки угроз и подготовки полетных заданий самолетов Р-15, что подтверждает ее возможности для надежной оценки и распознавания обстановки по совокупности различной нечеткой информации, разработки обоснований к замыслу, решениям, планам, при непосредственном управлении, в том числе в «сетецентричных» системах [94] (2010).

нечеткая логика — совокупность логических операций над высказываниями, в которых есть лингвистические переменные и нечеткие множества.

В отличие от стандартной (четкой) логики, оперирующей бинарными состояниями (да/нет, истина/ложь, 1/0), она позволяет определять нечеткие промежуточные значения, например, «более приоритетный — менее приоритетный», «воспрещение — подавление — вывод из строя — уничтожение — разгром» [94] (2010).

нечеткие алгоритмы (лингвистические) — упорядоченное множество нечетких правил, содержащих нечеткие указания (например, «если..., то...») [94] (2010).

нечеткие знания — переменные во времени и контексте совокупности именованных отношений между объектами и окружением.

Традиционное понимание знания — совокупность обобщенных данных (описаний объектов и их окружения, явлений, фактов) [94] (2010).

4.3.5.2.4. Гибридные системы вычислительного интеллекта

вычислительный интеллект (ВИ) [Soft Computing] — научное направление, где решаются задачи искусственного интеллекта на основе новых нетрадиционных методов вычислений.

В настоящее время считают, что вычислительный интеллект включает в себя следующие основные методы:

нейросетевые — использующие обучение, адаптацию, классификацию, системное моделирование и идентификацию систем на основе исходных данных;

нечеткой логики — основанные на теории нечетких множеств и обеспечивающей эффективные средства математического отражения неопределенности и нечеткости исходной информации, позволяющие построить модель, адекватную исследуемой предметной области;

генетические — использующие синтез, настройку и оптимизацию исследуемых систем с помощью специальным образом организованного случайного поиска и эволюционного моделирования.

Эти методы являются основными в вычислительном интеллекте, однако, необходимо заметить, что число новых методов примкнувших

к ним в последнее время постоянно расширяется, не являясь строго определенным. Ниже перечислены наиболее значимые из них: когнитивная компьютерная графика — методы визуализации данных, позволяющие активировать наглядно-образные механизмы мышления ЛПР, облегчающие принятие решения в сложной обстановке или нахождение решения сложной проблемы; фрактальная геометрия; теория хаоса; нелинейная динамика [208] (2009).

технология вычислительного интеллекта — совокупность новых методов и средств обработки знаний, документооборота, методов выработки и выбора альтернативных вариантов решений, объединенных в целостную технологическую систему для принятия и доведения решений до исполнителей.

Эта совокупность предполагает, как правило, наличие развитого человеко-машинного интерфейса, системы (или элементов) вычислительного интеллекта и возможность использования электронных карт местности [208] (2009).

трудноформализуемые задачи — задачи, которые не могут быть заданы в численной форме, цели которых не могут быть выражены в терминах точно определенной целевой функции, алгоритмического решения которых либо не существует, либо его нельзя применять в силу ограниченности вычислительных ресурсов, невозможно получить всю необходимую информацию [208] (2009).

4.3.5.2.5. Продуктивное управление

интеллектуальная творческая деятельность органов управления — организация личностей, реализующих процесс управления для достижения сформулированной цели и удовлетворения своих потребностей с использованием имеющихся сил и средств [192] (1997).

продуктивное управление — целостное, гармоничное и безопасное управление войсками на основе механизмов продуктивного формирования решений и продуктивности самих сформированных решений.

Основу интеллектуальной деятельности в продуктивном управлении составляет принятие решений, которое представляет собой процесс выработки последовательности действий в интересах достижения

сформированной цели и удовлетворения потребностей (духовных, информационных, материальных) организации в продуктивном управлении [192] (1997).

интеллектуальная система поддержки принятия решений (ИСППР) — система обеспечения интеллектуальной деятельности (в отличие от традиционного представления таких систем как индивидуальных интеллектуальных систем, ориентированных на помощь в решении задач отдельным должностным лицом, что сводит ее к экспертной системе).

Предлагаются следующие базовые положения для ее создания. Основу управленческой деятельности составляет организация управления, включающая в себя комплекс мероприятий по подбору коллектива людей, определению способов и языка взаимодействия, круга решаемых ими задач на основе принципов конструирования организационных систем. На базе сформированной организации осуществляется управление при выполнении боевых задач. В реальной управленческой деятельности лицо, принимающее решения, и образованная им организация должностных лиц постоянно сталкиваются с проблемными ситуациями, возникающими из-за неопределенности исходной информации и риска принимаемых по этим ситуациям решений. Традиционная схема решения как выбор одной из имеющихся альтернатив в проблемных ситуациях не работает; управление и принятие решений осуществляются для достижения сформулированной или сформированной цели и удовлетворения потребностей лица, принимающего решения, и должностных лиц, участвующих в управлении. Проблемная ситуация характеризуется ее разрешимостью, т.е. возможностью выработать решение, устраняющее ее проблемность, и опасностью того, что ее последствия могут носить катастрофический характер для людей, участвующих в управлении, всей системы управления и общества в целом. Складывающиеся в процессе управления ситуации характеризуются гармоническим соотношением их составляющих, целостностью и безопасностью. При выработке замысла, составляющего основу решения, ЛПР использует информацию о проблемной ситуации, включающую не только данные и знания, но и смысл ситуации (в том числе свой личностный смысл) [192] (1997).

смысл — идеальное содержание, идея, сущность, предназначение, цель, ценность и т.п. какого-либо объекта, субъекта, процесса, яв-

ления и т.п., представляемые человеком в конкретной ситуации для разрешения им своих проблем.

Смысл выражает целостное содержание мысли человека об объекте [192] (1997).

база смыслов — включает в себя смыслы ситуаций, процессов, явлений, объектов и отношения между смыслами, которые складываются на основе различных операций [192] (1997).

средства обработки смыслов — анализ процесса мышления в целом и принятия решения в частности показывает, что фактически человек в конкретной ситуации исходит из вопроса «зачем?», а не «что?» и «как?», т.е. идет от смысла. Обработка смыслов составляет основу мышления личности. Не сформировав для себя смысла того или иного объекта, процесса, явления, человек оказывается не в состоянии решать сложные проблемы.

В связи с этим перспективные интеллектуальные системы управления Вооруженными Силами должны, на наш взгляд, обеспечивать обработку смыслов, а не только знаний и данных. Это, в свою очередь, обусловливает необходимость моделирования как рациональной умственной деятельности должностного лица органа управления, так и включения в указанный процесс его воли и эмоций.

Одним из актуальных направлений создания средств обработки смыслов является разработка системы распознавания управленческих (функциональных и проблемных) ситуаций. Важная ее особенность заключается в том, что результат распознавания должен отражать смысл ситуации, который в нее вкладывает должностное лицо конкретного органа управления [68] (1999).

4.3.5.2.6. Навигационные комплексы надводных кораблей с использованием элементов искусственного интеллекта

комплекс навигации и стабилизации надводных кораблей ВМФ, основанный на интеллектных компонентах — комплекс средств автоматизации, решающий ряд основных задач, к которым относятся: обеспечение навигационной безопасности плавания, в том числе и задачи тактического маневрирования и расхождения с целями; выработка и выдача необходимых навигационных и динамических па-

раметров в системы оружия; выработка и выдача необходимых навигационных и динамических параметров в систему управления движением корабля; обеспечение заданных требований по точности и надежности выработки необходимых навигационных и динамических параметров; оценка гидрометеорологической обстановки.

При этом не только повышаются требования к качеству получаемых решений для традиционных задач навигации и управления, но и появляются тенденции возложения на комплекс навигации и гиростабилизации новых, ранее не свойственных ему функций, исполнение которых еще в недавнем прошлом считалось прерогативой человека. Обе эти тенденции порождают задачи, характеризующиеся плохой формализуемостью и высокой степенью неопределенности. Модели в таких задачах невозможно с достаточной степенью адекватности описать, например, дифференциальными или разностными уравнениями. Знания о них и о способах их решения, как правило, ограничены знаниями экспертов, представляемыми в виде правил [209] (2008).

морская навигация — является как наукой, так и искусством.

Действительно, в построении траекторий движения корабля или оценки безопасности плавания существенное значение имеет человеческий фактор. Задачи обработки информации, управления, контроля и диагностики характеризуются существенной степенью модельной неопределенности. Выбор состава средств навигации, момента и типа коррекции навигационного комплекса, критерия при формировании закона управления, а также принятие решений штурманом по различным проблемам управления предполагают учет многих факторов, характеризующих текущую ситуацию [209] (2008).

искусственные нейронные сети — применяются для решения целого класса задач, где используются не уравнения динамики и не столько правила, как в традиционных экспертных системах, сколько опыт. Нейронные сети являются важным инструментом автоматизации принятия решений, поскольку построение алгоритмов или логических исчислений для решения многих задач упирается в сложность учета всех мыслимых сочетаний факторов и формализации закономерностей, связывающих условия задачи с результатом. В сложных системах автоматического управления нейронные сети хорошо поддерживают рефлекторный уровень управления. Более мощные интеллектные системы могут совмещать и нейронный, и логический механизмы принятия решений.

В настоящее время область практических приложений нейронных сетей очень широка: от электромеханических систем (роботы) до сложных плохо описываемых процессов [209] (2008).

эволюционные (генетические) алгоритмы — генетические алгоритмы со специальными структурами данных.

Эволюционные алгоритмы — это алгоритмы, оперирующие с популяцией индивидов. Они довольно легко применимы в прототипировании для апробации в решении тех или иных задач. Однако результаты могут быть очень хорошими в одних или плохими в других задачах. Эволюционные алгоритмы могут комбинироваться с нейронными сетями.

В качестве примера использования эволюционных алгоритмов в задачах управления можно привести планирование маршрута для корабля. Целью любой навигационной схемы является достижение заданной точки с рациональным расходованием ресурсов, без столкновений с другими объектами и т.п. Часто путь корабля планируется заранее в режиме офлайн. Это характеризуется тем, что необходимые сведения вводятся заранее (маршрутные точки, скорости и др.), данные и знания не меняются в процессе решения задачи и время реакции продолжительное (измеряется минутами или часами) в отличие от систем управления со значительно меньшим временем реакции, измеряемым в миллисекундах. В данной задаче навигации планирование офлайн осуществляется в предположении, что среда известна полностью, статична и корабль может реализовать заданный маршрут так, как он запланирован. Однако ограничения планирования офлайн (неполнота информации) приводят к необходимости планирования в реальном времени, т.е. в процессе движения. Это осуществимо, если обеспечить приобретение знаний о среде с помощью первичных датчиков информации корабля и использовать их для преодоления препятствий в процессе перемещения в среде.

Эволюционные алгоритмы позволяют объединить планирование офлайн и планирование в реальном времени (планирование онлайн): планирование офлайн, основываясь на карте, ищет близкий к оптимальному глобальный путь, а планирование онлайн отвечает за учет возможных отклонений обстановки (например из-за обнаружения первоначально неизвестных объектов) путем замены части глобального плана другим оптимальным подмаршрутом [209] (2008).

системы, основанные на знаниях (СОЗ) — являются более адекватными компонентами систем управления для реализации высокоинтеллектуальных функций. В этом случае знания могут быть представлены на некотором логическом языке, и их обработка с помощью соответствующих средств позволяет получить некоторые предпочтения на множестве допустимых управлений в целях выбора одного из них.

В общем случае СОЗ оперируют с более широкой информацией — логическими, объектно ориетированными и другими моделями, основанными на знаниях экспертов. Вместе с тем СОЗ могут использовать и традиционные алгоритмы, базирующиеся на уравнениях динамики. Поэтому, как и в случае использования нейронных сетей и эволюционных алгоритмов, класс решаемых задач значительно расширяется.

Базовая информация СОЗ делится на данные (значения различных величин, элементарные факты и т.п.), знания и умения. Причем различие данных и знаний определяется уровнем сложности их представления. **Данные** — это константы и факты, т. е. элементарные формулы. **Знания** — это формулы с кванторами, которые образуют так называемые предикатные языки. В рамках лингвистического подхода к представлению знаний (используемого, например, в нечетких логиках) данные и знания представляются с помощью не только чисел, но слов и предложений естественного языка.

В СОЗ присутствует не только знание, но и **умение**. Оно представлено процедуральной информацией, для которой характерно прежде всего исполнение, в то время как данные хранятся и пересматриваются, а знания преобразовываются и применяются. При этом в отличие от данных знания могут иметь не только информационную часть, но и описательную для более эффективной их актуализации. Кроме того, в качестве информационных единиц знания могут выступать как встроенные процедуры, что придает знаниям активность, их первичность по отношению к процедурам [209] (2008).

4.3.5.2.7. Информационно-расчетное обеспечение управления войсками

проблема информационно-расчетного обеспечения управления — в ходе реальных боевых действий достичь идеального информационного обеспечения расчетов очень сложно. В боевых условиях

всегда будет иметь место наличие неполной, недостаточной, недостоверной, противоречивой информации (и даже дезинформации), когда исходные данные будут частично, а иногда и полностью отсутствовать или в лучшем случае поступят в органы управления в форме интервальных (диапазонных). Более того, входная информация может доставляться даже в форме лингвистических сообщений типа «больше — меньше», «дальше — ближе» и т.п. [118] (2013).

фактор информационной неопределенности — существование такого фактора при принятии командирами общевойсковых тактических формирований оптимальных (обоснованных, целесообразных) решений обусловлено следующими основными причинами:

крайне сжатыми сроками добывания, подготовки и обработки первичной (исходной) информации для процессов управления в современных высокодинамичных боевых действиях, а также требованиями работы в режиме реального времени;

необходимостью решения проблемы опережения вероятного противника в действиях с учетом постоянного сокращения продолжительности циклов боевого управления;

недостаточным количеством, низкими возможностями и надежностью существующих и отдельных разрабатываемых средств сбора (добывания), передачи, обработки, хранения и выдачи информации;

сложными природными условиями добывания информации (местность, погода, время суток и др.);

возрастающим противодействием (огневым, радиоэлектронным и др.) противника силам и средствам добывания, передачи, приема, обработки и хранения информации, реализации информационных процессов, приводящим к их потерям или снижению возможностей;

повышением эффективности маскировки объектов и намерений противника, в том числе с применением методов дезинформации;

недостаточной разработанностью эффективных и оперативных методов и технических средств распознавания, классификации объектов, а также теории прогноза намерений противника;

недостаточным уровнем профессиональной подготовки личного состава, неквалифицированным использованием им существующих сил и средств добывания, передачи, приема, обработки и хранения информации;

невысокой степенью состояния теории и практики создания, актуализации и использования единого информационного (информаци-

онно-коммуникационного) пространства, количественной и качественной оценки информации в сообщениях;

отсутствием современных высокоэффективных космических средств и комплексов сбора и передачи данных обстановки, а также специализированных наземных пунктов (групп, подразделений) приема и обработки подобного рода информации;

низким уровнем защиты информации в телекоммуникационных каналах и вычислительных средствах от сбоев, вирусов, компьютерных атак противника;

недостаточным информационным (а также программным, техническим, организационным) сопряжением технических средств систем управления разнородных и разновидовых общевойсковых формирований, формирований других силовых министерств и ведомств, а также местных органов власти для повышения качества информационного обеспечения процессов управления;

малоэффективным внедрением теоретических методов и технических средств восстановления информации при появлении сбоев, искажений, а также современных информационных нанотехнологий, систем искусственного интеллекта в работу органов управления и в целом всей системы управления общевойсковыми тактическими формированиями;

не всегда оправданным увлечением «модными» теориями управления (типа «сетецентрических войн», основанных на идеологии использования исключительно сверхразвитых и сверхсложных, практически идеальных информационных систем, работающих только с однозначными и полными данными), отвлекающими специалистов от решения актуальных вопросов реального совершенствования информационно-расчетного обеспечения процессов управления в самых сложных условиях обстановки, и др. [118] (2013).

информационный потенциал общевойскового тактического формирования — величина, характеризующая возможности системы управления по формированию, хранению, обработке, обмену и управлению информационными ресурсами общевойскового тактического формирования [118] (2013).

дефазификация — операция перехода от нечеткости к однозначности данных [118] (2013).

оптимизация решений (планов) — управление общевойсковым тактическим формированием в условиях информационной неопределенности (отсутствия информации о возможных действиях или намерениях противника).

Важно всегда помнить, что упущенный выигрыш всегда оказывает на ситуацию меньшее влияние, чем реализованный проигрыш. Для командира общевойскового тактического формирования начать бой, который будет проигран, гораздо хуже, чем упустить ситуацию, в которой можно было бы его выиграть [118] (2013).

4.3.5.2.8. Экспертные системы

данные[2] — совокупность сведений об объектах предметной области, свойствах объектов и связей между свойствами объектов, а также различные значения и параметры, используемые при решении задач данной предметной области [77] (2015).

знания[2] — совокупность правил манипулирования данными, под которыми понимаются алгоритмы совершения над множеством данных (арифметических или логических) [77] (2015).

ситуация — зафиксированное в определенный момент времени или в определенных условиях множество количественных характеристик (параметров) сложившейся обстановки [77] (2015).

4.3.5.3. Разработка программного обеспечения

4.3.5.3.1. Производство сложных программных продуктов

программная инженерия — область компьютерной науки и технологии, занимающаяся построением больших и сложных программных комплексов для ЭВМ, требующих участия больших коллективов разработчиков различных специальностей и квалификаций.

Такие системы существуют и применяются долгие годы, развиваясь от версии к версии, претерпевая множество изменений, улучшение существующих функций, добавление новых или удаление устаревших

возможностей, адаптацию для работы в новой среде, устранение дефектов и ошибок.

Суть методологии программной инженерии состоит в использовании систематизированного, научного и предсказуемого процесса планирования, проектирования, производства и сопровождения сложных программных продуктов [134] (2011).

качество функционирования — совокупность свойств, определяющих пригодность продукта для обеспечения надежного и своевременного представления информации потребителю (или системе) для ее дальнейшего использования по назначению [134] (2011).

4.3.5.3.2. Автоматизированное перепроектирование процессов управления

автоматизированное перепроектирование процессов управления (АППУ) — кардинальное улучшение количественных и качественных показателей эффективности управления путем замены старых методов управления на новые.

Под кардинальным понимается улучшение на порядок, что позволяет добиться не менее чем 90%-го сокращения стоимостных или временных затрат либо такого же повышения качества.

Основные отличия автоматизированного перепроектирования процессов управления от традиционного подхода заключаются в следующем.

Во-первых, несколько работ объединяются в одну, т.е. создается команда, которая несет ответственность за весь процесс. Сравнительные оценки, выполненные организациями, прошедшими перепроектирование, показывают, что при этом уменьшается число исполнителей и примерно в 10 раз сокращается время («горизонтальное сжатие процесса»). Снижается количество ошибок, улучшается управляемость за счет уменьшения численности исполнителей и четкого разграничения ответственности между ними.

Во-вторых, исполнители принимают решения самостоятельно, вследствие чего происходит «вертикальное сжатие процессов» и, как результат, уменьшаются временные задержки, снижается стоимость, ускоряется реакция на запросы заказчика и повышаются полномочия исполнителей.

В-третьих, шаги процесса выполняются в естественном порядке. При перепроектировании происходит отказ от линейного упорядочения работ, свойственного традиционному подходу: там, где это возможно, работы выполняются параллельно, а значит, уменьшается время, которое тратится на устранение несоответствий между предыдущими и последующими шагами процесса.

В-четвертых, работа выполняется там, где это целесообразно. В традиционных системах управления работа организуется вокруг специалистов, сгруппированных в тематические подразделения (вычислительный центр, оперативный отдел и т.п.), и процесс затрагивает несколько подразделений, взаимодействующих друг с другом в письменной форме. Перепроектирование устраняет излишнюю интеграцию, что позволяет повысить эффективность.

В-пятых, уменьшается количество проверок и управляющих воздействий, которые, как показывает практика, непроизводительны и стоимость которых довольно часто превосходит стоимость потерь из-за их отсутствия. Поэтому задача перепроектирования заключается в том, чтобы осуществлять проверки и управляющие воздействия только в той мере, в которой это экономично и целесообразно.

В-шестых, преобладает смешанный (централизованный и децентрализованный) подход. Современные технологии позволяют органу управления действовать на уровне подразделений полностью автономно (децентрализованно), сохраняя при этом возможность пользования централизованными данными. Таким образом, устраняются бюрократические промежуточные звенья и повышается качество управления.

В ходе автоматизированного перепроектирования процессов управления должна быть создана оптимальная структура организации и разработаны алгоритмы деятельности ее подразделений и должностных лиц, ориентированные на достижение главной задачи — реализацию заданных функций управления (производство конечной продукции). Основные составляющие автоматизированного перепроектирования процессов управления — структурно-функциональный анализ, оценка сбалансированности загрузки подразделений, унификация описания продукции на всех этапах ее жизненного цикла, синтез оптимальной структуры и алгоритмов деятельности [91] (2000).

4.3.6. Защита информации

4.3.6.1. Информационная безопасность

информационная безопасность страны — одна из важных составляющих ее национальной безопасности, оказывающая существенное влияние на защиту национальных интересов страны в различных сферах жизнедеятельности общества и государства[45] [177] (2015).

информационная безопасность — состояние защищенности информации в АСУ войсками (силами) от внутренних и внешних деструктивных воздействий [64] (2006).

информационное право — политика и право, считающиеся относительно самостоятельными формами общественного сознания, взаимосвязаны таким образом, что приоритет всегда остается за политическими новациями. Правовые нормы (институты) лишь закрепляют их в соответствующих областях деятельности людей, причем в рамках легитимного политического процесса все последующие изменения, затрагивающие какой-либо предмет правового регулирования, неизбежно будут влиять на развитие законодательного фундамента. Это в полной мере касается положений Доктрины информационной безопасности РФ, которые ввиду своей масштабности и актуальности призваны, на наш взгляд, составить основу новой отрасли права — информационного права [111] (1998).

4.3.6.1.1. Угрозы информационной безопасности вооружения и военной специальной техники, укомплектованных электронной компонентной базой иностранного производства

электронная компонентная база в вооружении и военной специальной технике — использование современных и перспективных схем (больших и сверхбольших интегральных схем, 3D-схем и т.д.), разработанных или изготовленных за рубежом, таит в себе высокий

[45] Военная доктрина Российской Федерации.

риск: программные и аппаратные трояны, содержащиеся в них, могут вызвать сбой или отказ в функционировании техники.

По мере дальнейшего роста сложности и развития функциональных возможностей микроэлектроники (прежде всего за счет интеграции на одном кристалле или в одном корпусе приемо-передатчиков, приемных устройств, антенн, устройств обработки и выделения сигналов и т.д.) опасность появления несанкционированного воздействия в изделиях иностранного производства будет только возрастать. Эту вероятность нужно обязательно учитывать, комплексно решая проблему обеспечения информационной безопасности данных изделий при создании современных и перспективных средств вооружения и военной техники [22] (2013).

аппаратный троян — внесенные в микросхему функциональные объекты (блоки), которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации операций, позволяющих осуществлять несанкционированное воздействие как на саму микросхему, так и на обрабатываемую информацию.

Такой троян состоит из двух составляющих — активатора (триггера), обеспечивающего обнаружение выполнения условия для срабатывания и блока «полезной нагрузки-схемы», выполняющей по сигналу активатора запланированные действия.

Для аппаратуры в составе объекта военной техники возможны два основных сценария воздействия аппаратных троянов:

— отключение или ухудшение характеристик микроэлектроники, входящей в состав аппаратуры (например, отключение блока навигации или передача неправильных координат у современного самолета может привести к срыву выполнения боевой задачи или даже к катастрофическим последствиям — потере боевой единицы и гибели пилотов);

— установление скрытого канала утечки данных или активация других вредоносных схем (например, в системе связи такой канал может грозить утечкой конфиденциальной информации) [22] (2013).

инвазивные методы — методы выявления аппаратных троянов, предполагающие выполнение процедур обратного проектирования.

Как показывают эксперименты, инвазивные методы весьма трудоемки и малоэффективны при технологических нормах менее 0,18 мкм или 180 нм [22] (2013).

неинвазивные методы — методы выявления аппаратных троянов, не использующие прямой доступ к кристаллу микроэлектроники, а работающие с ней как с черным или серым ящиком.

Перспективная группа методов по выявлению аппаратных троянов использует внешние проявления наличия дополнительной вредоносной схемы и методики исследования по побочным каналам. Так как вредоносная схема в процессе работы устройства потребляет и выделяет энергию, то по дополнительному энергопотреблению, выделению тепловых и электромагнитных волн существует достаточно высокая вероятность ее обнаружения.

Для обнаружения постоянно работающих троянов методы исследования по побочному каналу излучения рекомендуется применять в совокупности с методами логического тестирования, в том числе для последующего проведения корреляционного анализа [22] (2013).

4.3.6.2. Защита информации при ведении боевых действий

защита информации при ведении боевых действий — комплекс мероприятий, эффективность которого, с одной стороны, зависит от усилий и затрат наших войск (сил) в ходе его реализации, а с другой — от условий обстановки, действий противника по хищению, уничтожению, потере, сокрытию, искажению, разглашению, фальсификации, компрометации истинной информации, используемой в процессе управления нашими войсками и оружием, а также по распространению и внедрению дезинформации.

Как показывают опыт учений и результаты математического моделирования наступательной операции оперативно-стратегического объединения Сухопутных войск, затраты наших войск (сил) на проведение мероприятий по защите информации могут быть в значительной степени определены заблаговременно путем тщательного изучения разведдоступности объектов наших систем управления, статистики по выходу из строя АСУ и вычислительной техники, ошибкам обслуживающего персонала и т.п. и противопоставления им соответствующих мероприятий, нейтрализующих выявленные каналы потери информации [58] (1998).

меры по обеспечению кибербезопасности — защита компьютерных сетей, в том числе военного назначения, от проникновения компьютерных взломщиков [164] (2009).

проблемы защиты информации в системах управления — для определения таких проблем необходимо выявить угрозы безопасности информации по степени их влияния на обеспечение информационного превосходства на поле боя.

Первая проблема заключается в существующей структуре систем управления войсками и оружием. Управление осуществляется только иерархически, по видам и родам войск и не соответствует межвидовому (и межродовому) характеру современных военных (боевых) действий и их скоротечности. Существующие автоматизированные системы управления и связи морально и технически устарели, обладают низкой устойчивостью, пропускной способностью, разведзащищенностью и не обеспечивают:

— своевременное автоматизированное доведение информации в цикле управления (кроме стратегических ядерных сил);

— межвидовое информационно-техническое взаимодействие, а также управление оружием на базе интегрированной разведывательной информации и обмен данными между системами разведки, навигации, целеуказания и поражения (подавления) в реальном масштабе времени.

Вторая проблема заключается в превосходстве средств технической разведки ведущих зарубежных государств, что обеспечивает им преимущество в определении источника, факта передачи информации и ее содержания и, как следствие, во вскрытии состава и топологии системы управления. На информационное противоборство ориентированы спутники двойного назначения орбитальной группировки, система радиоразведки и мониторинга радиообстановки, различные системы визуального, радиоэлектронного и оптического наблюдения.

Среди проблем защиты информации на первый план выступает проблема защиты информации **от несанкционированного использования**. Объясняется это повышенной уязвимостью информации в ЛВС штабов, т.е. наличием сравнительно широких возможностей скрытого доступа к ней. Анализ процесса защиты информации показывает, что основными способами защиты информации от несанкционированного доступа, которые могут быть использованы в ЛВС штабов, служат препятствие, управление, преобразование (шифрование), регламентация, принуждение, побуждение, позволяющие в определенной мере

снизить вероятность утечки информации за счет несанкционированного доступа посредством использования различных средств и методов защиты.

Еще одна существенная проблема обеспечения защиты информации — необходимость **передачи по каналам связи информации различной степени секретности**, требующей сохранения ее конфиденциальности и подлинности. Эффективно эти задачи могут быть решены только средствами криптографической защиты информации [212] (2012).

4.3.6.2.1. Обеспечение защиты информации в АСУ войсками и оружием

безопасность информации в АСУ — защищенность содержательной информации от искажения при переработке, разрушения при эксплуатации, раскрытия (утечки) и модификации при несанкционированном доступе и использовании, т.е. обеспечение внешнего качества содержательной информации при генерации (измерении и др.), преобразовании и коммуникации [137] (1998).

достоверность информации в АСУ — соответствие в пределах заданной точности реальных информационных единиц (символов, знаков, записей, сообщений, программ, документов и т.д. — информационных массивов) их истинному значению и отсутствие ошибок в переработке информации [137] (1998).

конфиденциальность информации в АСУ — статус, предоставленный информационным массивам [137] (1998).

сохранность информации в АСУ — готовность определенных информационных массивов к целевому применению и способность обеспечивать постоянное наличие и своевременное предоставление массивов, необходимых для автоматизированного решения целевых и функциональных задач АСУ [137] (1998).

4.3.7. Оценка эффективности АСУВ

эффективность системы — главная, основная характеристика качества, полезности системы.

При этом эффективность выступает как самая общая, полная, основная характеристика системы, которая качественно или количественно определяет ее способность выполнять свою основную функцию, способствующую достижению главной цели ее применения или функционирования. В соответствии с основной целью функционирования систем различают оперативно-тактическую, экономическую, техническую, социальную и другие виды эффективности систем [109] (2004).

показатель эффективности системы — численная мера или характеристика, которая количественно характеризует степень достижения системой цели своего функционирования.

Иногда это может быть количественная оценка свойства, выбранного в качестве характеристики эффективности системы.

При этом выбор или формулировка показателей эффективности АСУВ является достаточно сложной теоретической и практической задачей. Во-первых, желательно иметь один обобщенный показатель эффективности, соответствующий основной цели создания и применения АСУВ. Во-вторых, такой показатель складывается из множества показателей, отражающих отдельные частные свойства, которые в разной степени и часто противоположно влияют на этот обобщенный показатель эффективности. В-третьих, в многофункциональных системах (а именно такой и является АСУВ) решается множество задач и реализуется множество функций, которые на различных этапах проектирования и функционирования имеют различную значимость и поэтому по-разному влияют на обобщенный показатель эффективности.

Показатели эффективности АСУВ должны отражать, с одной стороны, эффективность системы более высокого порядка, составной частью которой является АСУВ, а с другой — способность АСУВ осуществлять решение задач по обработке информации и управлению с требуемым качеством в заданном диапазоне условий применения рассматриваемой системы [109] (2004).

боевая эффективность АСУВ — способность АСУВ своевременно и высококачественно решать задачи по управлению войсками (силами) и средствами.

В качестве показателей боевой эффективности обычно используется математическое ожидание предотвращенного ущерба или математическое ожидание количества уничтоженных целей [109] (2004).

функциональная эффективность АСУВ — способность АСУВ обеспечить качественное выполнение управленческих функций, удобство работы должностных лиц органов и пунктов управления со средствами автоматизации.

Функциональная эффективность АСУВ показывает, насколько рациональны системотехнические решения, принятые при ее создании, а также технические и программные средства, используемые в ней.

К наиболее существенным частным показателям функциональной эффективности АСУВ, которые в наибольшей степени влияют на реализацию боевых возможностей войск (сил) и боевых средств, относятся: боевая готовность, емкость, пропускная способность, оперативность, качество решения задач управления, помехоустойчивость, живучесть, скрытность, мобильность, пределы работы [109] (2004).

боевая готовность АСУВ — степень соответствия АСУВ решению задач управления войсками (силами) и средствами в любой момент времени.

Количественно этот показатель оценивается временем перевода аппаратуры АСУВ из одной степени боевой готовности в другую, более высокую. Так как АСУВ предназначены для повышения эффективности боевого применения войск (сил) и боевых средств, то время перевода АСУВ в боевой режим не должно превышать времени перевода войск (сил, боевых средств) в готовность к ведению боевых действий (к участию в воздушной операции) [109] (2004).

емкость АСУВ — предельные возможности АСУВ по решаемым задачам управления войсками (силами) и боевыми средствами.

Она может оцениваться различными показателями по конкретным задачам управления. Так, емкость АСУВ по обработке информации характеризуются максимальным количеством целей, по которым одновременно может производиться прием, обработка и выдача информации. Емкость АСУВ может оцениваться максимальным количеством каналов одновременного наведения истребительной авиации или числом батарей, дивизионов зенитных управляемых ракет, которые могут управляться автоматизировано (или автоматически). Требования к емкости АСУВ в основном определяются организационно-штатной структурой войск и ожидаемым характером действий воздушного противника [109] (2004).

пропускная способность АСУВ — предельные информационные возможности АСУВ при решении задач управления с заданным качеством.

Количественно пропускная способность АСУВ может быть оценена циклом решения конкретных задач в единицу времени с определенной дискретностью и точностью [109] (2004).

оперативность АСУВ — быстродействие АСУВ, т.е. возможность системы реагировать на изменения боевой обстановки.

Количественно оперативность системы может быть оценена временными затратами боевого расчета командного пункта (должностных лиц органа управления) при решении управленческих задач (работное время). Чем меньше работное время, тем выше быстродействие системы, тем выше ее оперативность. Уменьшение составляющих работного времени без снижения качества решения задач является одним из важнейших направлений по повышению оперативности управления. Быстродействие системы зависит от степени автоматизации, уровня подготовки и слаженности боевых (оперативных) расчетов командного пункта и личного состава органов управления [109] (2004).

качество решения задач управления в АСУВ — возможности АСУВ решать поставленные задачи с требуемой полнотой, своевременностью, достоверностью и точностью.

Количественно этот показатель может выражаться значениями ошибок решения определенной задачи и вероятностью правильного ее решения [109] (2004).

помехоустойчивость АСУВ — способность АСУВ выполнять свои функции в условиях воздействия помех, умышленно создаваемых противником, а также естественных помех существования системы управления.

Помехоустойчивость АСУВ зависит от помехозащищенности источников информации, системы связи АСУВ и построения алгоритмов обработки информации и боевого управления в КСА. Основной показатель помехоустойчивости — заданная вероятность выполнения поставленных задач управления с использованием АСУВ при воздействии помех определенной интенсивности [109] (2004).

живучесть АСУВ — свойство АСУВ сохранять или быстро восстанавливать свою боевую способность по решению задач управления в сложных условиях боевой обстановки.

Она складывается из боевой устойчивости и эксплуатационной надежности.

В понятие «живучесть» могут входить и такие свойства АСУВ, как ее способность получать информацию от источников по различным заранее предусмотренным вариантам, а также сохранять возможность управления объектами в ходе боевых действий при изменении ими своего местоположения в ходе боевых действий. В целом живучесть АСУВ будет определяться живучестью самых уязвимых ее элементов с точки зрения способности их противостоять воздействию противника, а также степенью резервирования наиболее сложных элементов АСУВ в процессе ее функционирования [109] (2004).

боевая устойчивость АСУВ — способность АСУВ противостоять огневому воздействию противника, оценивается количественно вероятностью функционирования при выходе из строя отдельных ее элементов [109] (2004).

эксплуатационная надежность АСУВ — вероятность безотказной работы АСУВ в течение определенного времени, а также вероятностью ее восстановления в течение заданного промежутка времени [109] (2004).

скрытность АСУВ — способность АСУВ обеспечивать решение возложенных на нее задач при сохранении в тайне от противника циркулирующей в ней информации, структуры системы управления и места расположения элементов системы управления [109] (2004).

мобильность АСУВ — способность АСУВ к передвижению в составе войск, как в период подготовки, так и в ходе ведения боевых действий.

Мобильность АСУВ оценивается возможностью ее транспортировки железнодорожным, воздушным, морским (речным) транспортом, а также возможностью совершать передвижение автомобильным транспортом в походных порядках войск [109] (2004).

пределы работы АСУВ — предельные значения характеристик, обрабатываемых и отображаемых АСУВ объектов по дальности, высоте и скорости движения [109] (2004).

капитальные затраты — ассигнования на научно-исследовательские и опытно-конструкторские работы по созданию АСУВ (включая разработку технических и программных средств), на серийное производство и закупку технических и программных средств, на подготовку личного состава, на последующую модернизацию системы и ее элементов [109] (2004).

эксплуатационные затраты — расходы за весь срок эксплуатации системы, включая затраты на содержание обслуживающего персонала, ремонт технических средств, приобретение эксплуатационных и расходных материалов [109] (2004).

4.3.8. Принципы обобщения опыта применения АСУ

принцип объективности — обязывает всех участников процесса обобщения опыта применения АСУ и СА исходить из реальных условий обстановки, в которой используются системы и средства, и опираться на фактические и достоверные результаты. Его реализация исключает как завышение, так и занижение полученных данных, дает возможность выработки практических рекомендаций по применению АСУ и СА. Необходимо отметить, что в течение последних лет вопросы объективности в подходе к оценке результатов, достигнутых в сфере внедрения и функционирования АСУ и СА, как и в других областях деятельности личного состава, являлись предметом особого внимания [145] (1990).

принцип комплексности — предполагает всестороннее рассмотрение опыта применения АСУ и СА, а также изучение каждой системы и средства только во взаимной связи. Данный принцип позволяет решить вопрос о степени оптимальности включения их аппаратно-программных средств в управленческую деятельность командования и оперативного состава органов и пунктов управления, оценить, насколько полно подразделениям автоматизации штаба удалось добиться реализации интегрированных потенциальных возможностей применявшихся систем и средств в повышении качества выполнения задач войсками (силами). Его результаты дают возможность оценивать и степень эффективности работы органов и пунктов управления в комплексировании систем и средств автоматизации управления [145] (1990).

принцип непрерывности — представляет собой, по существу, требование к организации и планированию деятельности личного состава по обобщению имеющегося опыта применения АСУ и СА как к непрерывно протекающему процессу. Он должен развиваться в связи с совершенствованием систем и средств, опыт применения которых анализируется и обобщается. Формы и методы этого процесса могут изменяться, но цель и основное его содержание целесообразно сохранять [145] (1990).

принцип автоматизации — предусматривает широкое использование АСУ и СА для сбора, обработки, анализа, хранения и выдачи статистических данных об их функционировании за определенный период времени. В этом существенную роль играет общесистемное обеспечение АСУ. Реализация этого принципа позволит резко сократить трудозатраты личного состава при выполнении этих работ. Сейчас уже имеются определенные результаты в этом направлении. Так, разработаны алгоритм и программа автоматизированного учета расходования вычислительного ресурса ЭВМ или вычислительного комплекса. Это дает возможность оператору, используя указанные программные средства, автоматически получить следующие сведения: какое подразделение производило расчеты (номера задач), используемые при этом варианты и затраты машинного времени в течение определенного периода (недели, месяца, квартала и т.д.); кто и сколько раз делал запрос на выдачу справок данного содержания; время, затраченное на обеспечение пользователя, и др. [145] (1990).

принцип плановости — предполагает планомерность действий коллектива специалистов по обобщению опыта функционирования АСУ и СА, объединенных единой программой или планом. Важным моментом при разработке программ является выбор интервалов между снятием показателей с аппаратуры, накапливающей и обрабатывающей статистические данные о ходе применения АСУ и СА. Величина интервалов должна обеспечивать своевременное принятие мер по устранению обнаруженных недостатков и распространению опыта [145] (1990).

принцип нормативности — предусматривает использование при организации и реализации мероприятий по анализу и обобщению опыта АСУ и СА в нормативных документах. Они нормируют как сам процесс сбора, обработки и представления данных по опыту примене-

ния систем и средств, так и порядок их отчетности, нормативные вероятностно-временные характеристики, требования по обеспечению сохранности информации в АСУ и вычислительных центрах. Практическое использование этого принципа позволяет сравнивать достигнутое количественное значение показателей функционирования систем и средств автоматизации с нормой, установленной на данный период времени. Однако широкому его применению может препятствовать отсутствие в некоторых звеньях управления требуемого набора нормативов по использованию АСУ и СА. Следует также отметить, что многие подразделения автоматизации проявляют большую заинтересованность и постоянное стремление к подкреплению своей работы научно обоснованными и проверенными практикой нормативами [145] (1990).

принцип «от младшего к старшему» — принцип, при котором низший уровень управления выполняет работу раньше и представляет полученные результаты для обобщения и доклада вышестоящей инстанции. Не исключается, что старший уровень, используя возможности, обеспечивающиеся при использовании принципа автоматизации, может приступить к выполнению определенной части своей работы еще до получения соответствующего отчета от младшей инстанции [145] (1990).

ТЕМАТИЧЕСКИЙ ПЕРЕЧЕНЬ ТЕРМИНОВ

АЛФАВИТНЫЙ УКАЗАТЕЛЬ ТЕРМИНОВ

АЛФАВИТНЫЙ УКАЗАТЕЛЬ АББРЕВИАТУР ТЕРМИНОВ

Аббр.	Термин	С.
ЕРИП	единое разведывательно-информационное пространство	80
ЕСАР	единая система автоматизации расчетов	255
ЕСК ВН	единая система карт военного назначения	264
ЕСКК ОС и ВТИ	единая система классификации и кодирования оперативно-стратегической и военно-технической информации	37
ЕСУ ТЗ	Единая система управления тактического звена[1]	297
ЕСУ ТЗ	Единая система управления тактического звена[2]	298
ЕФП	единое функциональное пространство	306
ЗЦВ	знание-центрическая война	176
ИАСУ ВМФ	единая интегрированная автоматизированная система управления ВМФ	258
ИВ	информационная война[7]	95
ИГИС в ЕИП	интегрированная геоинформационная среда в едином информационном пространстве	362
ИИ СУВ	информационная инфраструктура системы управления войсками (силами)[2]	13
ИКИС	интегрированная компьютерная информационная сеть корабля	261
ИМС ВС РФ	информационно-моделирующая среда ВС РФ	334
ИМС	информационно-моделирующая среда	334
ИО	информационная операция[4]	134
ИО	информационная операция[7]	136
ИО	информационное оружие[4]	106
ИПД	информационное противодействие	107
ИП	информационное противоборство[6]	98
ИРЗ	информационно-расчетные задачи	335
ИРС ГШ	Информационно-расчетная система Генерального штаба	239
ИС ВС	информационная служба Вооруженных Сил	56
ИСПВД	интеллектуальная система поддержки военных действий	308
ИСППР	интеллектуальная система поддержки принятия решений	372
ИСППР	интеллектуальная система поддержки принятия решения	313
ИССПД	интегрированная система связи и передачи данных	82
ИТВ	информационно-техническое воздействие[2]	154
ИТКС	информационно-телекоммуникационная система	81
ИУО	информационно-ударная операция	137
ИУС ВН	информационно-управляющая система военного назначения	300
ИУС	информационно-управляющая система	187
ИЦВ	инфомационно-центрическая война	176
КАБЦКД	комплекс автоматизированной базы цифровых картографических данных	262
КАИС ВН	корпоративные автоматизированные информационные системы военного назначения	289
КВИ	компьютерные военные игры	277
КОУ	сетецентричный огневой, ударный контур	209

Аббр.	Термин	С.
КСБУ	командная система боевого управления	236
КУД	классификатор управленческой документации	35
КФОП	компьютерные формы оперативной подготовки[1]	276
КФОП	компьютерные формы оперативной подготовки[2]	276
КШММ РТВ	комплекс штабных математических моделей боевого применения радиотехнических войск	254
ЛВС	локальные вычислительные сети	91
ММО	математическая модель операции	278
МС	моделирующий стенд	352
МТМДКП	мобильный телемедицинский диагностический комплекс пациента	266
МФО	модель фронтовой операции	336
НАРМ ЛВ	носимое автоматизированное рабочее место лечащего врача	266
НИТ	новые информационные технологии	15
НКМКБ	носимый комплекс мониторинга кардиологических больных	266
НТФ	нормативно-технический фонд	53
ОБЭ	операция базовых эффектов	210
ОКТЭСП	Общероссийский классификатор технико-экономических и социальных показателей	35
ОМО	организационно-мобилизационные органы ВС РФ	271
ОФИС	оперативная фактографическая информационная система	256
ПБУ	пункты боевого управления	245
ПЦВ	платформо-центрическая война[2]	175
РЕ	расчетная единица	338
РИП	разведывательно-информационное пространство соединения	80
РМК	расчетно-моделирующие комплексы	335
РПС	разведывательно-поражающая система	310
САК РЗ	Система автоматического комплексирования расчетных задач	22
СИО БД	системы информационного обеспечения боевых действий	123
СМО	специальное математическое обеспечение[1]	331
СМПО АСУВ	специальное математическое и программное обеспечение АСУВ	332
СМПО	специальное математическое и программное обеспечение[1]	331
СМПО	специальное математическое и программное обеспечение[2]	332
СОА	сервис-ориентированная архитектура	289
СОД	система обработки документов	33
СОЗ	системы, основанные на знаниях	376
СППР	система поддержки принятия решений	312
СПС	правовые информационные системы (справочные правовые системы, справочно-правовые системы)	268
СЦВ	сетецентрическая война[7]	170
СЦВ	сетецентрическая война[8]	176
СЦО	сетецентрическая операция	207
СЦС	сетецентричная система	184

Аббр.	Термин	С.
СЭД МО РФ	автоматизированная информационная система электронного документооборота Министерства обороны Российской Федерации	35
ТСфВ	техносферная война	156
УАСУВ	универсальная автоматизированная система управления войсками	307
УПТК	унифицированные программно-технические комплексы	304
УСД	унифицированная система документации	35
ФБД	фактографическая база данных	54
ФМК	фактографическая медицинская книжка	267
ЦМ	Центр моделирования ВС РФ	274
ЦОД	центр обработки данных	290
ЦОП ВАГШ	Центр оперативной подготовки Военной академии Генерального штаба	274

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АВАКС	—	авиационная система дальнего радиоэлектронного обнаружения (AWACS, Airborne Warning and Control Sistem)
АИС	—	автоматизированная информационная система
АРМ	—	автоматизированное рабочее место
АС	—	автоматизированная система
АС ВН	—	автоматизированная система военного назначения
АСУ	—	автоматизированная система управления
АСУВ	—	автоматизированная система управления войсками (силами)
АСУС	—	автоматизированная система управления военной связью
БД	—	база данных
БЛА	—	беспилотный летательный аппарат
БМП	—	боевая машина пехоты
БПЛА	—	беспилотный летательный аппарат
БТР	—	бронетранспортер
БЭСМ	—	быстродействующая электронная счетная машина
в.	—	век
ВА	—	воздушная армия
ВАГШ	—	Военная академия Генерального штаба ВС РФ
ВВС	—	Военно-воздушные силы, военно-воздушные силы (зарубежных стран)
ВВСТ	—	вооружение, военная и специальная техника
ВВТ	—	вооружение и военная техника
ВДВ	—	Воздушно-десантные войска, воздушно-десантные войска (зарубежных стран)
ВКО	—	воздушно-космическая оборона
ВКС	—	Военно-космические силы (устар.)
ВМБ	—	военно-морская база
ВМС	—	военно-морские силы
ВМФ	—	Военно-Морской Флот, военно-морской флот (зарубежных стран)
ВС	—	Вооруженные Силы , вооруженные силы (зарубежных стран)
ВС РФ	—	Вооруженные Силы Российской Федерации
ВТИ	—	военно-техническая информация
ВТО	—	высокоточное оружие
ВЦ	—	вычислительный центр
г.	—	год (после обозначения года)
ГИС	—	геоинформационная система, географическая информационная система
ГЛОНАСС	—	российская глобальная навигационная спутниковая система
ГОЗ	—	Государственный оборонный заказ
ГОМУ	—	Главное организационно-мобилизационное управление Генерального штаба ВС РФ
ГОСТ	—	межгосударственный стандарт
ГОСТ Р	—	государственный стандарт Российской Федерации
ГОСТ РВ	—	государственный военный стандарт Российской Федерации

ГПВ	—	Государственная программа вооружения
ГШ	—	Генеральный штаб ВС РФ, главный штаб
ДА	—	дальняя авиация
ДПЛА	—	дистанционно-пилотируемый летательный аппарат
др.	—	другой, другие
ЕИП	—	единое информационное пространство
ЕС	—	единая система
ЕСКК	—	Единая система классификации и кодирования
ЕСУ	—	единая система управления
ЗАО	—	закрытое акционерное общество
ЗИП	—	запасные части, инструменты, принадлежности
ИАСУ	—	интегрированная автоматизированная система управления
и др.	—	и другие
ИЛО	—	информационное и лингвистическое обеспечение
им.	—	имени
ИПС	—	информационно-поисковая система
ИРС	—	информационно-расчетная система
ИС	—	информационная система
ИСЗ	—	искусственный спутник Земли
ИСО	—	Международная организация по стандартизации
ИТ	—	информационная технология
и т.д.	—	и так далее
ИТКС	—	информационно-телекоммуникационная система
и т.п.	—	и тому подобное
КБ	—	конструкторское бюро
КВ	—	короткие волны; коротковолновый
КНР	—	Китайская Народная Республика
КНШ	—	комитет начальников штабов
КОУ	—	огневой, ударный контур
КП	—	командный пункт
КСА	—	комплекс средств автоматизации
КШМ	—	командно-штабная машина
лат.	—	латинский
ЛВС	—	локальная вычислительная сеть
ЛПР	—	лицо, принимающее решение
млн	—	миллион
млрд	—	миллиард
МО РФ	—	Министерство обороны Российской Федерации
МЭК	—	Международная электрическая комиссия
НАСА	—	Национальное управление по аэронавтике и исследованию космического пространства
НАТО	—	Организация Североатлантического договора
НИИ	—	научно-исследовательский институт
НИО	—	научно-исследовательская организация
НИОКР	—	научно-исследовательские и опытно-конструкторские работы
НИР	—	научно-исследовательская работа
НИУ	—	научно-исследовательское учреждение

НПО — научно-производственное объединение
НСИ — нормативно-справочная информация
ОАО — открытое акционерное общество
ОВА — Общевойсковая академия ВС РФ
ОВС — Объединенные вооруженные силы
ОВУ — органы военного управления, орган военного управления
ОКР — опытно-конструкторская работа
ОМО — организационно-мобилизационные органы
ОМП — оружие массового поражения
ООН — Организация Объединенных Наций
ОПК — оборонно-промышленный комплекс
ОС — операционная система
ОСПО — общесистемное программное обеспечение
ПВО — противовоздушная оборона
ПО — программное обеспечение
ПОЗ — подвижный отряд заграждения
ПУ — пункт управления
ПЭВМ — персональная электронная вычислительная машина
РАН — Российская академия наук
РВиА — ракетные войска и артиллерия
РВСН — Ракетные войска стратегического назначения
ред. — редакция
РЗ — расчетная задача
РСЗО — реактивная система залпового огня
РФ — Российская Федерация
РХБЗ — радиационная, химическая и биологическая защита
РЭБ — радиоэлектронная борьба
РЭП — радиоэлектронное подавление
с. — страница
СА — средства автоматизации
СВ — Сухопутные войска, сухопутные войска (зарубежных стран)
см. — смотри
СМИ — средства массовой информации
СМО — специальное математическое обеспечение
СМПО — специальное математическое и программное обеспечение
СПО — специальное программное обеспечение
СССР — Союз Советских Социалистических Республик
ст. — статья
СУБД — система управления базами данных
СЦВ — сетецентрическая война, сетецентричная война
СЦС — сетецентрическая система, сетецентричная система
США — Соединенные Штаты Америки
СЯС — стратегические ядерные силы
ТВД — театр военных действий
ТЗ — тактическое звено
ТТЗ — тактико-техническое задание
УКВ — ультракороткие волны, ультракоротковолновый

УСД	—	унифицированная система документации
УФД	—	унифицированная форма документа
ФГУП	—	федеральное государственное унитарное предприятие
ЦВКГ	—	центральный военный клинический госпиталь
ЦНИИ	—	центральный научно-исследовательский институт
ЦОП	—	центр оперативной подготовки
ЭВМ	—	электронная вычислительная машина
DNS	—	Domain Name System (доменная система именования)
GPS	—	Global Positioning System (система глобального позиционирования)
IEEE	—	The Institute of Electrical and Electronics Engineers, Inc. (Институт инженеров по электротехнике и радиоэлектронике, США)
NNEC	—	NATO Network Enabled Capabilities
USB	—	Universal Serial Bus (универсальная последовательная шина)
WINS	—	Windows-Internet Naming Service (служба имен в интернете для Windows)

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аблов И.В. Концепция построения информационно-аналитической системы для углубленной экспертизы диссертационных работ // Военная мысль. — 2016. — № 1. — С. 44—52.

2. Авдонин И.В. Использование автоматизированных рабочих мест органами военной юстиции при раскрытии и расследовании преступлений // Военная мысль. — 2014. — № 1. — С. 34—43.

3. Агеев Н.В. Почему и как происходит искажение истории // Военная мысль. — 2006. — № 9. — С. 59—65.

4. Акулинчев А.Б. Проблемы цифровизации военных сетей связи и пути их решения // Военная мысль. — 2006. — № 9. — С. 76—80.

5. Александров А.Е. О перспективах реализации сетецентрических концепций // Военная мысль. — 2014. — № 5. — С. 18—25.

6. Андреев В.Г. Оружие и война: новые тенденции развития // Военная мысль. — 1999. — № 3. — С. 49—53.

7. Андрийчук В.П. Система подготовки РВиА по стрельбе и управлению огнем в условиях единого информационного пространства // Военная мысль. — 2014. — № 1. — С. 10—17.

8. Антонович П.И. О сущности и содержании кибервойны // Военная мысль. — 2011. — № 7. — С. 39—46.

9. Асеев А.А., Дудник Б.Я., Кулешов И.А. Проблемы организации военной связи // Военная мысль. — 2005. — № 2. — С. 31—35.

10. Ахмадишин И.Н., Баранюк В.В. Организационные вопросы создания информационной службы ВС РФ // Военная мысль. — 2003. — № 4. — С. 45—49.

11. Ахмадишин И.Н., Тютюнников Н.Н., Баранюк В.В. К вопросу построения системы автоматизации документооборота // Военная мысль. — 1996. — № 1. — С. 55—57.

12. Бабич В.В. Как не дать командиру заблудиться в едином информационном пространстве тактического звена // Военная мысль. — 2011. — № 12. — С. 56—71.

13. 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.

14. Балыбин В.А., Донсков Ю.Е., Бойко А.А. О терминологии в области радиоэлектронной борьбы в условиях современного информа-

ционного противоборства // Военная мысль. — 2013. — № 9. — С. 28—32.

15. Баранюк В.В. Единое информационное пространство ВС РФ: проблемы создания // Военная мысль. — 2003. — № 3. — С. 36—38.

16. Баранюк В.В. Основные направления создания единого информационного пространства ВС РФ // Военная мысль. — 2004. — № 11. — С. 29—34.

17. Баранюк В.В., Ахмадишин И.Н. Проблемы построения Единого информационного пространства Вооруженных Сил Российской Федерации и возможные пути их решения // Военная мысль. — 2013. — № 12. — С. 66—71.

18. Барвиненко В.В. Об автоматизации управления группировками Вооруженных Сил // Военная мысль. — 1999. — № 2. — С. 26—29.

19. Барынькин В.М. Проблемы развития системы управления на современном этапе // Военная мысль. — 1996. — № 4. — С. 29—32.

20. Беднов Г.П., Лазарев А.В., Москвич Г.Е. Некоторые аспекты уточнения понятий военного искусства // Военная мысль. — 2007. — № 7. — С. 14—22.

21. Безуглый А.С., Гавриленко С.П. Об информационном моделировании в АСУВ // Военная мысль. — 1994. — № 5. — С. 29—33.

22. Белов Е.Н., Пономарев А.А., Семенов А.В., Федорец В.Н. Угрозы информационной безопасности вооружения и военной специальной техники, укомплектованных электронной компонентной базой иностранного производства // Военная мысль. — 2013. — № 12. — С. 35—43.

23. Белоконь С.П., Шиманский М.В. Военная организация Союзного государства // Военная мысль. — 2006. — № 2. — С. 19—25.

24. Бирюков В.В. Проблемы управления информатизацией ВС РФ // Военная мысль. — 1999. — № 4. — С. 35—41.

25. Бобков Ю.Я., Тютюнников Н.Н., Баранюк В.В. О построении единой системы классификации информации МО РФ // Военная мысль. — 1996. — № 6. — С. 48—53.

26. Бобошко А.А., Муравьев Н.Л., Пономарев С.Ю. Основные проблемы автоматизации организационно-мобилизационных органов ВС РФ // Военная мысль. — 1999. — № 6. — С. 50—53.

27. Богданов А.Е., Попов С.А., Иванов М.С. Перспективы ведения боевых действий с использованием сетецентрических технологий // Военная мысль. — 2014. — № 3. — С. 3—12.

28. Бородакий Ю.В. Развитие методологических основ построения информационно-управляющих систем военного назначения // Военная мысль. — 2009. — № 6. — С. 33—41.

29. Бреслер И.Б. Некоторые концептуальные подходы к построению современной АСУ авиацией // Военная мысль. — 2008. — № 9. — С. 27—30.

30. Буренов В.М., Мельников И.Д. Информационное обеспечение автоматизированных систем обоснования перспектив развития ВВТ // Военная мысль. — 2002. — № 5. — С. 42—46.

31. Буренок В.М. Совершенствование информационного обеспечения деятельности Вооруженных Сил Российской Федерации // Военная мысль. — 2006. — № 9. — С. 28—31.

32. Буренок В.М., Горчица Г.И., Ищук В.А., Цырендоржиев С.Р. Проблемные вопросы моделирования военных действий в целях создания перспективных систем вооружения // Военная мысль. — 2015. — № 11. — С. 34—45.

33. Вайнер А.Я. О противоборстве в сфере управления // Военная мысль. — 1990. — № 9. — С. 18—23.

34. Военная политика Российской Федерации в области международной информационной безопасности: региональный аспект // Военная мысль. — 2007. — № 2. — С. 32—40.

35. Военная политика Российской Федерации в области обеспечения международной информационной безопасности / И.Н. Дылевский, С.А. Комов, С.В. Коротков, С.Н. Родионов, А.В. Федоров // Военная мысль. — 2006. — № 4. — С. 2—7.

36. Военно-политические аспекты государственной политики Российской Федерации в области международной информационной безопасности / И.Н. Дылевский, В.О. Запивахин, С.А. Комов, А.Н. Петрунин, В.П. Эльяс // Военная мысль. — 2015. — № 1. — С. 11—17.

37. Воробьев И.Н. Информационно-ударная операция // Военная мысль. — 2007. — № 6. — С. 14—21.

38. Воробьев И.Н. О тактике // Военная мысль. — 2002. — № 1—6; 2003. — № 1—12.

39. Воробьев И.Н., Киселев В.А. Военная наука на современном этапе // Военная мысль. — 2008. — № 7. — С. 26—31.

40. Воробьев И.Н., Киселев В.А. Кибернетика в системе сетецентрических действий // Военная мысль. — 2012. — № 4. — С. 17—25.

41. Воробьев И.Н., Киселев В.А. Киберпространство как сфера непрямого вооруженного противоборства // Военная мысль. — 2014. — № 12. — С. 21—28.

42. Воробьев И.Н., Киселев В.А. Направления развития тактики сетецентрических действий // Военная мысль. — 2014. — № 5. — С. 10—17.

43. Воробьев И.Н., Киселев В.А. От современной тактики к тактике сетецентрических действий // Военная мысль. — 2011. — № 8. — С. 19—27.

44. Воробьев И.Н., Киселев В.А. Стратегия непрямых действий в новом облике // Военная мысль. — 2006. — № 9. — С. 2—10.

45. Выпасняк В.И. О реализации сетецентрических принципов управления силами и средствами вооруженной борьбы в операциях (боевых действиях) // Военная мысль. — 2009. — № 12. — С. 23—30.

46. Выпасняк В.И., Гуральник А.М. Оценка состояния системы управления войсками в ходе операции (боя) // Военная мысль. — 2008. — № 7. — С. 32—41.

47. Выпасняк В.И., Гуральник А.М., Тиханычев О.В. Моделирование военных действий: история, современное состояние и перспективы развития // Военная мысль. — 2014. — № 7. — С. 28—37.

48. Выпасняк В.И., Калиновский Д.Б., Тиханычев О.В. Моделирование вооруженного противоборства: перспективы развития // Военная мысль. — 2009. — № 7. — С. 12—20.

49. Галимов Р.С. Обеспечение устойчивого управления войсками при ведении маневренной обороны // Военная мысль. — 2014. — № 6. — С. 26—32.

50. Глазов Б.И. Способ классификации и моделирования информационных отношений сотрудничества и соперничества // Военная мысль. — 1998. — № 1. — С. 48—55.

51. Голубев Ю.Н., Гринь В.Р. О некоторых способах трансформации военных знаний в исходные данные для проектирования информационной инфраструктуры системы управления войсками (силами) // Военная мысль. — 2010. — № 11. — С. 41—49.

52. Голубев Ю.Н., Гринь В.Р., Каргин В.Н. К вопросу об управлении качеством военно-научных знаний // Военная мысль. — 2014. — № 12. — С. 42—58.

53. Голубев Ю.Н., Гринь В.Р., Ширманов А.В. Терминологические заторы на путях военной информатизации // Военная мысль. — 2012. — № 6. — С. 44—53.

54. Голубев Ю.Н., Каргин В.Н. Военная системология и военная информатизация: единство концептуальных подходов // Военная мысль. — 2006. — № 6. — С. 75—80.

55. Голубев Ю.Н., Каргин В.Н. Информационные технологии в управлении войсками // Военная мысль. — 2005. — № 6. — С. 42—51.

56. Гончаров С.В., Артамонов Н.Ф. Достижение информационно-психологического превосходства в современных боевых действиях (по взглядам руководства армии США) // Военная мысль. — 2014. — № 6. — С. 61—69.

57. Горбачев Ю.Е. Сетецентрическая война: миф или реальность? // Военная мысль. — 2006. — № 1. — С. 66—76.

58. Гордиенко Д.В. Оценка эффективности защиты информации при управлении войсками (силами) и оружием оперативно-стратегических (оперативных) объединений // Военная мысль. — 1998. — № 2. — С. 33—38.

59. Грачев И.А. Принципы построения специального математического и программного обеспечения АСУ войсками (силами) // Военная мысль. — 2002. — № 6. — С. 64—68.

60. Грачев И.А. Специальное математическое и программное обеспечение автоматизированной системы управления: теоретический аспект // Военная мысль. — 2004. — № 7. — С. 25—28.

61. Грачев И.А., Каргин В.Н. Информационные технологии в автоматизированных системах военного назначения // Военная мысль. — 2001. — № 6. — С. 18—22.

62. Григорьев А.И. Информационные и коммуникационные технологии в деятельности военно-медицинской службы ВС РФ // Военная мысль. — 2011. — № 4. — С. 38—47.

63. Гринь В.Р. Вербальная модель инфосферы управления войсками (силами): ресурсный подход // Военная мысль. — 2008. — № 3. — С. 62—69.

64. Гринь В.Р. Качество и безопасность автоматизированных систем управления войсками (силами): единство целого и частного // Военная мысль. — 2006. — № 12. — С. 26—31.

65. Гринь В.Р., Козичев В.Н., Ширманов А.В. Проблемно-ориентированная обработка нормативно-технической информации // Военная мысль. — 2004. — № 2. — С. 21—24.

66. Грудинин И.В., Шапкин П.М. О проблеме информационного обеспечения управления огнем группировок войск ПВО СВ // Военная мысль. — 2007. — № 6. — С. 29—33.

67. Гуральник А.М. Геоинформационные системы: вопросы разработки // Военная мысль. — 2004. — № 6. — С. 23—27.

68. Деев В.В., Плюснин Л.Ю. Интеллектуальные системы, основанные на смыслах // Военная мысль. — 1999. — № 1. — С. 28—30.

69. Дежин Е.Н. Информационная война по взглядам китайских военных аналитиков // Военная мысль. — 1999. — № 6. — С. 73—76.

70. Деминюк А.В., Хамзатов М.М. «Молниеносная война» нового поколения: возможный сценарий // Военная мысль. — 2004. — № 10. — С. 74—78.

71. Довженко В.Н., Завгородний В.Н. Поддержка принятия решений при управлении войсками (силами) // Военная мысль. — 2014. — № 6. — С. 19—25.

72. Долбня А.Г., Гавриленко С.А., Искандеров Ю.М. Интеллектуализация автоматизированной системы управления связью ВМФ // Военная мысль. — 2004. — № 3. — С. 18—23.

73. Долгополов А.В. Основные подходы к совершенствованию организационной структуры органов управления межвидовыми группировками войск (сил) в современных условиях ведения военных действий // Военная мысль. — 2012. — № 3. — С. 34—41.

74. Долгополов А.В., Богданов С.А. Эволюция форм и способов ведения вооруженной борьбы в сетецентрических условиях // Военная мысль. — 2011. — № 2. — С. 49—58.

75. Донсков Ю.Е., Морареску А.Л., Панасюк В.В. К вопросу о дезорганизации управления войсками (силами) и оружием // Военная мысль. — 2017. — № 8. — С. 19—25.

76. Донсков Ю.Е., Никитин О.Г. Место и роль специальных информационных операций при разрешении военных конфликтов // Военная мысль. — 2005. — № 6. — С. 30—34.

77. Донсков Ю.Е., Никитин О.Г., Беседин П.Н. Роль интеллектуальных систем поддержки принятия решений при управлении радиоэлектронной борьбой в общевойсковых тактических формированиях // Военная мысль. — 2015. — № 10. — С. 33—40.

78. Донсков Ю.Е., Фомин В.В. Информационное превосходство: пути реализации в операциях // Военная мысль. — 2003. — № 11. — С. 57—61.

79. Донсков Ю.Е., Фомин В.В., Матвеев Д.С. Формирование группировок войск при подготовке и выполнении ими боевых задач в условиях сетецентризма // Военная мысль. — 2012. — № 8. — С. 14—21.

80. Донсков Ю.Е., Храмов В.Ю., Беседин П.Н. Интеллектуализация процессов управления РЭБ как один из основных путей повышения ее эффективности // Военная мысль. — 2008. — № 2. — С. 50—54.

81. Дульнев П.А., Ковалев В.Г., Ильин Л.Н. Асимметричное противодействие в сетецентрической войне // Военная мысль. — 2011. — № 10. — С. 3—8.

82. Дылевский И.Н., Запивахин В.О., Комов С.А., Коротков С.В., Кривченко А.А. О диалектике сдерживания и предотвращения военных конфликтов в информационную эру // Военная мысль. — 2016. — № 7. — С. 3—11.

83. Дылевский И.Н., Комов С.А., Петрунин А.Н. Об информационных аспектах международно-правового понятия «агрессия» // Военная мысль. — 2013. — № 10. — С. 3—12.

84. Дымов Н.Г. Основные направления совершенствования деятельности органов управления оперативного звена // Военная мысль. — 2005. — № 6. — С. 22—29.

85. Егоров А.А. О классификации математических моделей боевых действий (операций) объединения ВВС // Военная мысль. — 2004. — № 5. — С. 10—18.

86. Егоров А.А. Об оценке достоверности результатов моделирования боевых действий (операции) объединения ВВС // Военная мысль. — 2005. — № 1. — С. 60—65.

87. Елисеев Н.И., Финько О.А. Теоретические аспекты развития системы электронного документооборота Министерства обороны Российской Федерации // Военная мысль. — 2015. — № 7. — С. 55—72.

88. Зайцев И.В., Молев А.А. Системы военной радиосвязи стран НАТО и направления их развития // Военная мысль. — 2014. — № 10. — С. 65—73.

89. Зоткин С.А., Зайчик Е.М., Кубасов И.А. К вопросу о стереологическом анализе операционного направления при управлении войсками // Военная мысль. — 2001. — № 4. — С. 24—30.

90. Зоткин С.А., Зайчик Е.М., Кубасов И.А. О применении геоинформационных технологий в управлении войсками (силами) // Военная мысль. — 1999. — № 2. — С. 34—36.

91. Иванов А.А. Информатизация Вооруженных Сил: проблемы и пути их решения // Военная мысль. — 2000. — № 2. — С. 29—34.

92. Ильин Л.Н., Ковалев В.Г., Муратханов А.С. Ориентиры для создания вооружения и военной техники сухопутных войск // Военная мысль. — 2011. — № 4. — С. 31—37.

93. Казарин Л.С. Характер войны как категория военной науки // Военная мысль. — 2002. — № 6. — С. 15—18.

94. Казарьян Б.И. О реализации технологий интеллектуализированного управления в системах автоматизации управления войсками и оружием // Военная мысль. — 2010. — № 10. — С. 20—27.

95. Казарьян Б.И. Операции, боевые действия, сетецентричная война // Военная мысль. — 2010. — № 2. — С. 25—37.

96. Калинин Ю.П., Озеранский Л.И. Информационные сети — перспектива автоматизации процессов управления войсками // Военная мысль. — 1997. — № 2. — С. 54—58.

97. Калистратов А.И. К вопросу о сетецентрических действиях в вооруженной борьбе будущего // Военная мысль. — 2008. — № 12. — С. 22—30.

98. Каратуев М.И. Автоматизация управления ракетными войсками и артиллерией: состояние и перспективы // Военная мысль. — 1999. — № 6. — С. 38—41.

99. Каргин В.Н., Козичев В.Н. Эволюция автоматизированных информационных систем в Вооруженных Силах // Военная мысль. — 2009. — № 7. — С. 29—39.

100. Карпов Е.А., Буренин Н.И., Зюзин Н.А. Единое военное информационное пространство: проблемы создания // Военная мысль. — 2004. — № 8. — С. 45—49.

101. Карулин В.П., Королев И.С. О системе технического обеспечения боевых действий РВСН // Военная мысль. — 2002. — № 4. — С. 62—68.

102. Кежаев В.А., Ефимов Н.Е., Васильковский С.А. Специальное математическое обеспечение процесса планирования огневого поражения противника // Военная мысль. — 1998. — № 1. — С. 56—61.

103. Кижицкий В.А., Завьялов В.Е., Саваренков С.М. Об уточнении содержания терминов «организация» и «управление» в терминологической системе теории военного управления // Военная мысль. — 2014. — № 10. — С. 59—64.

104. Климов С.М., Зорин Э.Ф., Половников А.Ю., Антонов С.Г. Основные направления обеспечения информационной безопасности ракетных комплексов стратегического назначения в условиях информационно-технических воздействий // Военная мысль. — 2016. — № 6. — С. 24—29.

105. Козирацкий Ю.Л., Будников С.А., Скопин Д.В. Основные аспекты контррадиоэлектронной борьбы // Военная мысль. — 2011. — № 10. — С. 9—15.

106. Козичев В.И., Каргин В.Н., Ширманов А.В., Голошев С.П. Перспективы создания корпоративных автоматизированных информационных систем военного назначения // Военная мысль. — 2015. — № 10. — С. 19—32.

107. Козичев В.Н. Интеллектуальные информационные системы: назначение и принципы создания // Военная мысль. — 2004. — № 7. — С. 22—25.

108. Колесниченко В.И. Военно-технические проблемы и основные принципы создания мобильных АСУ ВВС // Военная мысль. — 2004. — № 12. — С. 21—29.

109. Колесниченко В.И. Об оценке эффективности АСУ ВВС // Военная мысль. — 2004. — № 11. — С. 35—40.

110. Комов С.А. Информационная борьба в современной войне: вопросы теории // Военная мысль. — 1996. — № 3. — С. 76—80.

111. Комов С.А. О доктрине информационной безопасности Российской Федерации // Военная мысль. — 1998. — № 3. — С. 72—76.

112. Комов С.А. О способах и формах ведения информационной борьбы // Военная мысль. — 1997. — № 4. — С. 18—22.

113. Комов С.А., Коротков С.В., Дылевский И.Н. Об эволюции современной американской доктрины «информационных операций» // Военная мысль. — 2008. — № 6. — С. 54—61.

114. Комольцев В.Л., Михеев П.И. Об обеспечении информационной совместимости при создании АСУ РВ и А // Военная мысль. — 2004. — № 6. — С. 19—22.

115. Кондаков С.Ю., Никитин Н.Г. Опыт создания и применения в ВМФ информационных технологий управления // Военная мысль. — 2005. — № 10. — С. 18—22.

116. Кондратьев А.Е. Общая характеристика сетевых архитектур, применяемых при реализации перспективных сетецентрических концепций ведущих зарубежных стран // Военная мысль. — 2008. — № 12. — С. 63—74.

117. Кондратьев А.Е. Проблемные вопросы исследования новых сетецентрических концепций вооруженных сил ведущих зарубежных стран // Военная мысль. — 2009. — № 11. — С. 61—74.

118. Кондратьев В.В., Ничипор В.И., Костенко А.Н. Информационно-расчетное обеспечение управления войсками в условиях инфор-

мационной неопределенности // Военная мысль. — 2013. — № 11. — С. 21—34.

119. Копылов А.В. О слабых сторонах американской концепции «сетецентрических войн (операций)» // Военная мысль. — 2011. — № 7. — С. 53—62.

120. Копытко В.К., Шептура В.Н. Проблемы построения единого информационного пространства Вооруженных Сил Российской Федерации и возможные пути их решения // Военная мысль. — 2011. — № 10. — С. 16—26.

121. Кораблин В.В. Терминосистема — важнейший элемент научно-методического аппарата военно-научных исследований // Военная мысль. — 2009. — № 8. — С. 66—70.

122. Коржан Э.А., Крюков Д.М., Котенко Л.В. Социализация и воспитание курсантов в условиях военного вуза средствами информационных технологий // Военная мысль. — 2015. — № 7. — С. 73—78.

123. Костарев С.В., Ефремов О.Ю., Зверев С.Э. Концепция сетецентрических войн в свете доктрины «Единый взгляд 2020» // Военная мысль. — 2014. — № 1. — С. 58—64.

124. Костин Н.А. Общие основы теории информационной борьбы // Военная мысль. — 1997. — № 3. — С. 44—50.

125. Костров С.А., Бегларян С.Г. Геоинформационные системы в управлении войсками и силами воздушно-космической обороны // Военная мысль. — 2010. — № 3. — С. 34—38.

126. Кретов В.С., Пинчук И.С., Заварзин А.В. Использование геоинформационных систем при планировании и проведении миротворческих операций // Военная мысль. — 2001. — № 6. — С. 23—27.

127. Кудренко О.А., Морозов С.В. Направления развития методологии автоматизированной разработки оперативных документов в перспективных АСУ войсками (силами) // Военная мысль. — 2014. — № 7. — С. 46—51.

128. Кузнецов В.И., Донсков Ю.Е., Коробейников А.С. О соотношении категорий «радиоэлектронная борьба» и «информационная борьба» // Военная мысль. — 2013. — № 3. — С. 14—20.

129. Кузнецов В.И., Донсков Ю.Е., Никитин О.Г. К вопросу о роли и месте киберпространства в современных боевых действиях // Военная мысль. — 2014. — № 3. — С. 13—17.

130. Кузнецов Н.Ф., Заец О.Г. О живучести системы управления общевойскового формирования // Военная мысль. — 2014. — № 8. — С. 3—9.

131. Куликов В.А. Классификация оружия и военной техники: проблемы и пути решения // Военная мысль. — 2003. — № 8. — С. 31—43.

132. Лактионов В.И. Интеллектуальные технологии в информационно-аналитической деятельности органов военного управления: проблемы внедрения // Военная мысль. — 2002. — № 6. — С. 60—64.

133. Лимно А.Н., Крысанов М.Ф. Информационное противоборство и маскировка войск // Военная мысль. — 2003. — № 5. — С. 70—74.

134. Липаев В.В. Концепция производства сложных программных продуктов // Военная мысль. — 2011. — № 1. — С. 36—45.

135. Липаев В.В. Отечественные прототипы компьютерных телекоммуникационных сетей в системах ПВО в 50—60-е годы прошлого века // Военная мысль. — 2011. — № 10. — С. 27—35.

136. Липаев В.В. Первый радиолокационный узел с цифровой ЭВМ // Военная мысль. — 2013. — № 10. — С. 59—65.

137. Ловцов Д.А. Основы обеспечения защиты информации в АСУ войсками и оружием // Военная мысль. — 1998. — № 3. — С. 51—55.

138. Ляпин В.Р., Барвиненко В.В. Единая информационно-моделирующая среда в системах военного назначения // Военная мысль. — 2015. — № 4. — С. 72—78.

139. Ляпин В.Р., Зимин В.Н., Барвиненко В.В. О построении комплексов средств автоматизации в АСУ войсками (силами) для ведения сетецентрических действий // Военная мысль. — 2011. — № 11. — С. 54—61.

140. Малышев Л.И. Военная стратегия Российской Федерации в начале XXI века // Военная мысль. — 2007. — № 11. — С. 16—25.

141. Международный режим нераспространения информационного оружия: утопия или реальность? / И.Н. Дылевский, В.О. Запивахин, С.А. Комов, С.В. Коротков, А.Н. Петрунин // Военная мысль. — 2014. — № 10. — С. 3—12.

142. Меньшиков В.А., Тарасов И.В. Компьютерные военные игры в оперативной подготовке органов управления Военно-космических сил // Военная мысль. — 1997. — № 5. — С. 30—35.

143. Метлицкий Г.И., Зайцев Ю.Е. Совершенствование системы управления воинскими частями // Военная мысль. — 2008. — № 4. — С. 18—22.

144. Мигунов А.А. Тенденции китайской стратегии ведения информационной войны // Военная мысль. — 2008. — № 11. — С. 62—67.

145. Митрофанов В.В. Об опыте применения АСУ войсками (силами) // Военная мысль. — 1990. — № 12. — С. 40—43.

146. Михайловский А.Б., Сайфетдинов Х.И. Компьютерные формы обучения должностных лиц Национального центра управления обороной Российской Федерации // Военная мысль. — 2016. — № 5. — С. 57—62.

147. Михайловский А.В., Сайфетдинов Х.И. Оперативные основы создания перспективного облика системы управления Вооруженными Силами Российской Федерации // Военная мысль. — 2015. — № 11. — С. 12—16.

148. Молчанов Н.А. Информационный потенциал зарубежных стран как источник угроз военной безопасности РФ // Военная мысль. — 2008. — № 10. — С. 2—9.

149. Мордвинов В.Ф. Об информатизации системы военного образования // Военная мысль. — 2006. — № 4. — С. 25—28.

150. Морозов А.С. Состояние и перспективы развития системы управления Сухопутных войск // Военная мысль. — 2004. — № 1. — С. 14—22.

151. Морозов И.В., Баушев С.В., Каминский О.Э. О понятии «информационно-космическое обеспечение» // Военная мысль. — 2010. — № 4. — С. 35—40.

152. Морозов С. В., Кудренко О.А. О подходе к созданию единой стационарно-мобильной автоматизированной системы управления войсками и оружием объединенного стратегического командования // Военная мысль. — 2013. — № 3. — С. 32—38.

153. Морозов С.В., Кудренко О.А. Формализация боевых документов в автоматизированных системах управления войсками // Военная мысль. — 2009. — № 7. — С. 40—45.

154. Наговицин А.И. Нетрадиционный способ передачи информации в тактическом звене // Военная мысль. — 2006. — № 4. — С. 71—75.

155. Новожилова Е.О. Войны настоящего и будущего // Военная мысль. — 2011. — № 2. — С. 3—12.

156. Ночевкин В.Н. Принципы построения моделей закономерностей операций (боевых действий) // Военная мысль. — 1999. — № 3. — С. 42—45.

157. Ночевкин В.Н. Проблемы создания штабных информационных технологий принятия решения на операцию // Военная мысль. — 1999. — № 2. — С. 30—33.

158. Образцов П.И. Информационно-технологическое обеспечение учебного процесса в высшей военной школе // Военная мысль. — 2003. — № 8. — С. 22—26.

159. Омельченко Ю.И. О требованиях к информации в системе управления противовоздушной обороной // Военная мысль. — 2006. — № 2. — С. 9—14.

160. Опарин А.И. Информационное обеспечение морского технологического комплекса ВМФ для подводных работ // Военная мысль. — 2015. — № 7. — С. 51—54.

161. Операции в киберпространстве: вопросы теории, политики и права / И.Н. Дылевский, С.А. Комов, С.В. Коротков, А.Н. Петрунин // Военная мысль. — 2011. — № 8. — С. 72—78.

162. Орлянский В.И. Вооруженная и информационная борьба: сущность и взаимосвязь понятий и явлений // Военная мысль. — 2002. — № 6. — С. 42—47.

163. Орлянский В.И. Информационное оружие и информационная борьба: реальность и домыслы // Военная мысль. — 2008. — № 1. — С. 62—70.

164. Орлянский В.И. Некоторые проблемы теории и практики обмана противника // Военная мысль. — 2009. — № 6. — С. 51—59.

165. Орлянский В.И., Дульнев П.А., Костенко А.Н. Универсальная автоматизированная система управления войсками — принципиальное условие успешного ведения сетецентрических войн // Военная мысль. — 2012. — № 12. — С. 12—20.

166. Осетров А.В., Богданов С.А. Основные элементы научно-методического аппарата военно-теоретических исследований // Военная мысль. — 2008. — № 7. — С. 62—69.

167. Осипов П.А., Николенко Е.И., Орлов В.Н. О переводе системы связи ВС РФ на цифровые способы передачи информации // Военная мысль. — 2005. — № 4. — С. 73—77.

168. Панус В.С., Максименко Н.Т. Информационно-коммуникационные технологии и военное образование // Военная мысль. — 2009. — № 6. — С. 48—50.

169. Перов Е.А., Переверзев А.В. О перспективной цифровой системе связи Вооруженных Сил Российской Федерации // Военная мысль. — 2008. — № 3. — С. 7—11.

170. Пертушина Е.А. О некотором опыте использования цифровых классификаторов в Военной академии Генерального штаба ВС РФ // Военная мысль. — 2010. — № 6. — С. 75—77.

171. Пирумов В.С., Родионов М.А. Некоторые аспекты информационной борьбы в военных конфликтах // Военная мысль. — 1997. — № 5. — С. 45—49.

172. Половнев О.В., Расчислов А.Л. О повышении оперативности и качества организации и поддержания взаимодействия войск // Военная мысль. — 2013. — № 4. — С. 24—29.

173. Посадский А.А. Тактический Интернет // Военная мысль. — 2005. — № 7. — С. 12—14.

174. Протасов А.А., Соболевский В.А., Сухорутченко В.В. Планирование применения стратегических вооружений // Военная мысль. — 2014. — № 7. — С. 9—27.

175. Прудников Д.П. Государственная информационная политика в области обороны: исходное определение // Военная мысль. — 2008. — № 3. — С. 43—48.

176. Прудников Д.П. Информационное обеспечение как важнейший компонент военно-управленческой деятельности // Военная мысль. — 2008. — № 7. — С. 42—45.

177. Пузенькин И.В., Михайлов В.В. Роль информационно-психологических средств в обеспечении обороноспособности государства // Военная мысль. — 2015. — № 7. — С. 11—15.

178. Разроев Н.И., Мельников Г.Ф., Тимков Г.Н. Интегрирующая роль электронных карт в процессах автоматизированного управления обороной страны // Военная мысль. — 2016. — № 3. — С. 9—15.

179. Раскин А.В., Пеляк В.С., Вялов С.А. Концепция сетецентрической войны: за и против // Военная мысль. — 2012. — № 7. — С. 14—21.

180. Раскин А.В., Пеляк В.С. К вопросу о сетевой войне // Военная мысль. — 2005. — № 3. — С. 21—27.

181. Раскин А.В., Пеляк В.С. Сетецентрическая война — война информационной цивилизации // Военная мысль. — 2008. — № 4. — С. 78—80.

182. Рахманов А.А. Сетецентрические системы управления: закономерные тенденции, проблемные вопросы и пути их решения // Военная мысль. — 2011. — № 3. — С. 41—50.

183. Родионов М.А. К вопросу о формах ведения информационной борьбы // Военная мысль. — 1998. — № 2. — С. 67—70.

184. Родионов С.Н. Политика и информационная безопасность государства в условиях военных конфликтов // Военная мысль. — 2005. — № 6. — С. 16—21.

185. Рябчук В.Д. Проблемы военной науки и военного прогнозирования в условиях интеллектуально-информационного противоборства // Военная мысль. — 2008. — № 5. — С. 67—76.

186. Рябчук В.Д., Ничипор В.И. Проблемы теории и практики создания единой автоматизированной системы управления тактического звена // Военная мысль. — 2010. — № 5. — С. 55—60.

187. Рябчук В.Д., Ничипор В.И., Кондратьев В.В. Методологические аспекты совершенствования управления общевойсковыми тактическими формированиями с применением перспективных АСУ // Военная мысль. — 2009. — № 5. — С. 39—45.

188. Сайфетдинов Х.И. Информационное противоборство в военной сфере // Военная мысль. — 2014. — № 7. — С. 38—41.

189. Сайфетдинов Х.И. Компьютерные формы оперативной подготовки: проблемы совершенствования и пути их решения // Военная мысль. — 2004. — № 7. — С. 2—11.

190. Сайфетдинов Х.И. Реформирование боевой подготовки: компьютерные формы обучения // Военная мысль. — 1998. — № 4. — С. 12—16.

191. Сайфетдинов Х.И., Ещенко В.И. ФГУП «Концерн «Системпром» — 20 лет плодотворной работы в области автоматизации управления войсками (силами) // Военная мысль. — 2011. — № 7. — С. 72—78.

192. Сайфетдинов Х.И., Куляница А.Л., Деев В.В. Информатизация управления войсками и искусственный интеллект // Военная мысль. — 1997. — № 5. — С. 14—23.

193. Самарин А.Ю., Кнауэр Г.Э. К вопросу о формировании единого информационного пространства ВВС // Военная мысль. — 2004. — № 10. — С. 22—24.

194. Самохин В.Ф., Лукьянчик В.Н., Артюшенко А.Н. Перспективы создания военного (боевого) Интернета в рамках нового облика ВС РФ // Военная мысль. — 2011. — № 8. — С. 57—64.

195. Сапожинский В.А., Костяев Н.И. О совершенствовании АСУ тактического звена // Военная мысль. — 2002. — № 5. — С. 51—54.

196. Саушкин В.П. Комплекс штабных математических моделей боевого применения радиотехнических войск // Военная мысль. — 2003. — № 6. — С. 48—51.

197. Селезнев Н.В. Развитие полевой системы связи на основе новых телекоммуникационных технологий // Военная мысль. — 2008. — № 3. — С. 20—24.

198. Сердюков А.Н. Развитие методов и средств обеспечения войск цифровой информацией о местности // Военная мысль. — 2006. — № 5. — С. 26—29.

199. Скоков С.И., Выговский И.И. Проблемы и направления совершенствования автоматизированного управления подготовкой и ведением военных действий // Военная мысль. — 2011. — № 9. — С. 61—67.

200. Скоков С.И., Грушка Л.В. Влияние концепции сетецентризма на эволюцию и функционирование системы управления Вооруженными Силами Российской Федерации // Военная мысль. — 2014. — № 12. — С. 33—41.

201. Смирнов А.И. Разведывательное обеспечение тактических действий соединений Сухопутных войск // Военная мысль. — 2013. — № 9. — С. 20—27.

202. Соловьев И.В., Ваколюк О.П. Проблемы развития корабельных систем управления // Военная мысль. — 2001. — № 1. — С. 31—33.

203. Стародубцев Ю.И., Бухарин В.В., Семенов С.С. Техносферная война // Военная мысль. — 2012. — № 7. — С. 23—31.

204. Стрельцов А.А. Основные задачи государственной политики в области информационного противоборства // Военная мысль. — 2011. — № 5. — С. 18—25.

205. Суровикин С.В., Кулешов Ю.В. Особенности организации управления межвидовой группировкой войск (сил) в интересах комплексной борьбы с противником // Военная мысль. — 2017. — № 8. — С. 5—18.

206. Сухов А.В. Информационные технологии в эргасистемах военного назначения: классификационный аспект // Военная мысль. — 2007. — № 7. — С. 33—40.

207. Тасбулатов А.Б., Орлянский В.И. Разработка современной классификации видов и средств поражения — неотложная задача военной науки // Военная мысль. — 2007. — № 4. — С. 55—61.

208. Терехов В.И. Применение гибридных систем вычислительного интеллекта для выбора рационального варианта управленческого решения // Военная мысль. — 2009. — № 11. — С. 29—34.

209. Титлянов В.А., Софиенко А.Н., Смирнов М.Ю., Якушев А.А. Навигационные комплексы надводных кораблей с использованием элементов искусственного интеллекта // Военная мысль. — 2008. — № 8. — С. 45—52.

210. Тиханычев О.В. Системы поддержки принятия решений — перспективное направление развития автоматизации управления войсками (силами) // Военная мысль. — 2012. — № 8. — С. 45—51.

211. Тиханычев О.В. Субъективные аспекты применения математического моделирования военных действий в работе органов военного управления // Военная мысль. — 2011. — № 10. — С. 49—53.

212. Травников С.А., Руцкий А.Г. Некоторые проблемы защиты информации в системе управления войсками // Военная мысль. — 2012. — № 2. — С. 24—29.

213. Тютюнников Н.Н., Харитонов Л.А. Автоматизированная технология обработки мобилизационной информации // Военная мысль. — 1997. — № 6. — С. 25—30.

214. Фомин В.В., Матвеев Д.С., Зубцова Л.Ф. Сетевое моделирование боевых действий в современных войнах (вооруженных конфликтах) // Военная мысль. — 2012. — № 4. — С. 28—34.

215. Фролов Б.П. Российская Военная Энциклопедия // Военная мысль. — 2000. — № 5. — С. 74—77.

216. Хамзатов М.М. Влияние концепции сетецентрической войны на характер современных операций // Военная мысль. — 2006. — № 7. — С. 13—17.

217. Харченко Е.Б. Проблемы безопасности инфокоммуникационных систем Вооруженных Сил Российской Федерации // Военная мысль. — 2014. — № 11. — С. 14—19.

218. Хомутов А.В. Опыт и перспективы использования концепции единой информационно-коммуникационной сети в управлении войсками // Военная мысль. — 2015. — № 11. — С. 17—22.

219. Цыгичко В.Н. Методологические основания математического моделирования операций войск (сил) // Военная мысль. — 1997. — № 1. — С. 22—26.

220. Чебан В.В. Военная наука и новые угрозы военной безопасности // Военная мысль. — 2003. — № 2. — С. 60—65.

221. Чекинов С.Г., Богданов С.А. Начальные периоды войн и их влияние на подготовку страны к войне будущего // Военная мысль. — 2012. — № 11. — С. 14—27.

222. Чекинов С.Г., Богданов С.А. Развитие современного военного искусства с точки зрения военной системологии // Военная мысль. — 2015. — № 11. — С. 23—33.

223. Чекинов С.Г., Богданов С.А. Эволюция сущности и содержания понятия «война» в XXI столетии // Военная мысль. — 2017. — № 1. — С. 30—43.

224. Чельцов Б.Ф. Уточнение подходов к созданию системы воздушно-космической обороны государства в условиях сетецентричных войн будущего // Военная мысль. — 2008. — № 9. — С. 2—10.

225. Шакалов Д.В. Научно-методический аппарат обоснования требований к автоматизированной системе управления боевой подготовкой // Военная мысль. — 2017. — № 5. — С. 67—73.

226. Шестюк В.П. Актуальные проблемы обеспечения информационной безопасности Российской Федерации // Военная мысль. — 2003. — № 6. — С. 28—32.

227. Юсупов Р.М., Бакурадзе Д.В., Сугак В.П. О понятии «Устойчивость автоматизированного управления войсками (силами) и боевыми средствами» // Военная мысль. — 1990. — № 9. — С. 67—68.

Справочное издание

Н.Н. Тютюнников

ВОЕННАЯ МЫСЛЬ В ТЕРМИНАХ И ОПРЕДЕЛЕНИЯХ

В трех томах

Том 3

Информатизация Вооруженных Сил

Терминологический словарь

Издательство «Перо»
109052, Москва, Нижегородская ул., д. 29-33, стр. 15, ком. 536
Тел.: (495) 973-72-28, 665-34-36
Подписано в печать 08.02.2018. Формат 70×100/16.
Усл. печ. л. 38,35. Тираж 500 экз. Заказ № 075.
Отпечатано в ООО «Издательство «Перо»