DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

Сурма И.В., Анненков В.И., Карпов В.В., Моисеев А.В.

«СЕТЕЦЕНТРИЧЕСКОЕ УПРАВЛЕНИЕ»: СОВРЕМЕННАЯ ПАРАДИГМА РАЗВИТИЯ СИСТЕМ УПРАВЛЕНИЯ В ВООРУЖЕННЫХ СИЛАХ ВЕДУЩИХ ДЕРЖАВ МИРА

Аннотация: *В статье показано, что поиск эффективных методов управления и современное развитие информационных технологий привели к появлению новых управленческих парадигм, одной из которых является «сетецентрическое управление». Отмечается, что в концептуально-теоретическом плане сетецентрический подход в военном деле реализуется в виде системы, которая состоит из трех подсистем, имеющих структуру взаимно пересекающихся решеток (информационной подсистемы, сенсорной — разведывательной подсистемы и боевой подсистемы — подсистемы отдельных тактических подразделений и боевого управления), среди которых информационная решетка-подсистема пронизывает собой всю систему современного управления и составляет ее основу. Представлен сравнительный анализ классического и сетецентрического подходов к управлению и показан опыт его реализации в сфере военного искусства на примере ряда стран (США, Франции, Великобритании, Германии, Израиля и Китая). Система сетецентрического управления представляет собой сочетание заблаговременно созданных и развернутых разветвленных автоматизированных электронных сетей сбора и первичной обработки информации, узлов хранения и анализа информации, а также контуров управления и принятия решений, которые совокупными усилиями создают единое информационное и управленческое пространство, охватывающее все пространство управления. Основной идеей «сетецентрической войны» является интеграция всех сил и средств в едином информационном пространстве, позволяющая многократно увеличить эффективность их боевого применения за счет реализации синергетического эффекта. Внедрение сетевых технологий в военную сферу является действительно революционным шагом, направленным на повышение боевых возможностей вооруженных сил за счет оперативности и эффективности их применения.*

Ключевые слова: *сетецентрическое управление, НАТО, глобальная информационная решетка, сетецентрические войны, J-структуры, синергический эффект, сетецентризм, сетевые технологии, перспективные средства разведки, ООДА.*

Развитие информационных технологий и поиск эффективных методов управления привели к появлению новых управленческих парадигм, одной из которых является «сетецентрическое управление». Это понятие в настоящее время находит широкое освещение в научных изданиях и активно внедряется в практику решения задач управления в различных областях деятельности (военной, финансовой, производственной, проектной и др.). Вместе с тем до сих пор отсутствует общий взгляд на данное понятие. В связи с этим возникает потребность в формировании единого взгляда на понятие «сетецентрическое управление» в частности, и «сетецентризм» в целом. Необходимо привести систему понятий различных экспертов и специалистов в единую интегрированную понятийную систему.

Сравнительный анализ классического и сетецентрического подходов к управлению представлен на рис.1. Проведенный анализ позволил определить, что под *сетецентризмом* следует понимать *информатизацию вооруженных сил, предусматривающую целенаправленный процесс системной интеграции компьютерных средств, информационных и коммуникационных систем с целью получения новых общесистемных свойств, позволяющих более эффективно планировать, организовывать и вести управление военными операциями (боевыми действиями).*

Отметим, что одна из доминирующих корректных точек зрения базируется на утверждении: *в основе сетецентрической парадигмы лежит синергия.*

В обобщённом виде, система управления, в кибернетическом аспекте, состоит из следующих функциональных блоков: источник информации (датчик); блок управления; исполнительные органы. Естественно, что объект управления и внешняя среда наличествуют по умолчанию.

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

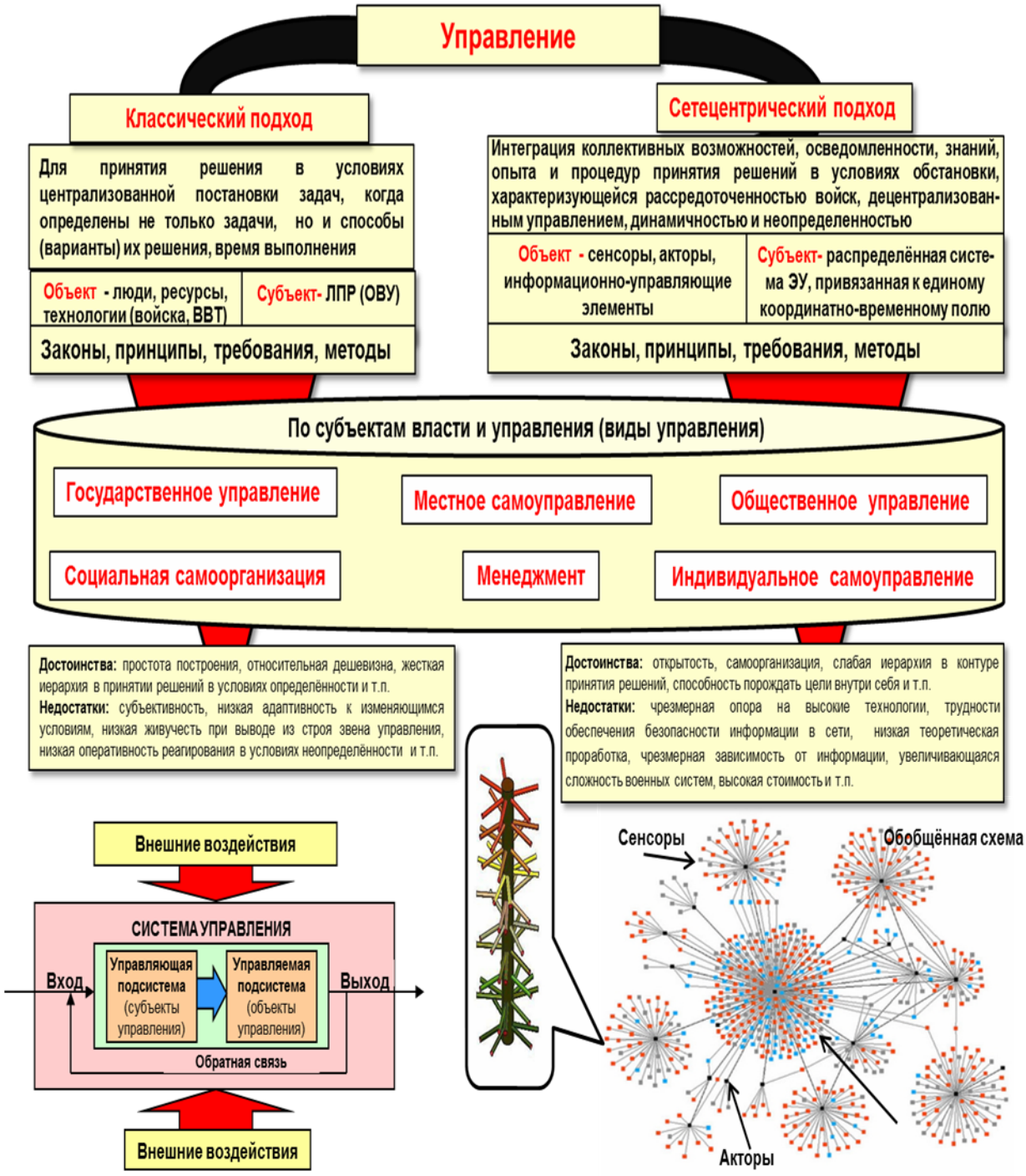

Рис.1. Классический и сетецентрический подходы к управлению

Источник информации (датчики, информационные агенты). В силу масштабности системы и её нестационарности, сенсорная решётка в общем виде не является нормализованным источником информации. Под нормальностью здесь понимается оптимальный уровень полноты и достоверности получаемых данных. С другой стороны, глобальность порождает потенциально высокий уровень информационной полноты и некоррелированности исходных данных, что создаёт предпосылки для проявления синергического эффекта — возможности восстановления пропущенной или искажённой информации.

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

Блок управления (лицо, принимающее решение, экспертный совет). В сетецентрической системе управления, этот модуль имеет специальную, многослойную структуру. Минимальная конфигурация — 3 слоя. Первый слой, обращённый к сенсорной решётке, состоит из лиц принимающих решения, специализирующихся в конкретных областях и вопросах. Они готовят информацию и формируют промежуточные решения для второго слоя — ответственного за тактические и стратегические решения. Третий слой на основе этих директив формирует оперативное управление, которое поступает на исполнительные органы. Естественно, что каждый из слоёв управления имеет доступ как к информационной решётке, так и к оконечным агентам. Подобная конфигурация позволяет принимать интегральное самосогласованное решение, которое опять же обладает высоким синергическим потенциалом в силу своей близости к оптимуму. Необходимо отметить, что реальные структуры управляющего блока несколько отличаются от приведённого здесь идеализированного случая.

Исполнительные органы (оконечные агенты). Их главный девиз: «*Координация во времени и в пространстве, распределение целей и задач*». Именно этот аспект зачастую ускользает от внимания специалистов, пытающихся сформулировать определение «сетецентрического управления». Сетецентрическая информационно-управляющая система реализуется через формирование единого координатно-временного поля и привязку к нему всех элементов системы, информационных агентов, событий, и собственно данных — формирование управления, планирование и исполнение сетецентрических операций идёт в едином пространстве состояний. Следовательно, синергия проявляется не только через агрегацию информации, но и через построение единого информационно-управляющего поля. Что позволяет синтезировать управляющие команды для всего множества исполнительных органов (оконечных агентов) скоординировано во времени и в пространстве, оптимально распределяя между ними цели и задачи. При этом каждое из элементарных управлений само по себе не способно привести к достижению цели управления (цели сетецентрической операции). При этом вполне возможно сделать действие того или иного оконечного агента (исполнительного органа), на начальной стадии операции, слабо наблюдаемым и/или практически непредсказуемым. Подобное управление обладает двумя немаловажными свойствами: скрытностью и внезапностью. Это опять же синергический эффект: сосредоточенные задачи решаются, как правило, силами и средствами, распределёнными в пространстве и времени.

В концептуально-теоретическом плане сетецентрический подход в военном деле реализуется в виде системы, которая состоит из трех подсистем (рис. 2), имеющих структуру решетки: информационной подсистемы, сенсорной (разведывательной) подсистемы, боевой подсистемы (подсистемы отдельных тактических подразделений и боевого управления).

Основу этой системы составляет информационная решетка, на которую накладываются взаимно пересекающиеся сенсорная и боевая решетки.

Информационная решетка-подсистема пронизывает собой всю систему в полном объеме. Элементами сенсорной системы являются сенсоры (средства разведки), а элементами боевой решетки — средства поражения. Эти две группы элементов объединяются воедино органами управления и командования. Взаимоотношения между всеми элементами подсистем и самими подсистемами достаточно сложные и многоплановые, что позволяет, например, «стрелкам» поражать цели сразу по получении информации от «сенсоров» или по получении приказа от органов управления, или в некоторых случаях самостоятельно.

Сетецентрическая система управления порождается эмерджментностью, которая и обуславливает её эффективность и продуктивность при решении ряда задач. При этом необходимо отметить, что управление к классу сетецентрического возможно отнести, только если оно содержит в своём составе все три означенные компоненты. В противном случае, надо говорить о псевдосетецентрических системах, или вырожденных сетецентрических системах управления.

Впервые термин «сетецентрический» (Network Centric) был использован вице-адмиралом ВМС США Артуром Себровски и Джоном Гарстка в опубликованной ими в журнале «Proceedings» в январе 1998 года статье «Сетецентрическая война: ее происхождение и будущее». Данная концепция была доработана и представлена в книге Джона Гарстка, Давида Альбертса и Фреда Стейна.

Необходимо отметить, что концепция «сетецентрической войны» по существу представляет собой не новый тип войны, а новый подход к подготовке, организации и ведению боевых действий, где в центре внимания оказывается сеть. Причем наиболее важным аспектом являются принципы ее организации и, во многом, самоорганизации.

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

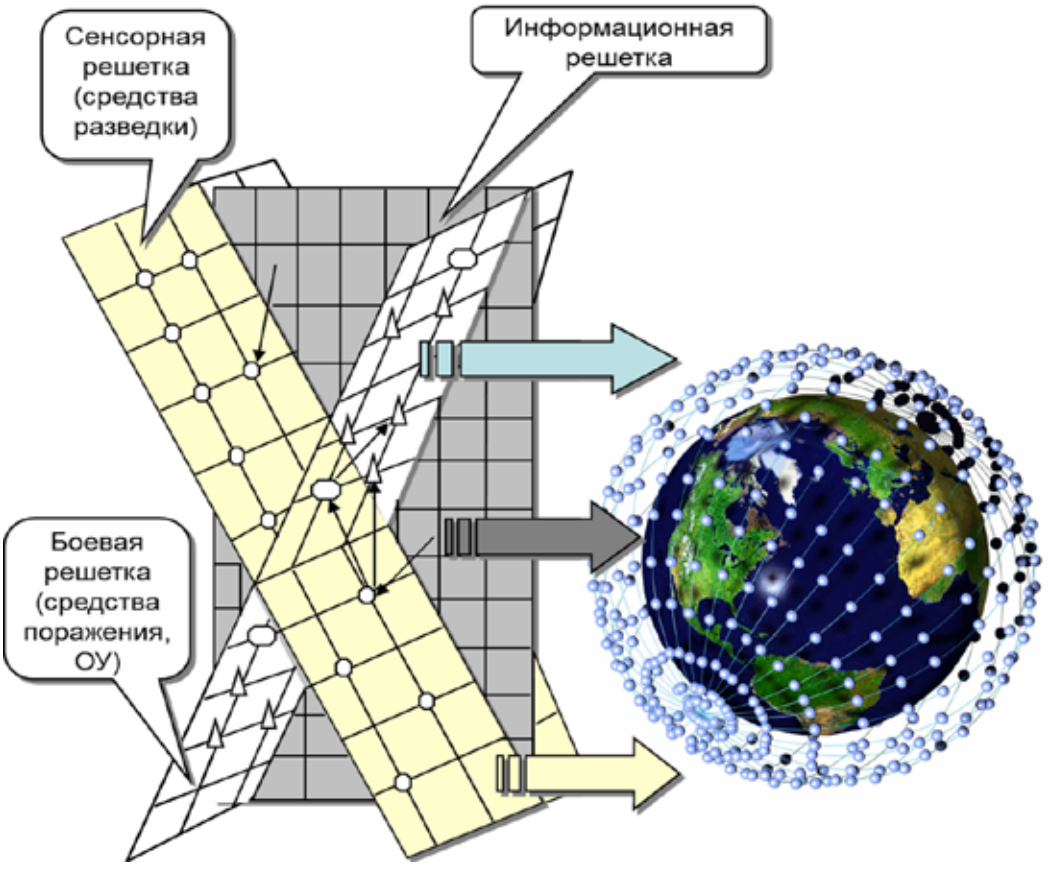

Рис. 2. Обобщённая модель сетецентрического подхода в военном деле

В основе такой сети лежит глобальная информационная решетка (ГИР). GIG — глобально взаимосвязанное, сквозное (end-to-end) множество информации, которое в ней накапливается, хранится, распространяется и распределяется по запросу от военных, политических деятелей и обслуживающего персонала. GIG включает свои и арендованные коммуникации, компьютерные системы и сервисы, программное обеспечение (включая приложения), данные, сервисы безопасности, другие связанные сервисы, а также системы обеспечения национальной безопасности.

Под самосинхронизацией американскими специалистами понимается способность военной структуры самоорганизовываться снизу, а не изменяться в соответствии с указаниями сверху. Организационная структура частей и подразделений, формы и методы выполнения ими боевых задач, как ожидается, будут видоизменяться по своему усмотрению, но в соответствии с потребностями вышестоящего командования. Жесткая иерархическая система военного управления сменится гибкой сетевой: подчиненные войска получат свободу в выборе методов действий, а организационно-штатная структура войск будет постоянно меняться, «приспосабливаться» к требованиям обстановки.

Внедрение концепции «сетецентрической войны» привело к тому, что сегодня вооруженные силы США только внешне напоминают свой облик в операции «Буря в пустыне» 1991 г. В Ираке они впервые использовали новую распределенную информационную систему боевого управления FBCB2 (Force XXI Battle Command Brigade or Below), охватывающую уровень бригады, батальона и роты. Информационная система собирает и распределяет данные, поступающие от всех источников разведывательной информации: спутника, самолета, вертолета, танка, БМП и даже отдельного пехотинца. В этой войне просматривается принципиально новая стратегия и тактика ведения боевых действий, прежде всего, благодаря новым информационным и сетевым технологиям.

Дальнейшее развитие концепции «сетецентрической войны» привело к принятию программы FCS (Future Combat System). Главными идеями последующей реорганизации вооруженных сил США стали следующие: объединение всех систем управления и

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

ведения боя в единую армейскую сеть и максимальное внедрение автоматизированных и роботизированных систем, замена техники и вооружения на более совершенные образцы с поддержкой их применения в единой армейской сети. В настоящее время, Объединенное стратегическое командование США (U.S. Strategic Command — USSTRATCOM) является головной структурой в вооруженных силах США[1], которая отвечает за планирование, координацию и ведение информационных операций в глобальном масштабе, в том числе за операции в компьютерных сетях.

Собственно сама структура управления, по мнению американских военных специалистов, является важнейшим элементом в системе реализации асимметричных преимуществ военной мощи США, элементом усиления важнейших компетенций переданных в оперативное подчинение Объединенному стратегическому командованию США компонентов ВС и ключевых взаимодействующих структур государства через формирование единой информационно-коммуникационной среды (сетецентрическое управление). Такая общая для всех информационно-коммуникационная среда обеспечит высокий уровень объединенности, взаимодействия и синхронизации всех компонентов национальной мощи. Именно поэтому руководство Объединенного стратегического командования ВС США при формировании уже новой структуры управления, отказалось от создания дополнительного уровня управления классической J-структуры[2] в пользу функционально-сетевого объединения уже существующих командований видов вооруженных сил и ряда взаимодействующих государственных структур.

С целью дальнейшего совершенствования новой организации Объединенного стратегического командования США в течение 2005–2006 годов были созданы шесть новых объединенных функциональных командований (Joint Functional Component Command — JFCC) и три центра. Вновь сформированные объединенные функциональные командования являются взаимозависимыми и предназначены для осуществления ежедневного оперативного планирования и организации действий, приданных и взаимодействующих сил и средств видов ВС как единого целого в своих функциональных областях: воздушно-космические операции, противоракетные операции, информационные и сетевые операции, разведывательные операции и операции по борьбе с распространением оружия массового поражения.

Следует отметить, что из девяти новых структур Объединенного стратегического командования США четыре непосредственно решают задачи разведки, информационных операций и операций в компьютерных сетях, к которым относятся командования разведывательных операций (JFCC-Intelligence, Surveillance and Reconnaissance — JFCC-ISR); операций в компьютерных сетях (JFCC-Network Warfare — JFCC-NW), которое иногда называют командованием «сетевой войны»[3]; объединенных информационных операций (Joint Information Operations Warfare Command — JIOWC)[4] и объединенный центр защиты компьютерных сетей (Joint Task Force-Global Network Operations — JTF-GNO)[5]. При этом штаб Объединенного стратегического командования ВС США сохранил за собой непосредственную ответственность за функционирование системы управления стратегическими наступательными силами ВС США.

Помимо сетецентрической модели организации и ведения боевых действий подобный подход применяется и при проектировании так называемых сетецентрических информационно-управляющих систем (ИУС) специального назначения. Наиболее перспективным направлением развития ИУС являются матричные ИУС. В их основе, как и в основе

[1] Одно из 10–ти объединенных командований в составе министерства обороны США. Шесть являются региональными: в Европейской зоне; в зоне Тихого океана; в зоне Северной Америки; в зоне Центральной и Южной Америки; Объединенное центральное командование; Объединенное африканское командование. Остальные четыре являются функциональными: Объединенное командование сил специальных операций; Объединенное командование единых сил; Объединенное командование стратегических переброс и Объединенное стратегическое командование.

[2] Ядром системы управления любого объединенного командования является его штаб, структура которого, как правило, состоит из управлений (отделов) номерной J-структуры, например: J-1 кадров (личного состава); J-2 разведывательное; J-3 оперативное; J-4 тыла; J-5 оперативного планирования; J-6 систем связи и информации и т.п.

[3] Дислоцируется совместно с АНБ на военной базе Форт-Мид (штат Мэриленд). Его численность составляет приблизительно 125 кадровых офицеров раз личного ранга и 35 гражданских специалистов.

[4] Дислоцируется на авиабазе Лэкленд (штат Техас). Численность личного состава составляет 186 офицеров различного ранга и около 40 гражданских специалистов.

[5] Дислоцируется на военной базе Арлингтон (штат Виргиния). Численность личного состава составляет около 210 офицеров различного ранга и около 80 гражданских специалистов.

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

концепции «сетецентрической войны», лежит глобальная информационная решетка. Под этим понятием понимается не только вертикальная интеграция между источниками информации, узлами принятия решения и исполнительными органами, но и широкое развитие горизонтальных связей между разнородными поставщиками, обработчиками и потребителями циркулирующей в ИУС информации.

От исследования вопросов, связанных с принципиальной реализуемостью этих систем, и прорисовкой их возможных архитектур и принципов функционирования, разработчики плавно переходят к детальной проработке вопросов связанных с техническими и организационными задачами развёртывания, эксплуатации и применения.

Из перекрёстного анализа открытых источников информации следует, что в этих информационно-управляющих системах, гетерогенных по своей сути, стараются эффективно увязать: различные форматы и типы циркулирующих данных; разнородные источники информации; различные способы первичной, вторичной и третичной обработки информации; разнородных потребителей.

Сетецентрическая парадигма реализуется через базовый функционал матричных информационно-управляющих систем, который включает в себя следующие основные составляющие: формирование единого координатно-временного поля и привязка к нему всех элементов системы, информационных агентов, событий, и собственно данных; сбор и интегрирование разнородной информации (в едином координатно-временном поле) полученной от различных источников с перекрёстным уточнением и добавлением; анализ и предсказание развития обстановки на стратегическом, тактическом и операционном уровнях; формирование единого информационно-управляющего поля; формирование среды поддержки принятия решений; трансляция и доведение информации и управляющих команд до потребителей и исполнителей; документирование всех событий и управляющих команд.

Отличительной чертой сетецентрических информационно-управляющих систем специального назначения является их глобальность — как в пространственном, так и в функциональном плане. Они функционируют в режиме реального времени, в асинхронном (событийном) режиме работы.

Исходя из вышеизложенного можно сделать вывод, что система сетецентрического управления представляет собой сочетание заблаговременно созданных и развернутых разветвленных автоматизированных электронных сетей сбора и первичной обработки информации, узлов хранения и анализа информации, а также контуров управления и принятия решений, которые совокупными усилиями создают единое информационно-управленческое пространство, охватывающее все пространство управления.

Электронные сети развертываются в узлах и органах сбора/обработки, анализа, оценки, диссимиляции информации о внешнем мире, на всех уровнях органов государственного управления и регулирования. Электронные сети сопрягаются и связываются в единый информационно-управленческий комплекс, обеспечивающий непрерывное оперативное управление имеющимися силами и средствами по вертикали и горизонтали на пространстве управления. Совокупными усилиями всех элементов комплекс создает единое «информационно-управленческое поле» (пространство), которое непрерывно поддерживается в рабочем состоянии, самосинхронизируется, обновляется информацией снизу и сверху, доступно для всех уровней управления по вертикали и горизонтали, и защищено от несанкционированного проникновения и воздействия.

Говоря об управлении, необходимо, в первую очередь, определить объект, которым необходимо управлять. Таким объектом управления является распределенная система. *Распределенная система — совокупность автономных, оснащенных компьютерным интеллектом объектов, объединенных общей глобальной сетью и способных действовать как самостоятельно, так и в группе для выполнения общей целевой функции.*

На основании всего вышеизложенного, предлагается дать следующее определение термина «сетецентрическая система управления». *Сетецентрическая система управления — система управления распределённой системой, характеризующаяся принципами открытости, самоорганизации, слабой иерархии в контуре принятия решений и способностью порождать цели внутри себя.*

В рамках проведения сетецентрической операции, в первую очередь, решается задача обеспечения *информационного превосходства.* Для чего необходимо:

1) искусственно увеличить потребность противника в информации и одновременно сократить для него доступ к ней;
2) обеспечить широкий доступ к информации своих подразделений через сетевые механизмы и

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

инструменты обратной связи, надежно защитив их от внедрения противника;

3) сократить собственную потребность в статичной информации через обеспечение доступа к широкому спектру оперативного и динамичного информирования.

При этом сетецентрической операции присущи:

1) *«Всеобщая осведомленность»* (shared awareness) за счет построение общей сводной информационной сети; превращение пользователей информации одновременно в поставщиков информации способных активировать незамедлительно обратную связь; максимальная защита доступа к сети противника с одновременной максимальной доступностью ее для подавляющего числа своих.
2) *Высокая скорость управленческих циклов* за счет адаптации к условиям боя и увеличения скорости принятия управленческого решения, что обеспечивает конкретное оперативное преимущество, а также блокирования реализацию управленческих решений противника и обеспечить заведомое превосходство в соревновании на уровне решений.
3) *Самосинхронизация*, которая обеспечивается возможностью боевых подразделений действовать практически в автономном режиме, формулировать самим и решать оперативные задачи на основе «всеобщей осведомленности» и понимания «намерения командира».

«Сетецентричной войне» характерно:

– *перераспределение силы* от линейной конфигурации на поле боевых действий к ведению точечных операций. Для этого необходимо перейти от формы физического занятия обширного пространства к функциональному контролю над наиболее важными стратегически элементами и к нелинейным действиям во времени и пространстве; усилить тесное взаимодействие разведки, операционного командования и логистики для реализации точных эффектов и обеспечение временного преимущества с помощью рассеянных сил;
– *глубокое сенсорное проникновение* — увеличение количества и развитие качества датчиков информации как в районе боевых действий, так и вне его. Это проникновение обеспечивается за счет объединение в единую систему данных, получаемых разведкой, наблюдением и системами распознавания; использование сенсоров как главных маневренных элементов; использование датчиков и точек наблюдения как инструмента морального воздействия; снабжение каждого орудия и каждой боевой единицы (платформы) разнообразными датчиками и информационными сенсорами — от отдельного бойца до спутника.

В настоящее время в НАТО реализуется концепция «Комплексные сетевые возможности» (NATO Network Enabled Capabilities — NNEC), 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.* Проводимые в настоящее время мероприятия осуществляются в трех ключевых областях: развертывание современных систем связи и передачи данных; разработка перспективных систем анализа и распределения информации, использующих унифицированные форматы представления и средства ее обработки; формирование современной когнитивной сферы, затрагивающей вопросы реформирования и оптимизации организационных структур органов управления, обработки и анализа информации, а также подготовку личного состава и уточнение уставных и доктринальных документов.

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. В конечном счете, достигается необходимый уровень боевых возможностей перспективных формирований. С другой стороны, осуществляется формирование новой оборонительной инфраструктуры НАТО в киберпространстве. Согласно договоренностям, достигнутым на Лиссабонском саммите, завершена модернизация всех коммуникационных и информационных систем НАТО. Одновременно преобразовывается сетевая архитектура альянса. Основные направления реализуемых мероприятий были сформулированы в «Оборонительной по-

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

литике НАТО в киберпространстве»[6], одобренном министрами обороны стран-участниц еще в июне 2011 года. Обеспечение кибербезопасности во всей структуре НАТО осуществляет Координационный совет по кибероборонe (Cyber Defence Management Authority (CDMA)). Он специализируется на увеличении функциональной гибкости всех имеющихся информационно-телекоммуникационных ресурсов и предотвращении киберугроз. Исполнительным органом является Управляющий директорат по делам кибероборонe (NATO Cyber Defence Management Board (CDMB)), деятельность которого строится с учетом того, чтобы все структурные подразделения НАТО находились под централизованной защитой с учетом новых современных требований к кибероборонe. В связи с этим Консультационное, командное и контрольное управление (NATO Consultation, Command and Control Agency (NC3A))[7] существенное внимание уделяет усилению защиты альянса от современных и будущих угроз в киберпространстве в соответствии с проектом NATO Computer Incident Response Capability — Full Operational Capability. Усовершенствуется Технический центр NCIRC (NCIRC Technical Center) в городе Монс (Бельгия) и разворачивается система поддержки решений (Cyber Defence Decision Support System). Также сформирована мобильная Группа быстрого реагирования (Rapid Reaction Team) и устанавливается дополнительная Справочная система (Reference System), которая ориентированна на персонал Центра для тестирования нового защитного программного обеспечения и изучения вредоносных кодов. Развернуты целая серия датчиков для сетевой ситуационной оценки (Cyber Defence Sensors) и системы для предотвращения кибератак, включая перспективные инструменты, в том числе необходимые для регистрации полных наборов информационных пакетов вредоносных кодов. Датчики Cyber Defence Sensors устанавливаются практически на всех серверах, и размещается значительное количество интеллектуальных сенсоров непосредственно в сети. Сенсоры обеспечат контроль максимально возможного сектора сетевого ресурса и непосредственно связаны с Техническим центром. В этом случае система принятия окончательных решений даст общую картину гарантированного предоставления информации (consolidated information assurance picture) и сформирует модель распределения данных, что обеспечит поступление информации только тому, кто в ней нуждается, и тогда, когда это необходимо, а не будет отвлекать пользователей избыточными материалами. Причем прообраз такой модели уже был успешно опробован в зонах боевых действий, в частности в Афганистане.

Во Франции такие мероприятия реализуются в рамках концепции, получившей наименование «Информационно-центрическая война» (Guerre Infocentre), 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.

Бундесвер работает над созданием перспективной системы оснащения и вооружения личного состава (Infanteristder Zuknft), позволяющей 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.

В Великобритании формируется собственная глобальная информационная инфраструктура, представляющая собой единую информационно-управляющую сеть со специализированными системами обеспечения безопасности и единым семейством программного инструментария. В будущем возможности формируемой информационной инфраструктуры планируется расширить и для организации взаимодействия и обеспечения доступа к информационным ресурсам вооруженных сил союзников: США, Канады, Новой Зеландии и Австралии.

Генеральный штаб ВС Израиля рассматривает внедрение перспективных информационных технологий как неотъемлемый и обязательный атрибут современных и будущих операций. Например, во время последней войны с Ливаном вооруженные

[6] NATO Policy on Cyber Defence» C-M(2011)0042, dated 7 Jun, 2011 (NR). Новая политика НАТО в сфере кибероборонe одобрена министрами обороны Альянса 7 июня 2011 г.

[7] Агентство NC3A в настоящее время является частью одного из трех управлений (Communications & Information Agency, C&I Agency) в структуре НАТО.

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

силы Израиля применяли перспективную систему управления и связи Tzayad, позволявшую объединять в группировку различные беспилотные летательные аппараты (БЛА) для решения задач поиска и уничтожения мобильных ракетных пусковых установок, применяемых боевиками движения Хезболла. Военные эксперты отмечали высокую эффективность действия израильских бригад, оснащенных такой системой.

Китай тоже серьезно «заболел» сетецентрической концепцией управления и ведения боевых действий. В последних документах ВС Китая встречается термин «интегрированная сетевая и электронная война» (Integrated Network-Electronic Warfare — INEW). Именно он и является отражением современной китайской концепции, сравнимой с концепцией «сетецентрической войны (операции)» ВС США.

Сравнительный анализ реализуемых сетецентрических концепций управления и ведения боевых действий ведущими державами мира позволяет отметить следующее.

Новые формирования, использующие перспективные сетецентрические концепции, могут применять новую тактику действий. Во время операции «Свобода Ираку» вооруженные силы США уже применяли тактику перемещения боевых формирований, получившую наименование *«тактика роя».*

Глобальность, предусматривает возможность боевых формирований получать доступ к информационной инфраструктуре министерства обороны, базам разведывательной информации, аналитических центров, находясь в любой точке земного шара и в любое время. Новые принципы управления позволяют реализовать и новые боевые возможности, но только современных, мобильных, высокотехнологичных формирований в любой точке их задействования (глобально).

Происходят изменения способов разведывательной деятельности, упрощение процедур согласования и координации при организации объединенного огневого поражения, а также некоторое нивелирование разграничения средств по звеньям управления, позволяющее применять стратегические средства разведки и огневого поражения для разведывательного и огневого обеспечения действий тактических формирований, как было в Афганистане и Ираке.

Американские эксперты отмечают, что, объединяя средства разведки в единую «систему систем», они, например, получают возможность «перешагнуть» дальность прямой видимости, расширить поле зрения (охвата), разрешающую способность, сократить скорость перенацеливания средств, обеспечить ведение разведки в любое время суток в любых погодных условиях, а также уменьшить недостатки каждого средства в отдельности.

Существенную роль реализация сетецентрических принципов играет и при организации объединенного огневого поражения. Например, устаревшие разведывательно-ударные комплексы представляли собой симбиоз определенного средства разведки и средства поражения с прямым каналом передачи данных целеуказания (как и принято до сих пор в ВС РФ). Применительно же к вооруженным силам США уже сейчас целесообразно говорить не об отдельных разведывательно-ударных комплексах, а о единой «системе систем», функционирующей в едином информационном пространстве.

Разработчики новых сетецентрических концепций утверждают, что последние 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).

Для демонстрации новых принципов управления министерство обороны США провело целый ряд экспериментальных учений. Аналогичным образом поступают и в вооруженных силах Китая.

Китайские военные специалисты осуществляли моделирование продолжительных боевых действий и исследовали работу центров и пунктов управления. В одном из сценариев учений они смоделировали высокоцифровизированную группировку войск противника, которая противостояла и успешно разгромила формирования Национальной освободительной армии Китая (НОАК), имеющие существенные ограничения в системе боевого управления, связи, вычислительной техники и разведки.

Применение современных информационных систем и интеграция боевых формирований в *единое информационно-коммуникационное пространство* позволяли войскам противника с высокой точностью «поражать» формирования НОАК на больших дальностях, т. е. еще до момента развертывания их в боевые порядки.

Концепция информационного превосходства в операциях ориентирована на повышение боевых возможностей формирований через объединение всех участников операции или боевых действий (средства

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

разведки, органы и пункты управления, средства поражения) для достижения единого понимания обстановки на поле боя, повышения оперативности управления и темпа операции, эффективности огневого поражения (воздействия) и живучести своих формирований, а также степени самосинхронизации (взаимодействия) всех участников операции.

В отличие от платформоцентрических принципов организации и ведения операций (боевых действий), когда боевые возможности зависели от индивидуальных возможностей боевых платформ, сетецентрические предусматривают достижение новых боевых возможностей формирований в первую очередь за счет синергетического эффекта комплексного использования совокупности всех имеющихся боевых платформ. Из этого определения и вырисовывается обобщенная модель сетецентрических операций, которые возможны только при наличии высокоэффективной информационной сети, обеспечивающей организацию взаимодействия и информационного обмена среди всех участников операции (боевых действий) и представляющей собой собственно *сетевую информационную инфраструктуру.*

В военных и политических изданиях часто упоминается аббревиатура ООДА. Этими четырьмя буквами обозначается основной элемент теории Джона Бойда (петля *Наблюдение-Ориентация-Решение-Действие).* Проведенный анализ сущности этой теории показывает, что она обладает высокой степенью универсальности и имеет перспективу широкого применения в задачах анализа и моделирования профессиональной деятельности отдельных людей и организаций в условиях конкурентной среды, характерной для войн, бизнеса, торговли и спорта. Особый интерес знакомство с Дж. Бондом и его теорией представляет для военных и специалистов, связанных с созданием новых военных технологий и перспективного вооружения. Недаром Дж. Бойда называют одним из главных военных стратегов и лидеров организации военной реформы в МО США.

Бойд обосновал следующий факт: для того, чтобы соответствовать реальности необходимо осуществлять действия в непрерывном цикле во взаимодействии с окружающей средой, учитывая ее постоянные изменения. Бойд, опираясь в своих исследованиях на эволюционную теорию Дарвина, сделал вывод, что естественный отбор действует не только в биологической среде, но и в социальной (проявляется в выживании людей в войнах и в бизнесе). В итоге он выдвинул гипотезу, что цикл деятельности и принятия решения ООДА является центральным механизмом адаптации, и что преимущество в скорости своего цикла действий и точности оценок обеспечивает преимущество над противником и ведет к достижению победы в военных действиях.

В настоящее время петля ООДА превратилась в стандарт описания цикла принятия решений во многих областях знания, в военные доктринальные документы министерств обороны США, Великобритании и Австралии.

Учитывая возможность применения цикла OODA в качестве модели описания и анализа в любой сфере военной деятельности и его масштабируемость для удобства дальнейших рассуждений, можно использовать термин *«универсальный цикл военной деятельности».* Отметим, что обоснованность и справедливость этих утверждений подкрепляется практикой ведения реальных боевых действий, успехами в обучении американских летчиков, моделированием и эффективным применением при планировании операций в Ираке и Афганистане.

В заключении можно сделать следующие выводы.

Концепция «сетецентрической войны» представляет собой систему научно-обоснованных взглядов подготовки и ведения военных действий в условиях глобального информационного обеспечения сил и средств вооруженной борьбы в реальном масштабе времени. Реализация концепции предусматривает 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 за заданное время. За счет этого достигается ускорение процесса управления силами и средствами, повышается темп операций, эффективность поражения объектов противника, повышается живучесть своих войск и уровень самосинхронизации боевых действий.

В основу концепции «сетецентрической войны» положены стандартизация, унификация и комплексное внедрение современных информационных технологий, что позволяет создать единое информационно-коммуникационное пространство. Единая сеть средств разведки, связи и органов управления увязывается с сетью средств поражения и сетями боевого и тылового обеспечения.

Основной идеей «сетецентрической войны» является интеграция всех сил и средств в едином

DOI: 10.7256/2073–8560.2014.2.11393
При цитировании этой статьи сноска на doi обязательна

информационном пространстве, позволяющая многократно увеличить эффективность их боевого применения за счет реализации синергетического эффекта. Внедрение сетевых технологий в военную сферу является действительно революционным шагом, направленным на повышение боевых возможностей вооруженных сил за счет оперативности и эффективности их применения.

Следует отметить, что исследование теоретических направлений повышения эффективности управления войсками (силами) и оружием только разворачивается. Ведётся поиск новых подходов к осуществлению комплексного поражения противника, организации управления войсками и оружием, взаимодействия и обеспечения. Для этого есть все необходимые предпосылки успешной реализации существующего научно-технического задела, а также перевода имеющихся разработок с уровня концептуально-теоретического осмысления проблемы в область практической реализации.

Библиография

1. В.И. Анненков, С.Н. Баранов, В.Ф. Моисеев, С.С. Хархалуп. Сетецентризм: геополитические и военно-политические аспекты современности. Учебник. — М.:РУСАВИА. 2013.
2. А.Е.Кондратьев. Проблемные вопросы исследования новых сетецентрических концепций вооруженных сил ведущих зарубежных стран. М.: Военная мысль, №11, 2009.
3. В.И. Выпасняк. О реализации сетецентрических принципов управления силами и средствами вооруженной борьбы в операциях (боевых действиях). М.: Военная мысль, №12, 2009.
4. А.А. Рахманов. Сетецентрические системы управления: закономерные тенденции, проблемные вопросы и пути их решения. М.: Военная мысль, №3, 2011.
5. И.В. Сурма. Глобальный наднациональный актор международных отношений и его социальная философия. Вестник МГИМО. М.: МГИМО. №4, 2013 г. С.141–151
6. С.А. Паршин, Ю.Е. Горбачев, Ю.А. Кожанов. Современные тенденции развития теории и практики управления в вооруженных силах США. — М.: ЛЕНАНД, 2009.
7. С.А. Паршин, Ю.Е. Горбачев, Ю.А. Кожанов. Кибервойны-реальная угроза национальной безопасности? — М.: КРАСАНД, 2011.
8. Кашкин С.Ю., Слепак В.Ю. Организационный механизм проведения военных операций Европейского Союза как средство обеспечения национальной безопасности государств-членов ЕС // Актуальные проблемы российского права. — 2013. — 7. — С. 864 — 868.

References

1. V.I. Annenkov, S.N. Baranov, V.F. Moiseev, S.S. Kharkhalup. Setetsentrizm: geopoliticheskie i voenno-politicheskie aspekty sovremennosti. Uchebnik. — M.:RUSAVIA. 2013.
2. A.E.Kondrat'ev. Problemnye voprosy issledovaniya novykh setetsentricheskikh kontseptsii vooruzhennykh sil vedushchikh zarubezhnykh stran. M.: Voennaya mysl', №11, 2009.
3. V.I. Vypasnyak. O realizatsii setetsentricheskikh printsipov upravleniya silami i sredstvami vooruzhennoi bor'by v operatsiyakh (boevykh deistviyakh). M.: Voennaya mysl', №12, 2009.
4. A.A. Rakhmanov. Setetsentricheskie sistemy upravleniya: zakonomernye tendentsii, problemnye voprosy i puti ikh resheniya. M.: Voennaya mysl', №3, 2011.
5. I.V. Surma. Global'nyi nadnatsional'nyi aktor mezhdunarodnykh otnoshenii i ego sotsial'naya filosofiya. Vestnik MGIMO. M.: MGIMO. №4, 2013 g. S.141–151
6. S.A. Parshin, Yu.E. Gorbachev, Yu.A. Kozhanov. Sovremennye tendentsii razvitiya teorii i praktiki upravleniya v vooruzhennykh silakh SShA. — M.: LENAND, 2009.
7. S.A. Parshin, Yu.E. Gorbachev, Yu.A. Kozhanov. Kibervoiny-real'naya ugroza natsional'noi bezopasnosti? — M.: KRASAND, 2011.
8. Kashkin S.Yu., Slepak V.Yu. Organizatsionnyi mekhanizm provedeniya voennykh operatsii Evropeiskogo Soyuza kak sredstvo obespecheniya natsional'noi bezopasnosti gosudarstv-chlenov ES // Aktual'nye problemy rossiiskogo prava. — 2013. — 7. — C. 864 — 868.