

УДК. 355.4

І.В. Тітов

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

## МЕРЕЖОЦЕНТРИЧНА КОНЦЕПЦІЯ ВЕДЕННЯ ВІЙНИ ХХІ СТОРІЧЧЯ

У статті розкриті сутність та інформаційні аспекти одного з сучасних підходів до ведення війни ХХІ сторіччя – мережоцентричної війни. Одним з основних факторів, що спричинили виникнення мережоцентричної війни, як війни нового покоління, є революція в галузі інформаційних технологій, яка останнім часом охопила і військову сферу. Концепція мережоцентричної війни визначає нові принципи управління військами та силами і передбачає в першу чергу об'єднання всіх учасників бойових дій в рамках єдиного інформаційного простору. На думку фахівців, основною перевагою мережоцентричної концепції ведення бойових дій є висока маневреність частин та з'єднань, прискорення процесів прийняття рішень і планування операцій.

**Ключові слова:** мережоцентрична війна, інформаційна мережа, інформаційний простір.

### Вступ

Постановка проблеми та аналіз останніх досліджень і публікацій. Розробивши ще на початку 80-х років так звану “концепцію інтеграції систем управління, зв'язку, розвідки та РЕБ” (С<sup>3</sup>IEW), Пентагон послідовно на протязі останніх двадцяти років здійснював цілеспрямовану технічну та інвестиційну політику в цій галузі. В результаті, в середині 90-х років, на основі останніх досягнень в галузі мікроелектроніки та обчислювальної техніки визначилось принципово новий напрямок технологічного прориву, пов'язаний з подальшим розвитком концепції С<sup>3</sup>IEW, що отримав назву “концепції інтеграції систем управління, зв'язку, розвідки РЕБ і комп'ютеризації для воїна” (С<sup>4</sup>IFTW).

Зараз ця концепція отримала нову назву С<sup>4</sup>KISR, а її сутність зводиться до гарантованої поразки будь-якої наземної цілі на основі застосування інформаційних систем та мереж в сполученні із засобами управління, зв'язку, спостереження та розвідки, що реалізує концепцію мережоцентричної війни (МВ). “Війнам майбутнього”, до яких належить і мережоцентрична війна (МВ), присвячено багато робіт, зокрема [1 – 4].

**Метою статті** є узагальнення основних положень щодо розробки та реалізації концепції ведення бойових дій в форматі мережоцентричної війни та висвітлення її інформаційних аспектів.

### Виклад основного матеріалу

Втілення мережевих технологій у військову сферу є дійсно революційним кроком, що сприяє підвищенню бойових можливостей збройних сил, але вже не тільки за рахунок вогневих, маневрових та інших характеристик індивідуальних платформ, а в першу чергу, за рахунок скорочення циклу бойового управління в операції (бою). Зараз фахівці говорять про перехід від так званої “платформоцентричної” війни до “мережоцентричної” (Network Centric War-

fare, NCW), авторами якої вважаються віце-адмірал ВМС США Артур Цебровски та Джон Гарстка [3].

З технологічної точки зору основою концепції МВ є представлення будь-якого озброєного формування у вигляді комп'ютерної мережі, що об'єднує елементи трьох видів (трьох підмереж): сенсори (засоби спостереження, виявлення та супроводження об'єктів противника у смугі відповідальності формування), засоби вогневого, радіоелектронного та іншого впливу (поразки) на виявленні об'єкти, інтелектуальні (інформаційно-керуючі) елементи, що виконують функції аналізу ситуації, прийняття та реалізації рішень щодо управління сенсорами, засобами впливу (поразки), передачі різноманітної інформації “по вертикалі і горизонталі” системи.

Всі три підмережі включають вузли, що працюють як з реальними, так і з віртуальними об'єктами. В сенсорній підмережі самі датчики можуть бути пасивними і активними, а розташовуватись – як в реальній, так і у віртуальній сфері бойового простору. Це стосується і підмережі виконавчих вузлів. До неї включені як традиційні засоби поразки (танки, літаки, кораблі та ін.), так і засоби впливу на цілі у віртуальному просторі: засоби масової інформації, комп'ютерні віруси та ін.

Концепція МВ була вперше апробована коаліційними силами на чолі із США в ході операції в Іраку навесні 2003 року.

Тоді відсутність в тактичній та оперативній ланках робочих карт (які до сьогодення часу є основним атрибутом управління з'єднаннями, частинами та підрозділами у Збройних Силах України), використання комп'ютерно-автоматизованої розподільчої системи бойового управління в бойових умовах дозволили американському командуванню передавати данні про об'єкти (цілі) в режимі реального часу всім бойовим ланкам – включно до командирів танків, БМП, БТР – відразу. Інформація від штучних супутників Землі, розвідувальних літаків та безпілотних літальних апаратів надходила в

цю систему бойового управління, селекувалася та доводилася до всіх інстанцій одночасно. Всі команди бойових підрозділів мали комп'ютери у міцних блоках. Положення всіх наземних мобільних об'єктів безперервно відслідковувались спеціальною системою. Комп'ютери штаба армійського корпусу спроможні відслідковувати до 1000 наземних цілей за годину. З'єднання армії США, що брали участь в Іракській війні 2003 року, розпочали бойові дії без підготовленого тилу, без завчасної розвідки, але боєприпаси та паливо, в основному, надходили саме в необхідний час, а досить розтягнуті комунікації не впливали на постачання військ. Для організації так званого адресного тилового постачання (focused logistics) коаліція використовувала розподілену інформаційну систему (Army's Movement Tracking System, MTS), в якій на основі радіовипромінюючих датчиків (radio frequency identification, RFID), стаціонарних та портативних сканерів, навігаційної супутникової системи GPS, бездротового доступу і тактичного Інтернету безперервно відслідковується положення всіх наземних рухомих об'єктів, від екіпажів яких тиловики отримують запити на постачання пального, боєприпасів, ЗПІ та інших видів забезпечення.

Сьогодні аналоговий радіозв'язок майже не використовується в ланці управління корпусу та бригади. Їх замінили бездротові інформаційні мережі, що дають можливість отримувати не тільки формалізовані повідомлення про виявлені і знищені цілі, втрати, витрати боєприпасів і пального, але й відео з місця бойових дій.

Виходячи з досвіду компанії в Іраку 2003 року, всі промислово-розвинуті держави світу приступили до створення глобальної інформаційної мережі (Global Information Grid, GIG), яка дозволяє забезпечити командуванню збройних сил цих держав управління військами в бойових умовах на основі інформаційно-керуючих систем. Це гарантує успішне ведення бойових дій проти армій, у яких подібні систем відсутні.

В будь-якій військовій операції має місце такий цикл подій: розвідка противника – оцінка обстановки – прийняття рішення – дії у відповідності до обраного плану [3]. Такий цикл умовно можна розділити на дві фази: інформаційну та кінетичну. Остання, в основному, визначається можливостями засобів поразки.

Останнім часом як вітчизняні, так і закордонні вчені займалися пошуком технічних рішень, пов'язаних в першу чергу із другою фазою, а саме – підвищенням мобільності, точності та вогневої потужності засобів збройної боротьби. Але, як показує практика, для підвищення ефективності кінетичної фази є певні обмеження, крім того суттєво підвищується і вартість розробок.

Таким чином, стає актуальним питання щодо розвитку інформаційної фази. Саме цьому аспекту зараз присвячені багато концепцій провідних дер-

жав, які спрямовані на об'єднання різнопланових компонентів в єдину інформаційну систему.



Рис. 1. Об'єднання джерел та споживачів інформації

За даними [5], Міністерство оборони Канади планує перевести свою армію у відповідність до концепції мережевої війни. Витрати на цю програму у найближчі десять років будуть становити 860 мільйонів доларів. Вже підготовлено 90 програм, що охоплюють питання створення безпілотних літальних апаратів, високоточних радарів тощо. В ході навчань Atlantic Littoral Intelligence Surveillance and Atlantic Littoral Intelligence Surveillance вже були протестовані перші напрацювання стосовно технології збирання даних від бойових кораблів, літаків-розвідників, безпілотних літальних апаратів та наземних засобів спостереження. Отримана інформація об'єднувалась, приводилася до єдиного стандарту бойового простору та робилася доступною через портал для всіх учасників навчань. Інформація являла собою цифрову карту з позначенням координат своїх та ворожих об'єктів. Доступ до такої інформації, окрім військових, мали прикордонники, служби порятунку та поліцейські.

Згідно з поглядами багатьох фахівців, при веденні бойових дій в єдиному інформаційному просторі значна роль відводиться безпілотним літальним апаратам (БПЛА) [6].

В рамках основного компонента англійської системи мережевої війни Network Enabled Capability, Міністерство оборони цієї країни виділило 317 мільйонів фунтів на восьмирічний проект виробництва нових БПЛА Watchkeeper Hermes 450 для реалізації програми збору розвідувальних даних Watchkeeper. Розгортання програми Watchkeeper – основного компонента концепції англійської системи мережевої війни має розпочатися у 2010 році.

Корпорація Boeing та військово-повітряні сили США продемонстрували в дії нову концепцію мережецентричної організації інформаційного простору поля бою на основі БПЛА – проект "Marti" [7]. Дослідження ведуться сумісно компаніями Phantom Works (що входить до концерну Boeing) та відділом інформаційних систем дослідницької лабораторії ВПС США. В рамках досліджень ведеться розробка гнучкої технології щодо забезпечення військ такти-

чною інформацією при використанні для цього БПЛА класів High-Altitude, Long Endurance та ScanEagle.

Для цього розроблена технологія так званої "підписки" користувачів на використання даних того чи іншого типу з урахуванням обстановки на певній частині території. Крім БПЛА передбачається використання аеростатів з висотою підйому біля 30 км. Нова технологія забезпечує надійне передавання різноманітної інформації із використанням стандартного інтернет-протоколу. На дисплеях користувачів відображається лише частина інформації, що необхідна для рішення поставлених задач та викликана користувачем. До кінця 2008 року проект "Marti" має вийти на фінальний етап.

Та поряд із цим існують певні проблеми, деякі з них пов'язані із недостатньою кількістю каналів зв'язку та обмеженням їх смуг частот. У зв'язку із цим британська компанія "Tael's optronic" займається проблемою передавання даних із використанням вузькосмугових каналів зв'язку [6]. При застосуванні набору стандартів стиснення зображень формату JPEG-2000 в сполученні із технологіями фірми передбачається можливість передавання зображень по вузькосмуговим каналам засобів тактичного зв'язку зі швидкістю до 16 кбіт/с.

Іншою інноваційною пропозицією компанії "Tadiran spektrielinc" є єдиний тактичний канал зв'язку (Tactical Common Data Link, TCDL) [6], призначений для передавання радіолокаційної інформації, зображень та відеоданих, які отримуються датчиками БПЛА зі швидкостями від 10,7 до 274 Мбіт (в перспективі) на відстані до 200 км.

Агентство військової розвідки США DIA замовило компанії McDonald Bradley розробку глобальної IT-інфраструктури, за допомогою якої розвідувальні інфраструктури Пентагону будуть мати змогу постачати важливу інформацію кінцевим споживачам на полі бою [5]. Контракт вартістю 8,15 млн. дол. виконується в рамках проекту по розвитку сервісно-орієнтованої архітектури міністерства оборони.

Для підмережі сенсорів глобальної інформаційної мережі розробляються різні види датчиків. Intelligent Munitions System (IMS) – система невеликих датчиків, сенсорів, маркерів та інших мініатюрних пристроїв, об'єднаних в одну мережу, установка якої на полі бою планується шляхом скидання з літаків або іншим шляхом. Unattended Ground Sensor (UGS) – "довгострокові" сенсори, що дозволяють збирати інформацію в тилу ворога. Вони теж можуть скидуватись з літаків або встановлюватись іншим шляхом. Такі датчики можуть працювати на протязі багатьох тижнів і навіть місяців, та встановлюватись як поодинокі так і групами. UGS вже активно використовується в американській та ізраїльських арміях.

При втіленні мережевих інформаційних технологій в бойове застосування військ збройних сил США, передбачається використання мобільних адаптивних

мереж, що дозволить суттєво підвищити рівень ситуаційної обізнаності та контролю критичних процесів [8].

Зараз особливий інтерес представляє проект CBMANET (Control-Based Mobile Ad Hoc Networking), який передбачає розробку концепції і технічної реалізації мобільної адаптивної мережі з розподіленим управлінням. Така система буде мати значно більші можливості в порівнянні з існуючими бездротовими мережами. Вузли такої мережі планується обладнати ненаправленими антенами та передавачами з потужністю випромінювання не більше 5 Вт.

Іншим напрямком робіт управління перспективних досліджень міністерства оборони США (до компетенції якого, до речі, належить і проект CBMANET) є програма WNaN (Wireless Network after Next), якою теж передбачається проектування адаптивних мереж нового покоління. Особливістю таких бездротових мереж має стати можливість швидкого настроювання мережевої конфігурації та мінімальна вартість мережевого обладнання [8]. Планується підтримка такими мережами принципу MIMO (Multiple Input Multiple Output).

Сьогодні у збройних силах США мають системи зв'язку, що дозволяють формувати прості конфігурації адаптивних мереж. Прикладом може бути сімейство радіостанцій NTDR, що працюють в діапазоні 225 – 400 МГц, та цифрові програмуємі радіостанції сімейства JTRS (Joint Tactical Radio System), що мають прийти їм на зміну.

Практична реалізація концепції МВ можлива лише за умов ефективного вирішення питань створення трьох ключових компонент: наднадійного комунікаційного середовища, яке має забезпечувати ефективне функціонування на основі комп'ютерних мереж збройних формувань та їх об'єднання в глобальну інформаційну мережу збройних сил; угруповування керуємих, надійних, інформативних довговічних та досить непомітних для противника сенсорів, що мають комплексуватись в комп'ютерні мережі збройних формувань; розподіленого програмного середовища, що має забезпечувати в реальному часі комплексну багаторівневу інтелектуальну обробку потоків (малоінформативних окремо та іноді протирічних) первинних даних про об'єкти, а також дозволяючого, в разі необхідності, оперативно змінювати логіку обробки, по мірі того, як буде змінюватись склад та можливості сенсорів.

Основні технічні передумови для реалізації концепції МВ в американських збройних силах існують, однак найбільш проблемним питанням практичного втілення цієї концепції є створення розподіленого програмного середовища.

Що стосується України, то зараз оснащення її Збройних Сил ОБТ здійснюється за пріоритетними напрямками, визначеними Державною програмою розвитку озброєнь і військової техніки до 2015 р. [9], в якій не передбачено нічого, що хоча б наближено відповідало яким-небудь положенням зазначе-

ної концепції. До того ж зараз, в умовах фінансових обмежень, головні зусилля Міністерства оборони та Генерального штабу спрямовуються на підтримання боєготовності ОВТ шляхом їх модернізації та подовження ресурсу [10]. І хоча у 2007р. фактичне фінансування за бюджетними програмами оснащення ОВТ, порівняно з попередніми роками, збільшилося майже втричі, та все одно є недостатнім для формування повноцінного, відповідного потребам Збройних Сил оборонного замовлення.

Однак не можливо не зазначити такі позитивні зміни в системі управління, як перехід від багаторівневої системи оперативного управління до найбільш оптимальної (як зазначено в [10]), триступеневої системи, створення Єдиної автоматизованої системи управління Збройних Сил тощо.

Першим кроком у створенні систем озброєння у відповідності із концепцією МВ може бути перспективна інтегрована інформаційно-телекомунікаційна система, основні аспекти створення та застосування якої були розглянуті в багатьох роботах, зокрема [11]. Вона має будуватись за багатопозиційним принципом, включати до свого складу активно-пасивні приймально-передавальні вузли, застосовувати в якості базової технологію цифрового діаграмування.

## Висновки

Імовірно, що протягом найближчих 15 – 20 років розвиток систем озброєнь та організаційних структур армій найбільш розвинутих держав світу буде проходити у відповідності до реалізації концепції МВ. Стосовно України, така концепція може бути корисною при формуванні раціонального складу та вигляду системи озброєння Збройних Сил України, як ключового положення воєнно-технічної політики держави.

## СЕТЕЦЕНТРИЧЕСКАЯ КОНЦЕПЦИЯ ВЕДЕНИЯ ВОЙНЫ XXI СТОЛЕТИЯ

И.В. Титов

*В статье раскрыты сущность и информационные аспекты одного из современных подходов к ведению войны XXI столетия – сетевидной войны. Одним из основных факторов, вызвавших возникновение сетевидной войны как войны нового поколения, является революция в области информационных технологий, которая в последнее время охватила и военную сферу. Концепция сетевидной войны определяет новые принципы управления войсками и силами и предусматривает в первую очередь объединение всех участников боевых действий в рамках единого информационного пространства. По мнению специалистов, основным преимуществом сетевидной концепции ведения боевых действий является высокая маневренность частей и соединений, ускорение процессов принятия решений и планирования операций.*

**Ключевые слова:** сетевидная война, информационная сеть, информационное пространство.

## NETWORK CENTRIC WARFARE CONCEPT OF CONDUCTING WAR XXI OF CENTURY

I.V. Titov

*In article the essence and the information aspects of one of modern approaches to conducting war XXI of century – Network Centric Warfare are opened. One of the major factors caused occurrence Network Centric Warfare as war of new generation, revolution is in the field of information technologies which recently has captured also military sphere. The concept Network Centric Warfare defines new principles of management of armies and forces and provides first of all association of all participants of operations within the framework of uniform information space. In opinion of experts, the basic advantage Network Centric concepts of conducting operations is the high maneuverability of parts and connections, acceleration of decision-making processes and planning of operations.*

**Keywords:** Network Centric Warfare, information grid, information space.

## Список літератури

1. Галка О.І., Льяшов О.А., Павлюк Ю.М. Основні тенденції розвитку та ймовірні форми воєн і збройних конфліктів майбутнього // Наука і оборона. – 2007. – № 4. – С. 10-15.
2. Романченко І.С., Сбитнев А.І. Мережоцентрична система ведення війни – міф XXI сторіччя чи виклик Збройним Силам України? // Наука і оборона. – 2006. – № 3. – С. 12-17.
3. Ставка на «войны будущего». [Електронний ресурс]. – Режим доступу: [http://nvo.ng.ru/concepts/2007-05-17/1\\_future.html](http://nvo.ng.ru/concepts/2007-05-17/1_future.html).
4. Московский А. Революция в военном деле как концепция реализации научно-технического и экономического превосходства США в войнах будущего [Електронний ресурс]. – Режим доступу: <http://www.pvgs.org/rus/pub3r.htm>.
5. Военные известия [Електронний ресурс]. – Режим доступу: <http://PCWeek/UA/2008-08-2.html>.
6. Д. Федутин Тенденции развития систем передачи данных при использовании БЛА // Зарубежное военное обозрение. – 2006. – № 4. – С. 23-27.
7. Проект Marti: новый сценарий сетецентрической войны [Електронний ресурс]. – Режим доступу: <http://CNews.ru>
8. Л. Разгуляев Перспективные мобильные адаптивные сети передачи информации для СВ США // Зарубежное военное обозрение. – 2008. – № 1. – С. 35-39.
9. Державна програма розвитку Збройних Сил України на 2006-2011 роки (основні положення). – К.: Міністерство оборони України, 2006. – 40 с.
10. Біла книга 2007. Оборонна політика України. – К.: Міністерство оборони України, 2008. – 120 с.
11. Тітов І.В., Слюсар В.І. Інтегрована інформаційно-телекомунікаційна система // Тези доповідей XI міжнародної молодіжної науково-практичної конференції «Людина і космос». – Дніпропетровськ: НКАУ. – 2007. – 183 с.

Надійшла до редколегії 16.09.2008

**Рецензент:** д-р техн. наук, проф. В.І. Слюсар, Центральний НДІ озброєння та військової техніки ЗС України, Київ.