УДК 316.259+355.01
DOI: 10.25140/2411-5363-2020-3(21)-163-184

Віталій Зацерковний, Павло Савков, Ігор Пампуха, Ірина Синявська

ОЦІНКА ПЕРЕВАГ МЕРЕЖЕЦЕНТРИЗМУ ТА МЕРЕЖЕЦЕНТРИЧНИХ ТЕХНОЛОГІЙ ДЛЯ РОЗБУДОВИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність теми дослідження. *Зважаючи на зміни характеру ведення сучасних війн і шляхи досягнення інформаційної переваги над супротивником, дослідження мережецентричних технологій є надзвичайно актуальним. Підвищення маневреності підрозділів, їхньої здатності до виконання бойових завдань на підставі безперервного інформаційного супроводження дає можливість отримати значну перевагу над противником, попереджувати, запобігати та знешкоджувати реальні та потенційні загрози національній безпеці.*

Постановка проблеми. *Сучасний рівень автоматизації, інформатизації та системи управління Збройних сил України за сукупністю значень характеристик своїх основних складових частин не відповідає сучасним вимогам*

Аналіз останніх досліджень і публікацій*. Розглянуто проблематику зовнішніх інформаційних впливів та інформаційних аспектів забезпечення національної безпеки держави, концептуальні проблеми війни й миру та проблему мережецентричних війн.*

Виділення недосліджених частин загальної проблеми. *Основною проблемою застосування принципів мережецентризму під час організації сучасного бою є недостатньо ефективні та неадаптовані до сучасних вимог інформаційні системи.*

Постановка завдання. *Першочерговим завданням є формування ефективної інформаційної системи на основі мережецентричних технологій, що дозволить скоротити час на прийняття рішення та прогнозувати можливі варіанти розвитку ситуацій та запобігати можливим наслідкам.*

Виклад основного матеріалу. *Завдяки прогресу у сфері інформаційно-комунікаційних технологій (ІКТ) з'явились нові зразки високоточної зброї, сучасні засоби розвідки, автоматичні і автоматизовані системи управління (АСУ) військами та зброєю. Комп'ютерні технології дали можливість керувати зброєю на відстані в кілька тисяч кілометрів, формувати високоточні точкові удари, корегувати дії військових підрозділів, здійснювати дії військових формувань відразу в декількох напрямках з метою знищення об'єктів супротивника або захоплення його території, досягати результату за короткий проміжок часу тощо. Необхідність максимального використання можливостей всіх наявних засобів розвідки і бойових платформ спричинила перехід від платформоцентричної моделі управління військами і зброєю, де основний акцент робився на кількість озброєння та військової техніки, до мережецентричної.*

Висновки відповідно до статті. *Визначена роль мережецентричних війн та їхній вплив на розвиток збройних сил передових в економічному сенсі країн. Застосування мережецентричних підходів спричинило появу чималих нових нетрадиційних форм і способів збройної боротьби, таких як «спеціальна операція», «тривимірна повітряно-наземна форма удару по супротивнику», «далекій вогневий бій» тощо, під час яких кораблі і підводні човни, літаки, космічні апарати, безпілотні літальні апарати (БПЛА), танки, польові радіостанції і портативні комп'ютери тощо спільно використовували інформацію за допомогою єдиних інтерфейсів, стандартів і протоколів. Визначені складові високої ефективності мережецентричних війн.*

Ключові слова: *інформаційна перевага; єдиний інформаційний простір; мережецентризм; мережецентрична система управління; мережецентрична війна.*

Рис.: 8. Бібл.: 42.

Актуальність теми дослідження. Розвиток людства наприкінці XX ст. ознаменувався глобалізацією та інформатизацією, які спричинили широкомасштабні зміни в економічній, соціальній, політичній, науково-технічній, культурній сферах та стрімкий розвиток інформаційно-комунікаційних технологій (ІКТ). Відбулось формування нового типу суспільних відносин та становлення інформаційного суспільства, де більшість працюючого населення зайняті виробництвом, збереженням, переробкою та реалізацією інформації, особливо її найвищої форми – знань [1]. Характерними особливостями цього суспільства стали революційні зміни в інформаційному менеджменті, діджиталізація (від англ. *digital* – цифровий), у результаті застосування якої більшість засобів комунікації та фіксації зовнішнього світу стали цифровими, швидкий розвиток робототехніки, штучного інтелекту, віртуальної реальності, інформаційних мереж і розвиненої інформаційної інфраструктури, вільний доступ людства до інформації, 3D-моделювання тощо.

Актуальність роботи зумовлена новими викликами, які постали перед людством взагалі та перед Україною зокрема в процесі глобалізації в усіх її вимірах та на всіх її рівнях. Автоматизація процесів повсякденної та бойової діяльності може підвищити бойові можливості військ (сил) на 15–30 % і одночасно на 50 % скоротити час, який витрачають органи управління на оперативне планування і доведення завдань до підлеглих. Проте нині збройні сили України (ЗСУ) надзвичайно повільно просуваються в цьому технологічному

напрямку. Рівень автоматизації діяльності органів військового управління (ОВУ) ЗСУ становить лише 10–30 % від потреб. Наявні комплекси засобів автоматизації та програмно-технічні комплекси не складають цілісних систем, чинні інформаційно-розрахункові задачі забезпечують лише мінімальний набір функціональності – не більше за 12–15 % від загальної кількості елементарних функцій посадових осіб органів військового управління [2].

Особливої гостроти набули проблеми теоретичного осмислення та практичного впровадження стратегії різних форм інформаційного протиборства, інформаційних війн та військово-інформаційної безпеки в різноманітних контекстах конфліктного розвитку світової спільноти.

Постановка проблеми. Трансформація ІКТ збільшила інформаційний простір та просторові параметри сучасного соціуму, який уже не може обходитись без електронних текстових документів, миттєвого обміну повідомленнями (англ. *instant messaging*), цифрової форми подання об'єктів, використання інформаційних ресурсів та віртуалізації виробництва, конвергенції та динамізму соціальних процесів тощо.

Зміни, що відбулись і продовжують відбуватись в інформаційному суспільстві, зажадали перегляду старих парадигм управління з погляду прийняття рішень, їх виконання і контролю, оскільки ієрархічним системам управління властиві жорсткі механізми координації дій підпорядкованих сил і засобів, а зміст, швидкість доставки, формати і якість інформації головним чином визначаються процесами виконання формальних вимог управління.

Управління сучасними складними системами, кількість яких із кожним днем зростає, спонукає відмовитись від жорсткої ієрархії управління, вимагає координації дій самостійних суб'єктів у реальному часі, їх гармонічної взаємодії з оточенням, а також синергії знань, інтуїції та інтелекту всіх учасників щодо забезпечення функціонування таких систем. У цих умовах стає все важче отримувати необхідну інформацію, без опанування потужних можливостей, що надаються інформаційними мережами світу. Це спричиняє пошук нових оригінальних ідей і підходів до управління в термінах самоорганізації, хаосу, динаміки складних систем, управління знаннями і колективного інтелекту. Як наслідок, виникла концепція і теорія мережецентризму та поява мережецентричних систем управління.

Основна ідея концепції мережецентричного управління лежить у підвищенні ефективності інформаційного забезпечення процесів управління.

Ефективність мережі зростає лінійно зі зростанням кількості її елементів і експоненційно – зі зростанням кількості зв'язків між ними. Впровадження в організаційну структуру системи управління мережевих елементів дозволяє підсилити взаємодію між окремими її ланками і зробити їх більш інформаційно насиченими. Раніше це зробити було неможливо, оскільки складність і заплутаність таких організаційних структур могли не тільки загальмувати, а часом і взагалі паралізувати процес управління [3].

Перевага ідей мережецентризму спричинила їхнє повсюдне впровадження майже у всі сучасні технології (інформаційні, соціально-гуманітарні, мобільно-комунікативні, системи швидкого обміну повідомленнями, блоги, соціальні мережі, мережеві онлайн-ігри тощо). Не були осторонь від впровадження і збройні сили (ЗС) передових країн. На базі новітніх інформаційних розробок стали з'являтись нові програмні, апаратні та сенсорні рішення, які дозволили скоротити цикл бойового управління, надавати командирам різного рівня та підрозділам на полі бою можливість перебування у стані «ситуаційної обізнаності» з чітким усвідомленням та фіксацією власного розміщення та завдань, місця та дій дружніх підрозділів, розташування та прогнозованих оцінок дій ворога. З'явились нові види високоточної зброї, засоби розвідки, автоматизовані системи управління (АСУ) військами та зброєю, нові концепції ведення війн і збройних конфліктів. Йде постійний процес удосконалення форм і способів застосування військ.

Інтеграція учасників бойових дій, об'єктів і пунктів управління військами і зброєю в єдиний інформаційний простір (ЄІП) дала можливість одержання синергетичного ефекту за рахунок повного використання доступних інформаційних ресурсів, підвищення якості взаємодії та рівня самосинхронізації та оперативності управління підпорядкованими силами й засобами, бойовими засобами і платформами [4; 5].

Аналіз останніх досліджень і публікацій. Теоретичні засади проблем забезпечення національної безпеки України викладено в працях учених О. Бодрука, Ю. Бута, О. Власюка, В. Горбуліна, А. Качинського, В. Крисаченка, О. Маначинського, М. Ожевана, Б. Парахонського, С. Пирожкова, Г. Сащука, Т. Стародуб, В. Телелима, В. Толубко, В. Циганова, О. Шевченка та ін.

Проблема зовнішніх інформаційних впливів та інформаційних аспектів забезпечення національної безпеки держави досліджувалась у працях: В. Бондаренка, Дж. Брауна, О. Вусатюка, Г. Джоветта, Д. Дубова, С. Кара-Мурзи, О. Литвиненка, А. Манойла, С. Недбаєвського, М. Ожевана, В. Петрика, Г. Почепцова. Серед закордонних авторів слід звернути увагу на дослідження Г. Почепцова, З. Бжезінського, Дж. Ная, Д. Белла, М. Кастельса, Д. Дарендорфа, К. Дойча, Г. Джоветта та інших.

Концептуальні проблеми війни і миру розглядаються в працях: Р. Арона, К. Гаджієва, К. Клаузевіца, Б. Ліддел-Гарта, Н. Макіавеллі, Х. Мольтке, К. Поппера, П. Прудона, Є. Рибкіна, С. Тюшкевича, М. Цюрупи, А. Швейцера та ін.

Із суто методологічного погляду проблему мережецентричних війн досліджували А. О. Зінченко, В. І. Слюсар, K. Cebrowski, Garstka John J., D. S. Alberts, А. А. Амбарцумян, Ю. С. Затуливетер, Дж. Арквілла та інші.

Виділення недосліджених частин загальної проблеми. Прогрес у створенні та вдосконаленні озброєння та військової техніки завжди здійснював істотний вплив на війни та форми їх ведення [6]. Розробка озброєння, його модернізація, як свідчить історія, завжди йшли від засобів індивідуального до засобів групового, а згодом і масового ураження, а військової техніки – шляхом створення і вдосконалення бойових платформ, від стародавніх колісниць та бойових слонів, до сучасних танків, бронетранспортерів, літаків, кораблів, підводних човнів, ракетних комплексів різного типу та космічних засобів.

На той час цілком виправданим був підхід підрахунку танків, літаків, підводних човнів, артилерійських гармат, авто- і мототехніки, кількості бійців тощо. У кого більше таких ресурсів, той і сильніше. Але сьогодні в армії конкурують уже не стільки активи, скільки моделі управління, де ключова роль належить двом складовим: інформації та часу. Час та інформація – це нематеріальні активи нарощування бойового потенціалу. У підсумку більш стійким є той, хто має більше інформації, швидше її обробляє, швидше приймає рішення і завдає свій удар у найбільш вразливе місце ворога. Збройні сутички, по суті, стають протиборством пунктів і центрів бойового управління й командних систем загалом. Конкурують уже не платформи, якими б сучасними вони не виглядали. Танки, БТР, артилерійські та ракетні системи так і будуть мертвим металом, якщо їхні розрахунки та екіпажі не зможуть отримати бойове завдання відповідно до ситуації. Засоби розвідки, зв'язку, цілевказівки, ураження також втрачають свою автономну самодостатність. Конкурують моделі та системи управління. Адже тільки в сучасній системі управління військами можна забезпечити кардинальний приріст бойових можливостей. Саме тому сьогодні у ЗС передових країн світу широко застосовується підхід на базі C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance), який і позначає взаємопов'язане існування та розвиток систем управління, зв'язку й розвідки на основі автоматизації процесів взаємодії.

Постановка завдання. Розробка концепції ГІС ВП, підходів щодо її створення, інтеграція ГІС ВП з технологіями ДЗЗ, розробка алгоритмів моніторингу інформаційного простору є першочерговими завданнями в розбудові сучасної української армії.

Об'єкт дослідження – інформаційне середовище функціонування збройних сил.

Предмет дослідження – підходи щодо ведення війн і військових конфліктів.

Мета роботи – оцінка переваг мережецентризму та мережецентричних війн.

Виклад основного матеріалу. Вплив розвитку засобів зв'язку на систему управління військами і зброєю представлений на рис. 1. Динаміка змін об'ємів передачі інформації в тактичній ланці управління з розвитком засобів зв'язку представлена на рис. 2.

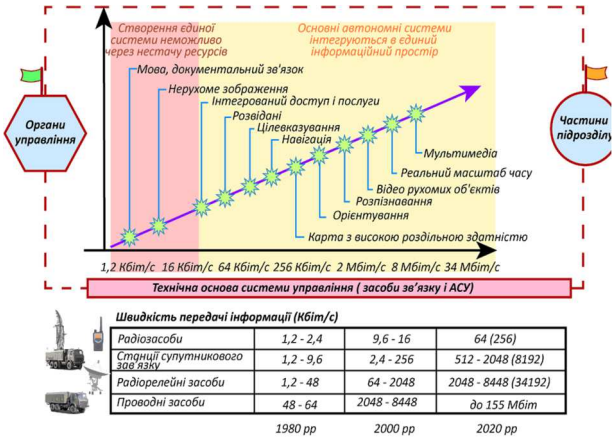

Рис. 1. Вплив розвитку засобів зв'язку на систему управління військами і зброєю [7]

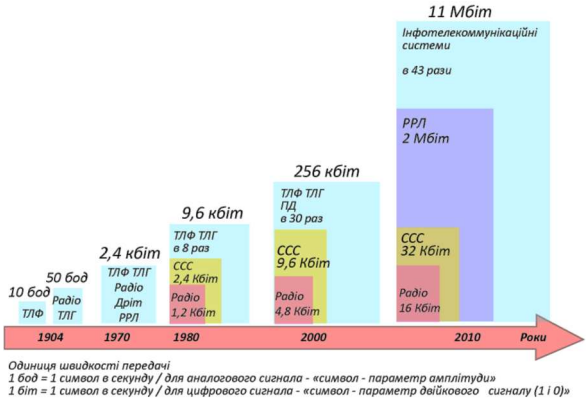

Рис. 2. Динаміка змін об'ємів передачі інформації в тактичній ланці управління з розвитком засобів зв'язку [7]

Рівень розвитку інформаційних технологій, наявність сучасних озброєнь, військової техніки та бойових платформ підвищив ефективність їх застосування на полі бою. Завдяки прогресу у сфері ІКТ з'явились нові зразки високоточної зброї, сучасні засоби розвідки, автоматичні й автоматизовані системи управління військами та зброєю. Комп'ютерні технології дали можливість керувати зброєю на відстані в кілька тисяч кілометрів, формувати високоточні точкові удари, корегувати дії військових підрозділів, спрямовувати дії військових формувань одразу в декількох напрямках з метою знищення об'єктів противника або захоплення його території, досягати результату за короткий проміжок часу тощо. При цьому противник може і не бачити нападника. Сучасні розвідувальні супутники оптичного, інфрачервоного, радіо- і радіотехнічного діапазонів зйомки дозволяють здійснювати безперервне і всепогодне спостереження за територією противника, передаючи розвідані в центри їх обробки практично в масштабі реального часу. Різного роду радіолокаційні станції, в тому числі наземні й повітряні станції дальнього радіолокаційного виявлення (ДРЛО) систем протиракетної і протиповітряної оборони (ПРО і ППО), дозволяють виявляти засоби озброєння противника на великих відстанях, у тому числі за горизонтом [8]. Сьогодні вже навіть сучасного бійця, озброєного стрілецькою зброєю із запасом патронів, підствольним гранатометом і ручними гранатами та із засобами спостереження і зв'язку для обміну інформацією, вважають бойовою платформою, правда з обмеженою вогневою міццю. Але проблеми в системі управління військами часом нівелювали цей прогрес, оскільки час від моменту одержання розвідданих, їх обробки, передачі органам управління для подальшого розрахунку й корегування цілевказівок і до моменту одержання ударними засобами даних про цілі виявлявся неспівставним з очікуваною динамікою бойових дій. А строго централізований та ієрархічний шлях проходження розвідувальної і командної інформації практично зводив нанівець потенційні ударні можливості різного роду бойових платформ [9].

Отже, бурхливий розвиток інформаційних технологій, якісні та кількісні зміни озброєння і військової техніки, засобів розвідки і спостереження за противником, необхідність удосконалення засобів автоматизації систем управління, зв'язку і передачі даних на межі століть привели до усвідомлення необхідності зміни форм і методів управління збройної

боротьби. Крім того, як свідчив досвід, у ході війн і збройних конфліктів дедалі частіше виникла необхідність раціонального використання бойової потужності різного типу бойових платформ зі звичайною зброєю, розкриття всіх їх потенційних можливостей. Стало очевидним, що успіх уже не міг забезпечуватись одним видом зброї: перемога потребувала злагодженої взаємодії всіх видів і родів військ – флоту, авіації, ракет середньої і малої дальності, артилерії, танків і піхоти [10-14].

Ефективне управління всіма видами й родами військ стало вимагати інтеграції наявних різнорідних АСУ військами і зброєю в єдину завадостійку систему управління і зв'язку для одержання інформаційної технічної переваги над противником, яка б ґрунтувалась на трьох складових: оперативному одержанні інформації, адекватному розумінні ситуації в бойовому просторі, ефективному використанні кожної бойової платформи. Наявність великої кількості різноманітної інформації про противника і свої сили та засоби на різних рівнях управління також вимагало подальшого розвитку систем і засобів збору, збереження та обробки інформації, її аналізу, оцінки й моделювання розвитку сценаріїв розвитку бойової обстановки, підготовки командуванням варіантів найбільш ефективних управлінських рішень, тобто досягнення інформаційної переваги над супротивником.

Одним із перспективних шляхів досягнення інформаційної переваги стало створення комплексів інформаційних мереж – технічної основи АСУ військами і зброєю та організація горизонтальних і вертикальних зв'язків для забезпечення обміну даними між будь-якими об'єктами в зоні бойового простору в реальному часі.

Наприкінці XX – початку XXI ст. на Заході почали активно розроблятись нові концепції війн – концепція асиметричної війни (англ. *asymmetric warfare*), конфлікт із нульовою сумою, конфлікти з ненульовою сумою, конфлікти з від'ємною сумою, конфлікти малої інтенсивності, м'якої сили, технології керованого хаосу, мережецентричної війни (МЦВ, англ. *Network Centric Warfare – NCW*), багатодоменного протистояння (англ. *Multidomain battle, MDB*) тощо, удосконалюватись форми і способи застосування військ.

Серед цього розмаїття концепцій досить перспективною виявилась концепція МЦВ, яка не тільки завоювала своїх чисельних прихильників, але й була прийнята за основу діючих програм розвитку та удосконалення ЗС багатьох передових в економічному сенсі країн світу і на сьогодні вже пройшла практичну апробацію в ході реальних військових конфліктів. Проте широко уживаний термін МЦВ є некоректним перекладом з англійської мови терміна «network-centric warfare (NCW)» – мережецентричні військові дії [15], оскільки йдеться не про нову форму або способи ведення військових дій (хоча принципово не виключається їх поява, наприклад, інформаційний вплив, інформаційна атака, інформаційна битва, інформаційна операція тощо), а про мережецентричний підхід до організації і ведення таких дій. Але оскільки термін МЦВ вже «прижився», то завдання полягає не в тому, щоб його змінити, а в тому, щоб його правильно розуміти і вживати.

Мережецентричність – комплексна властивість системи, що включає в себе різні компоненти: інфраструктуру, платформи, підсистеми, процеси і людей по стійкій глобально взаємозв'язаній інформаційно-мережевій взаємодії, при якій інформація для її спільного використання надається компонентам системи своєчасно і безшовно [16].

Сучасному розумінню мережецентризму передує велика кількість етапів, пов'язаних з об'єднанням пунктів управління (ПУ) і зв'язку, автоматизованих систем управління та обчислювальної техніки, їх підключення до вже сформованої мережі управління озброєнням, різноманітних засобів розвідки, високоточної зброї, а також зв'язку і передачі даних, здатних інтегруватися в уже розгорнуту систему управління на театрі війни й забезпечувати доведення інформації до користувачів у реальному часі.

Мережецентрична система управління – система управління розподіленою інформаційною системою, в якій її базові елементи (сили і засоби спостереження, АСУ й особи,

що приймають рішення (ОПР), а також підпорядковані сили і засоби, об'єднані в ЄІП. При цьому така система управління характеризується принципами відкритості, самоорганізації, слабкої ієрархії в контурі прийняття рішень і здатністю породжувати цілі всередині себе. Така інтеграція підвищує можливості інформаційної взаємодії і робить неефективними існуючі способи дестабілізуючого впливу, орієнтовані на придушення або ураження окремих елементів системи управління. Це відбувається через те, що ці способи переважно спрямовані на порушення процесів передачі даних, характерних для ієрархічних систем управління. При мережецентричному підході ці дії є неефективними, завдяки створенню високозв'язного мережевого середовища в складі єдиного інформаційного простору (ЄІП), коли для передачі інформації можна використовувати безліч шляхів, при цьому порушення функціонування окремих ліній або підмереж зв'язку не буде критичним для порушення управління мережецентричної системи загалом.

Фактично, мережецентричні системи управління – це матричні інформаційно-керуючі системи, в основі яких лежить глобальний інформаційний взаємозв'язок її елементів [17]. Для такої системи характерними є не тільки вертикальна інтеграція між силами й засобами спостереження, ПУ і підпорядкованими силами і засобами, але й розгалужена мережа горизонтальних зв'язків на тому ж самому рівні управління між різнорідними елементами системи, які є джерелами і споживачами інформації, що циркулює в системі [17].

Аналіз війн і військових конфліктів кінця XX – початку XXI століть засвідчив, що основними факторами, які впливали на збройну боротьбу, стали фізико-географічні умови ведення збройної боротьби, розвиток засобів збройної боротьби, особливості підготовки повітряно-наступальних та повітряно-наземних наступальних операцій. Характерною тенденцією проведення операцій стало залучення багатонаціональних сил. Особливого значення набув підготовчий період, який об'єднав повітряно-морську транспортну, розвідувальну операції, операцію з забезпечення життєдіяльності військ. Характерним для цього часу стала демонстрація сили (зосередження вздовж берегів імовірного супротивника значних сил флоту, проведення широкомасштабних навчань, перебазування авіації на передові аеродроми тощо), який тривав близько п'яти місяців [18].

Військові конфлікти (війни) у Перській затоці (1991 р. – операція «Буря в пустелі», 2003 р. – операція «Свобода Іраку»), в Югославії (1999 р. – операція «Союзницька сила»), в Афганістані 2002 р. – «Непохитна свобода»), Сирії (2016-2020 рр.) стали конфліктами високих технологій та набули специфічних рис: рішучості в досягненні політичних цілей, спрямування на параліч систем державного, військового управління і критичної інфраструктури супротивника, динамічності, швидкоплинності, високої технологічності застосовуваних засобів. Вирішальне значення для досягнення перемоги стало застосування багатонаціональними силами засобів збройної боротьби, створених на базі новітніх технологій, зокрема безпілотних літальних апаратів (БПЛА), керованих авіаційних засобів ураження, засобів радіоелектронної боротьби (РЕБ), розвідки, автоматизованого управління військами та зброєю [19; 20].

Досвід ведення бойових дій регулярними військами проти іррегулярних збройних формувань засвідчив, що застосування військ мало певні особливості:

– по-перше, виконання завдань здійснювалось об'єднаннями військ різновидової і різновідомчої належності за відсутності чітко вираженої лінії фронту на розрізнених, нерідко ізольованих напрямках, у відриві з'єднань, частин і підрозділів від головних сил при високому ступені самостійності в умовах, коли супротивник широко застосовував засади, партизанські способи боротьби, нічні дії і зазвдавав раптові удари;

– по-друге – поставлені завдання вирішувались шляхом переважно нетрадиційних способів, різними загонами і групами, сформованими за цільовим призначенням;

– по-третє – підготовка бою і управління з'єднаннями, частинами і підрозділами різко ускладнювалась унаслідок одночасного ведення бойових дій у декількох різних районах за наявності відкритих фронтів і розтягнутих тилових комунікацій.

Під час бойових дій з'явилось чимало нових нетрадиційних форм і способів збройної боротьби: «спеціальна операція», «тривимірна повітряно-наземна форма удару по супротивнику», «далекій вогневий бій» тощо, під час яких кораблі й підводні човни, літаки, космічні апарати, БПЛА, танки, польові радіостанції і портативні комп'ютери тощо спільно використовували інформацію за допомогою єдиних інтерфейсів, стандартів і протоколів [21].

Одним з елементів спеціальної операції стали спеціальні військові дії, що здійснювались загальновійськовими з'єднаннями, частинами у взаємодії з формуваннями інших силових структур. Їхнім змістом стали ізоляційно-обмежувальні, розвідувально-пошукові, ударно-вогневі і рейдово-штурмові операції, спрямовані на розгром незаконних збройних формувань. Поява даної форми тактичних дій обумовлена тим, що в збройних конфліктах традиційні види бою (наступ і оборона) уже не охоплювали весь зміст збройного протиборства з іррегулярними формуваннями противника [22].

Потрібно також відзначити ефективну організацію багатонаціональними силами коаліції радіоелектронного придушення об'єктів супротивника. Новим елементом у РЕБ стало руйнування телевізійних передавальних центрів і радіомовних станцій. Актуальними стали такі форми дій, як «електронний удар», «електронний наступ», «операція з виведення із ладу автоматизованих, комп'ютерних систем управління» тощо.

Таким чином, необхідність максимального використання можливостей всіх наявних засобів розвідки і бойових платформ спричинила перехід від «платформоцентричної» моделі управління військами і зброєю, де основний акцент робився на кількість озброєння та військової техніки, до «мережецентричної» (рис. 3), яка являє собою сталу систему поглядів на військово-технічне забезпечення та ведення бойових дій в умовах тотальної комп'ютеризації сил і засобів збройної боротьби.

Узагальнена структура мережецентрчної системи управління представлена на рис. 4, де абревіатура ТКМ позначає телекомунікаційні мережі.

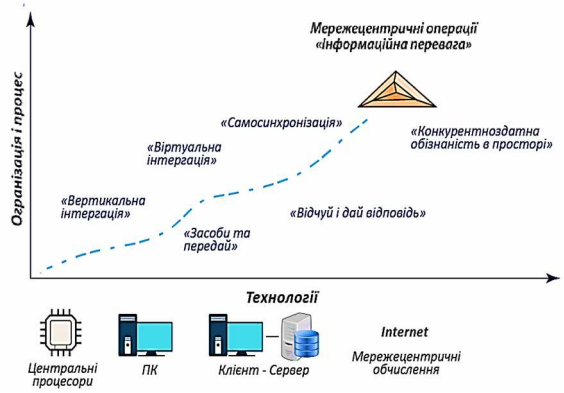

Рис. 3. Еволюція технологій і перехід до мережецентричних операцій [23]

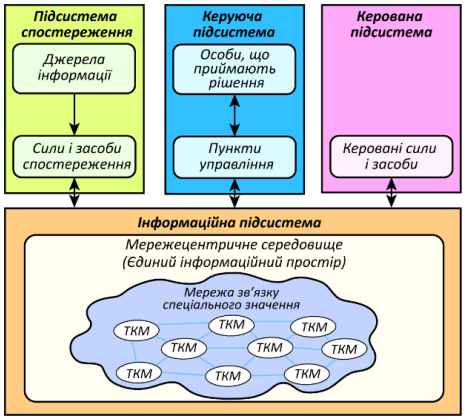

Рис. 4. Узагальнена структура мережецентричної системи управління [24]

Термін «мережецентризм» уперше з'явився в американській комп'ютерній індустрії і став результатом прориву в інформаційних технологіях, який дозволив організувати інтероперабельну взаємодію між комп'ютерами, незважаючи на використання в них різних операційних систем спочатку у США а потім і в усьому світі.

Цілком природно, що й ідеологами військового застосування цього терміна також стали американці. У середині 1990-х років група співробітників корпорації «РЕНД» під керівництвом Дж. Аркілли і Д. Ронфельдта розробила підходи щодо ведення мережевих війн (МЦВ), які вони виклали у статті «Пришестя мережевої війни» [25].

Подальша розробка теорії МЦВ (emerging theory of war) пов'язана з іменами колишнього міністра оборони США Дональда Рамсфелда і військового чиновника Пола Вулфовіца. Безпосередніми розробниками концепції МЦВ вважаються віцеадмірал Артур К. Сібровські – керівник Офісу реформування ЗС США (Office of the Force Transformation) і науково-технічний радник управління систем С4 (Командування, управління, зв'язок, комп'ютерні мережі) Об'єднаного штаба ЗС США Джон Гарстка, які перші використали термін «мережецентричний» (Network Centric) і опублікували основні положення концепції в журналі «Proceedings» у січні 1998 р. у статті «Мережецентрична війна: її походження і майбутнє». Себровскі і Гарстка побудували свою публікацію на прикладах із галузі економіки, включаючи фінансовий сектор, і деяких позитивних результатах з проведених реформ, наприклад, зміни структури і методів роботи поліції Нью-Йорка. Вони зазначали, що МЦВ і пов'язані з нею революції у військовій справі відбуваються і черпають свою енергію з кардинальних змін в американському суспільстві. Попереду цих змін знаходяться коеволюція економіки, інформаційних технологій, бізнес-процесів і організацій, а вони зв'язані одне з одним трьома темами:

– зміщенням акценту з платформи на мережу;

– перехід від розгляду діючих осіб як незалежних суб'єктів до їх розгляду як частини екосистем, що постійно адаптуються;

– важливість прийняття стратегічних рішень, спрямованих на адаптацію або навіть виживання в таких змінюваних екосистемах.

Доопрацьована і детально представлена концепція була опублікована в праці [25].

Концепція МЦВ була прийнята і реалізована на практиці Пентагоном як доктрина і польовий статут під час президентства Дж. Буша-молодшого (2001-2009 рр.).

Ключовим поняттям концепції МЦВ є «мережа» (англ. *the network*), новий інформаційний простір, де розгортаються основні стратегічні операції як розвідувального, так і військового характеру, а також їхнє медійне, дипломатичне, економічне і технічне забезпечення. Війна стає мережевим явищем, а військові дії – різновидом мережевих процесів. Регулярна армія, всі види розвідок, технічні відкриття, високі технології, журналістика і дипломатія, економічні процеси і соціальні трансформації, цивільне населення і кадрові військові регулярні частини і окремі слабо оформлені групи – усе це інтегрується в єдину мережу (в єдиний інформаційний простір, ЄІП), де циркулює інформація.

З технічного погляду в основу концепції МЦВ покладені стандартизація, уніфікація та комплексне впровадження новітніх інформаційних технологій, що дозволяє створити єдиний інформаційно-комунікаційний простір. Як наслідок, відбувається інтеграція складових інформаційного простору з мережами засобів ураження, бойового і тилового забезпечення, засобів розвідки і контррозвідки, зв'язку, органів управління формування громадської думки, дипломатичних відомств, релігійної, колективної і етнопсихології, економічного забезпечення, академічної науки, технічних інновацій моніторингу соціальних процесів тощо, між якими здійснюється постійний інформаційний обмін. Доступ до інформації в ЄІП регламентується відповідними повноваженнями.

Інтеграція сенсорів (датчиків, джерел даних), осіб, що приймають рішення та виконавців, забезпечило доведення до учасників дій необхідної інформації про ситуацію, прискорило процес управління силами і засобами і сприяло підвищенню темпів проведення військових операцій, маневреності військ і ефективність ураження супротивника їх ситуаційну боєздатність і, врешті-решт, бойову міць [26].

Швидкість прийняття рішень є процесом, при якому позиція інформаційної переваги перетворюється в конкурентну перевагу.

Концепція МЦВ – це не тільки розгортання цифрових мереж з метою забезпечення як вертикальної, так і горизонтальної інтеграції всіх учасників операції. Це ще і зміна тактики дії перспективних формувань із розосередженими бойовими порядками, оптимізація способів розвідувальної діяльності, спрощення процедур узгодження та координації вогневого ураження, а також деяке нівелювання розмежування засобів між ланками управління.

Підвищення бойових можливостей сучасних формувань – прямий наслідок поліпшення інформаційного обміну і зростання ролі самої інформації, тобто реалізації принципів нової концепції. Це нова форма і спосіб управління ЗС в організації і веденні бойових дій, де в центрі уваги виявляється мережа, найбільшим важливим аспектом якої є принципи організації і багато в чому самоорганізації (самосинхронізації), під якою розуміють здатність військової структури самоорганізовуватись знизу, а не змінюватись згідно з указівками зверху.

Жорстка ієрархічна система військового управління замінюється гнучкою мережевою: підпорядковані військові формування отримають свободу у виборі методів дій, а організаційно-штатна структура військ передбачає постійні зміни, адаптування до вимог обстановки на полі бою [15].

Мережецентричні дії засновані на доступі командира до всієї необхідної йому інформації режимі реального часу, за рахунок створення спеціальної мережі, яка дозволяє йому одержувати всю необхідну інформацію і віддавати накази. Це ключовий момент у цій концепції, оскільки за допомогою комп'ютера і зв'язку, командир може одночасно швидко з'єднуватися й бачити кожний військовий підрозділ, кожну бойову платформу, бійця, знати, що він бачить, що чує, що робить. Відповідно підрозділи, платформи й окремі бійці можуть бачити ситуацію на полі бою. Також завдяки силам розвідки в них є змога бачити і противника, де він перебуває і в якій кількості. Водночас противник навіть не здогадуватиметься, що його вже повністю розвідали. І кожної секунди командир може контролювати все поле бою [27].

Як відомо з теорії системного аналізу, об'єднання декількох систем, за умови належної взаємодії (зв'язків) дозволяє досягти синергетичного (емерджентного) ефекту, який набагато перевищує суму компонентів її складових і забезпечує три умови успіху на полі бою: беззаперечну перевагу в розвідданих про бойовий простір, практично безпомилкова постановка бойових задач, миттєва й усебічна оцінка ситуації.

Збройні сили, об'єднані надійними інформаційними мережами, отримали можливість якісно нового обміну інформацією, що підвищило якість інформації і рівень загальної інформованості про ситуацію на полі бою (театрі бойових дій), забезпечило такий рівень співробітництва і самосинхронізації, який дозволив підвищити завадостійкість і швидкість передачі команд управління та підвищити ефективність виконання бойових задач. За рахунок інформаційного обміну та зростання значення самої інформації відбулось підвищення можливостей військових формувань щодо вогневого ураження сил супротивника, зростання їх мобільності, ефективності управління силами й засобами мережецентричних сил і врешті-решт, зростання темпів операцій, рівня самосинхронізації бойових дій тощо [28].

Збільшення бойової потужності географічно (просторово) розосереджених, добре екіпірованих і матеріально оснащених військових формувань (мережецентричних сил) відбувається за рахунок утворення переваг в інформаційному протиборстві за рахунок широкого застосування автоматизованих систем управління військовими формуваннями наземного, морського, повітряного і космічного базування, розвідки, моніторингу, РЕБ

наземного, морського, повітряного і космічного базування, зброєю, засобами розвідки тощо й полягає в інтеграції всіх вражаючих, логістичних, інформаційних, дипломатичних, соціальних та інших засобів у мережецентричну систему, яка містить у собі всі рівні й напрями управління [29].

МЦВ може вестись на всіх рівнях військових дій – тактичному, оперативному і стратегічному. Принципи її ведення жодним чином образом не залежать від географічного регіону, бойових задач, складу і структури використовуваних військ.

У концептуально-теоретичному плані Себровскі і Гарстка представили мережецентричну модель у вигляді системи, що складається з трьох підсистем-решіток – глобальної інформаційної, сенсорної (розвідувальної) і бойової (засоби ураження, бойова техніка і особовий склад окремих тактичних підрозділів та бойового управління) і які взаємно перетинаються. Графічна інтерпретація мережецентричного підходу представлена на рис. 5 [31]. Складові схема моделі представлена на рис. 6 [31].

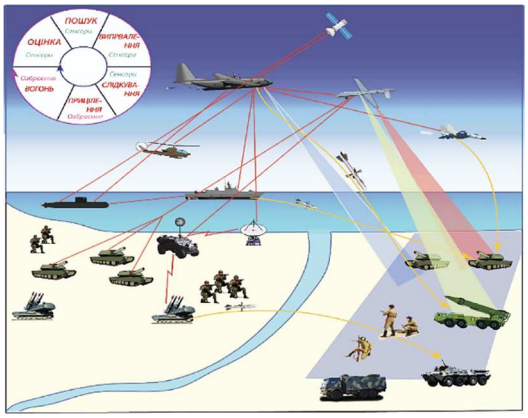

Рис. 5. Мережецентрична концепція ведення бойових дій

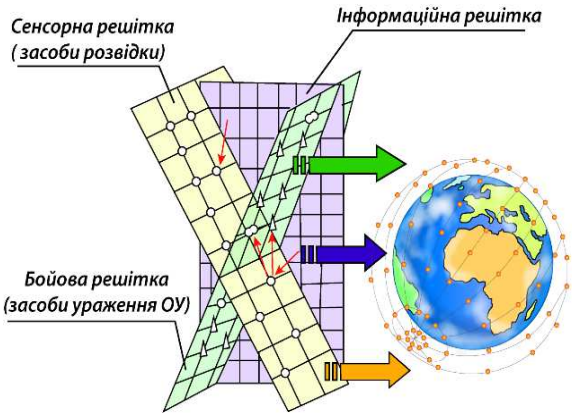

Рис. 6. Складові мережецентричної моделі

Основу ЄІП становить так звана «Глобальна інформаційна решітка» (ГІР, англ. *Global Information Grid – GIG Centric Warfare – NCW*), яка забезпечує командування ЗС можливістю управління військами в бойових умовах на основі інформаційно-керуючих систем. Функціонування ГІР забезпечує потужне угрупування розвідувальних, комунікаційних і навігаційних космічних літальних апаратів на навколоземній орбіті. Це гарантує успішне ведення бойових дій проти супротивника, у якого відсутні подібні системи. Значну частину такої інформації складає космічна інформація, яка є базовою для геоінформаційних систем військового призначення (ГІС ВП) системи підтримки прийняття рішень у бойовій і мирній обстановці.

ГІР поєднує всі сили і засоби ЗС країни евентуального супротивника та її союзників в єдину систему управління, розвідки, вогневого ураження, логістики й забезпечує їх всією необхідною інформацією для ведення війни. ГІР покликана забезпечити абсолютне інформаційне домінування на полі бою, що, у свою чергу, дозволить випередити противника на всіх етапах підготовки і ведення бойових дій [15] є наскрізною (end-to-end), тобто забезпечує можливість накопичення безлічі інформації, її збереження, розповсюдження та надання за запитами. При цьому доступ до повідомлень мають тільки користувачі, що зареєстровані в мережі, для інших, зокрема й передавальних серверів, інформація є недоступною.

ГІР пронизує собою всю систему сучасного управління ЗС США і виступає її основою та містить власні й орендовані комунікації, комп'ютерні системи і сервіси, програмне забезпечення (включаючи додатки), дані, сервіси безпеки, інші пов'язані сервіси і національні системи безпеки США.

У технічному плані перед МО США в особі Агентства з перспективних військових розробок – DARPA, поставлена задача до 2020 року в режимі реального часу поєднати процеси: дешифрування об'єктів супротивника, їх географічну прив'язку, видачу цілевказівок і знищення об'єктів. При цьому для космічної інформації геометричний параметр об'єкта по прив'язці й розміру не повинен перевищувати 1 метр.

Елементами сенсорної решітки виступають засоби розвідки (сенсори або датчики, інформаційні агенти тощо), а елементами бойової решітки є засоби ураження (стрільці). Ці дві групи елементів об'єднуються органами управління і командування.

Зв'язки і відносини між усіма елементами підсистем і самими підсистемами доволі складні й багатопланові, що дозволяє, наприклад, «стрільцям» уражати цілі одразу після отримання інформації від «сенсорів», після отримання наказу від органів управління, або в деяких випадках самостійно [15].

Основним змістом сучасних МЦВ стають спільні центрально-мережеві операції, що являють собою зону боїв і ударів, виконуваних ЗС розосередженими по всьому просторі театру військових дій (ТВД) взаємозв'язаними (єдиним задумом, оперативно, інформаційно тощо) і взаємозалежними різнорідними тактичними формування ЗС.

Головні характерні компоненти розосереджених по всьому ТВД ЗС:

– високоефективна «інформаційна решітка»;

– доступ до всієї необхідної інформації;

– високоточна зброя;

– високоефективна система управління і зв'язку;

– інтегрована «сенсорна решітка», з'єднана в єдину мережу із системою засобів ураження та системою управління і зв'язку.

Активне використання даних отриманих за допомогою аерокосмічної розвідки, безпілотних літальних апаратів (БПЛА), високоточної зброї, захищених стійких каналів зв'язку з високою пропускною спроможністю, засобів радіоелектронної боротьби (РЕБ) дозволяє завдавати безперервні удари по супротивнику з далеких відстаней. При цьому відбувається розгортання комп'ютерних (інформаційних) мереж з метою забезпечення як вертикальної, так і горизонтальної інтеграції елементів бойової побудови, зміна тактики дій військових формувань із розсердженими бойовими порядками, оптимізація способів розвідувальної діяльності, спрощення процедур узгодження та координації вогневого ураження, безперервний оптимальний розподіл цілей і вироблення цілевказівок у зоні відповідальності підрозділу (бойової одиниці), а також нівелювання розмежування засобів по ланках управління. Крім того, розосередженість військових формувань разом зі швидкістю дій мобільних сил дозволяє в реальному часі здійснювати зміни напрямків ударів і введення в оману командування ЗС супротивника, як про свої поточні наміри, так і про загальну оперативну обстановку.

Наразі у Міністерстві оборони США термін «мережецентричний» розуміють як характерну властивість надійного, глобально взаємопов'язаного мережевого оточення, що охоплює інфраструктуру, системи, процеси та людей і в якому дані для спільного використання надаються користувачам повністю та своєчасно [33].

Подальший розвиток концепції МЦВ привів до прийняття Програми FCS (Future Combat System). Головними напрямками наступної реорганізації ЗС США стали: об'єднання всіх систем управління і ведення бою в єдину армійську мережу і максимальна заміна живих солдатів і службовців на автоматизовані і роботизовані системи. А додатковою ціллю FCS, яка логічно випливає з основних, стала заміна техніки і озброєння на більш досконалі й технічо нові зразки з підтримкою роботи в єдиному армійському середовищі мережі [34].

Крім мережецентричної моделі організації і ведення бойових дій подібний підхід застосовується і при проєктуванні так званих мережецентричних інформаційно-керуючих систем (ІКС) спеціального призначення. Найбільш перспективним напрямом розвитку ІКС є матричні ІКС. В їх основі, як і в основі концепції МЦВ, лежить глобальна інформаційна решітка.

На думку розробників концепції, «мережецентричний» спосіб ведення бойових дій дає можливість здійснити перехід від війни на виснаження до швидкоплинної і більш ефективної форми ведення збройної боротьби, характерними особливостями якої є швидкість управління та самосинхронізація, тобто здатність військової структури самоорганізовуватись знизу, не очікуючи вказівок зверху [35]. Крім того, концепція МЦВ відповідає новим вимогам, умовам інформаційного суспільства й найближчим часом «якщо не замінить собою традиційну теорію війни, то істотно, якісно і безповоротно її змінить». Вона може застосовуватись як для мирного, так і для військового часу, охоплювати всі рівні управління, а принципи її ведення не залежать від географічного регіону, бойових задач, складу і структури ЗС. Самі ж ЗС у цьому випадку являють собою розгалужену мережу гарно інформованих, але географічно розподілених сил. МЦВ – не новий тип війни, а новий підхід до організації та ведення бойових дій, де в центрі уваги опиняється інформаційно-комунікаційна мережа. Мережецентричні військові дії характеризуються не тільки забезпеченням передачі розвідувальної інформації всім учасникам цих дій в реальному часі, але й високим рівнем організації (самоорганізації) функціонування елементів бойової побудови, яка проявляється в безперервному оптимальному розподілу цілей та вироблення цілевказівок у масштабі зони відповідальності [21]. Це ще і зміна тактики дій перспективних формувань із розосередженими бойовими порядками, оптимізація способів розвідувальної діяльності, спрощення процедур узгодження і координації вогневого ураження, а також певне нівелювання розмежування засобів по ланцюгах управління [36].

Висока ефективність МЦВ досягається:

– інформаційною перевагою шляхом штучного збільшення потреби супротивника в інформації при одночасному обмеженню доступу до неї; забезпеченню максимально можливого доступу до інформації своїх військових формувань через мережеві механізми й інструментарій зворотного зв’язку при надійному захисті від їх проникнення противника; забезпеченні доступу до широкого спектра оперативного й динамічного інформування;

– забезпеченням загальної поінформованості шляхом побудови інтегративної інформаційної мережі, яка передбачає постійну актуалізацію інформації, що отримується від різних видів розвідки та інших джерел одержання інформації; перетворенням користувачів інформації одночасно і в її постачальників, які одразу ж активують зворотний зв’язок; максимальним захистом доступу до цієї мережі противника при максимальній доступності до неї своїх військових формувань і платформ;

– заміну наказів командира загальними вказівками про завдання; підвищення автономності й самостійності підлеглих; уникненні строгої і однозначної формалізації управління;

– зменшенням циклу прийняття рішень та збільшенням швидкості їх передачі з метою досягнення оперативної переваги; блокуванням реалізації стратегічних рішень супротивника і забезпеченні своєї переваги в змаганні на рівні рішень;

– реалізацією самосинхронізації дій бойових підрозділів практично в автоматичному режимі, самостійному формулюванні і розв’язанні оперативних задач на основі загальної поінформованості і розуміння намірів командира, що істотно підвищує самостійність і творчу ініціативу командирів підрозділів;

– географічним розподілом сил шляхом переходу від лінійної конфігурації на полі бою до точкової конфігурації; контролюванням не величезних просторів, а найбільш важливих стратегічних районів; веденні наступу не фронтальними силами, а точковими підрозділами; забезпеченні високої взаємодії всіх сил для швидкісного маневру;

– демасифікацією, заснованою на використанні інформації для досягнення бажаних ефектів, обмеженням необхідності зосередження великих сил у конкретному місці; збільшенні швидкості й темпу переміщення на полі бою для того, щоб суттєво ускладнити супротивнику можливість своєчасного виявлення такого переміщення. Цей принцип війни вимагає збільшення кількості і якості інформаційних джерел як у районі бойових дій, так і поза ними. А це забезпечується за рахунок інтеграції в єдину систему даних, отримуваних розвідкою, системами моніторингу й розпізнавання, використанням сенсорів (датчиків) як головних маневрових елементів, так сенсорів морально-психологічного впливу [37];

– глибоким сенсорним проникненням, яке забезпечується збільшенням кількості і якості датчиків як у районі бойових дій, так і поза ним шляхом об'єднання в єдину систему даних, отримуваних розвідкою, системами спостереження та розпізнавання; постачанням кожної гармати різноманітними датчиками та інформаційними сенсорами; використанням датчиків і пунктів (точок) спостереження на полі бою і поза ним;

– зміною стартових умов ведення військових дій, яке полягає в попередньому впливі на стартові умови війни шляхом закладання в них такої структури, яка завідомо приведе до перемоги над противником; провокуванням поєднання в часі та просторі подій, які покликані вплинути на потенційного супротивника і блокувати його відповідну ініціативу;

– стиснутістю операції, в яких долаються структурні і процедурні розмежування між різними військовими службами, а повний доступ до різнорідної інформації забезпечується навіть на найнижчому рівні бойових одиниць. За рахунок цього підвищується розгортання і застосування бойової сили та забезпечення боєприпасами; відміняється фрагментація процесів (організація, розгортання, використання, забезпечення тощо) та функціональних сфер (операцій, розвідки та логістики); відмінюються структурні розмежування на низових базових групах;

– застосуванням операцій, що ґрунтуються на ефектах (ОБЕ, англ. Effects-based operations), тобто сукупності дій, спрямованих на формування моделі поведінки друзів, нейтральних сил і ворогів у будь-якій ситуації (миру, кризи або війни). При цьому учасникам нічого не нав'язується прямим чином, але при цьому вони виконують те, що потрібно тим, хто вибудовує цю модель управління.

Графічна інтерпретація переваг мережецентричної моделі бойових дій представлена на рис. 7 [38].

Відповідно до концепції МЦВ стверджується, що сучасні конфлікти розгортаються в чотирьох суміжних сферах: фізичній, інформаційній, когнітивній та соціальній. Кожна з них має важливе самостійне значення, але вирішальним у МЦВ є синергетичний (емерджентний) ефект за рахунок цілеспрямованих дій різних факторів цих структур.

Фізична сфера – це традиційна сфера війни, у якій відбувається зіткнення фізичних сил у часі та просторі. Ця сфера містить у собі середовище ведення бойових дій (море, суша, повітря, космічний простір), бойові платформи і фізичні носії комунікаційних мереж. Цей аспект піддається

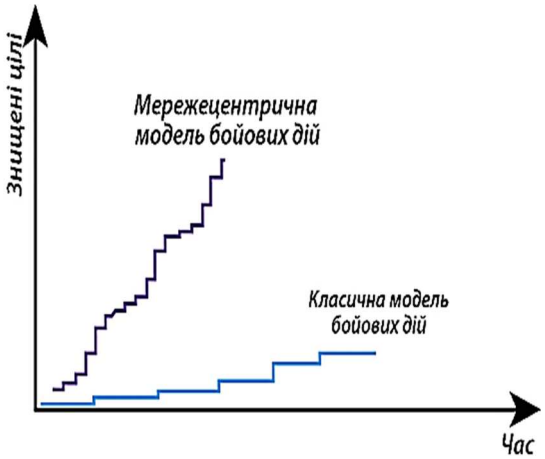

Рис. 7. Переваги мережецентричної моделі бойових дій

виміру й раніше слугував основою при визначенні сили ЗС і їх здатності вести бойові дії. В інформаційну епоху цей чинник є не таким важливим, тому слід розглядати фізичний аспект як деякий граничний ефект дії мережевих технологій, основна частина яких знаходиться в інших сферах, але які проєктують на фізичну сферу свої ефекти.

Інформаційна сфера – це сфера, де створюється, обробляється і розподіляється інформація. Ця сфера покриває системи передачі інформації, базові сенсори, моделі обробки інформації тощо. Це переважне середовище епохи мережевих війн, яка відокремилась в самостійну категорію – «інформосферу» – поряд з фізичними середовищами і набуває важливого значення. Інформаційна сфера в епоху мережевих війн пов'язує між собою всі рівні ведення війни та є найбільш пріоритетною. Переваги або недоліки в накопиченні, передачі, обробці й охороні інформації набувають поступово вирішального значення.

Когнітивна сфера – це здатність бійця до розумового сприйняття і переробки зовнішньої інформації. Саме вона є тим простором, де переважно здійснюється ОБЕ. Усі основні війни й битви розгортаються і виграються саме в цій сфері. Саме в когнітивній сфері знаходяться такі явища, як «намір командира», доктрина, тактика, техніка і процедури. МЦВ надають цьому фактору важливе значення, хоча процеси, що здійснюються в цій сфері, виміряти значно складніше, ніж у фізичній сфері. Але їх цінність і ефективність набагато важливіше.

Соціальна сфера являє собою поле взаємодії людей, де переважають історичні, культурні, релігійні цінності, психологічні установки, етнічні особливості. У соціальному просторі розвиваються стосунки між людьми, вибудовуються природні ієрархії в групах – лідери, відомі, тощо, складаються системи групових відношень. Соціальна сфера є контекстом мережевих війн, яку треба брати до уваги найбільш ретельним чином. Війни інформаційної епохи засновані на свідомій інтеграції всіх чотирьох сфер. З них і створюється мережа, яка знаходиться в основі ведення військових дій [38].

Особливостями мережецентричних війн слугують:

– широка можливість використання географічно розподілених військових формувань. Якщо попередньо через різного роду обмеження була необхідність розташування частин і підрозділів тилового забезпечення в безпосередній близькості до місць дислокації своїх військ або до об'єкта оборони, то нова концепція зняла ці обмеження і практично довела свою ефективність в Іраку. Для організації адресного тилового постачання – основи бойового застосування військ у маневровій війні, армія США використовувала розподілену інформаційну систему Army's Movement Tracing System – MTC, яка на основі радіовипромінювальних датчиків, стаціонарних і портативних сканерів, навігаційної супутникової системи GPS, безпровідного доступу і тактичного Internet безперервно відслідковувала положення всіх наземних рухомих об'єктів (танків, бронетранспортерів, бойових машин піхоти (БМП) тощо) на всьому іракському театрі бойових дій. Від екіпажів наземних рухомих об'єктів підрозділи тилу одержували запити на постачання палива, боєприпасів, запасних частин та інших видів забезпечення. Усього в цій системі було задіяне близько 4000 бортових комп'ютерів і 100 серверів, що працювали під операційною системою Windows NT. Система MTC коштувала армії 418 млн дол. США, отриманих компаніями NSI Global inc. і Comtech Mobile Datacom Corp. за постачання необхідного обладнання протягом трьох років;

– наявність високоінтелектуальних ЗС, які використовують високотехнологічне сучасне інформаційно-комунікаційне обладнання, високоточну зброю, інформацію одержану від всеохоплюючого моніторингу бойового простору, які розуміють наміри командування, мають певні знання та навички і забезпечують значно більшу ефективність, на відмінну від ведення автономних, порівняно розрізнених дій. Перед початком війни (2003 р.) над Іраком були розміщені 40 американських супутників. Це дозволило основній ударній силі, що брала участь в операції «Шок і хвилювання» – 5-му армійському

корпусу самостійно відслідковувати до 1000 наземних цілей супротивника протягом години. Командири ескадрилей палубної авіації могли брати участь у плануванні вильотів своїх екіпажів разом із колегами з армійської авіації, користуючись загальною інформаційною системою, чого, наприклад, не було в 1991 р. Більше того, понад 80 % бойових вильотів авіації проводились «наосліп» (відсутність у пам'яті бойових комп'ютерів літаків попередньо визначених цілей). Інформація про цілі надходила в бортові комп'ютери від наземних частин безпосередньо з лінії зіткнення. Для цього американці розгорнули спеціальну систему бойового планування і управління авіацій на театрі військових дій (ТВД) «TBMCS» (Theater Battle Management Core Systems). Крім того, використовувалась нова розподілена інформаційна система бойового управління FBCB2 (Force XXI Battle Command Brigade or Below), яка охоплювала рівень «бригада – батальйон – рота». Усі командири бойових підрозділів і передові артилерійські наводчики для орієнтування на місцевості і передачі бойових донесень мали в своєму розпорядженні штатні кармані комп'ютери (500 МГц) 4 Гбайт (Windows 95|NT) з міцним корпусом;

– наявність доволі ефективних інформаційних комунікацій між об'єктами в бойовому просторі, що дає можливість географічно розподіленим об'єктам виконувати спільні бойові дії, а також динамічно розподіляти відповідальність і весь обсяг роботи, щоб пристосуватись до ситуації. Це більше ніж у 7 разів (порівняно з 1991 р.) збільшило сумарну смугу пропускання (до 3 ГГц) орендованих Пентагоном каналів супутникового зв'язку для передачі інформації.

Враховуючи особливості проведення МЦВ стосовно до можливого театру бойових дій, концепція передбачає чотири основні фази ведення бойових дій.

1. Досягнення інформаційної переваги за допомогою випереджувального знищення (виведення з ладу, придушення) розвідувально-інформаційного забезпечення супротивника (засобів і систем розвідки (сенсорів), мережоутворюючих вузлів, центрів обробки інформації та управління тощо).
2. Завоювання переваги в повітрі шляхом придушення (знищення) системи протиповітряної оборони (ППО) супротивника.
3. Послідовне знищення залишених без управління і інформації засобів ураження супротивника, насамперед ракетних комплексів, авіації, артилерії, бронетехніки.
4. Остаточне придушення або знищення осередків опору супротивника.

Успішне здійснення кожної з фаз операції ґрунтується на значно меншій тривалості бойового циклу «виявлення – впізнання – цілевказівка – ураження» або циклу «спостереження – орієнтування – прийняття рішення – дії» порівняно з супротивником, на більш точних і повних відомостях про угруповання супротивника [39; 40].

Крім безпосередньо бойових дій, мережентрична парадигма може використовуватись у моніторингу озброєння, боротьбі з тероризмом, підтримці операцій по боротьбі з наркобізнесом і контрабандою, операціях по контролю за виконанням санкцій і перехопленню суден у морі, контролі за збереженням закритих зон, забезпеченням свободи проходження суден і прольоту літаків; наданні гуманітарної допомоги, сприянні цивільній владі, захисту національного суверенітету, проведення антиповстанських операцій; операціях з евакуації мирного населення, миротворчих операцій, захисту судноплавства, рятувальних операціях, операціях з демонстрації сили, проведення каральних ударів і рейдів, наданні підтримки повстанцям тощо [41].

Виявивши, які преференції дає американський підхід, у тому ж напрямку потягнулися і інші країни. Зокрема, в НАТО реалізується концепція «Комплексні мережеві можливості» (NATO Network Enabled Capabilities), у Франції – «Інформаційно-центрична війна» (Guerre Infocentre), у Швеції – «Мережева оборона» (Network Based Defense), у ФРН – Управління через мережу, в Австралії – Комплексна мережева війна, в Китаї –

«Система бойового управління, зв'язку, обчислювальної техніки, розвідки, спостереження і вогневого ураження» (Command, Control, Communications, Computers, Intelligence, Surveillance, Recognizance & Kill) (рис. 8).

Рис. 8. Концепції мережецентричних війн та збройних конфліктів, що розробляються США, НАТО та деякими іншими країнами

Ключовим засобом забезпечення обміну інформацією і спільного її використання в НАТО розглядають ініціативу створення «Федеративної мережі місій» (англ. NATO Federated Mission Networking (FMN)). Міграція FMN на тактичний рівень створює умови для ефективного ведення мережецентричних операцій.

Саме в «мережецентризмі» військові зарубіжних країн бачать інноваційний інструмент підвищення бойових можливостей ЗС, чисельність яких піддається постійному скороченню, і цілком об'єктивно розраховують на отримання економічної вигоди.

Під мережецентричними силами розуміють зброю і війська, які здатні реалізувати концепцію МЦВ.

Звичайно, розглядати концепцію МЦВ як панацею для одночасного вирішення всіх проблем у галузі військового управління не варто. Але застосування комплексного підходу, який передбачає передусім координацію зусиль державного та військового керівництва, зміну їхніх поглядів на управління військовими формуваннями, створення уніфікованих АСУ військами та озброєнням, розробку сучасних технічних засобів розвідки та високоточної зброї, а також підготовку всього особового складу до роботи з новітніми інформаційно-комунікаційними системами, дозволить побудувати ЗС, здатні адекватно реагувати на будь-які загрози національній безпеці нашої держави.

Крім того, аналіз військових конфліктів, зокрема операція «Буря в пустелі», свідчить, що одне з'єднання, оснащене сучасними засобами автоматизації управління військами, може успішно протистояти трьом з'єднанням, не оснащеним такими засобами. Стає очевидним, що з урахуванням ситуації на сході нашої держави, де підрозділи ЗС України змушені протистояти противнику, який має перевагу в чисельності й вогневих засобах, використання концепції МЦВ може стати тим інноваційним напрямом розвитку, що дозволить вивести обороноздатність країни на принципово новий рівень.

Створення єдиної інформаційної мережі здатне в кілька разів збільшити потужність ЗС без збільшення їх чисельності. МЦВ дозволяє піднятись на новий рівень управління військами, суттєво зменшуючи час прийняття рішень. Застосування нових інформаційних технологій дозволяє змінити класичне співвідношення сил як сторони, що наступає, так і сторони, що обороняється на протилежне, за умови, що сторона, яка обороняється, не має можливості вести МЦВ.

Висновки відповідно до статті. Сучасний стан автоматизації діяльності органів військового управління (ОВУ) ЗС України не перевищує 10-30 % від потреб. Проведений авторами аналіз, свідчить, що автоматизація процесів повсякденної та бойової діяльності на основі мережецентричних технологій дає можливість підвищити ефективність засто-

сування військ щонайменше на 15-30 % і одночасно скоротити на 50 % час, який витрачають органи управління на оперативне планування і доведення завдань до підлеглих. Наявні комплекси засобів автоматизації та програмно-технічні комплекси не становлять цілісних систем, чинні інформаційно-розрахункові задачі забезпечують лише мінімальний набір функціональності – не більше ніж 12-15 % від загальної кількості елементарних функцій посадових осіб органів військового управління.

Отже, у чинній (де-факто ручній та голосовій) системі управління керівному складу ЗСУ для вироблення та прийняття рішень залишається лише 15-17 % від часу, відведеного на оперативне планування. За цим показником Україна поступається всім країнам блоку НАТО, членом якого вона прагне стати. В свою чергу, ЗС провідних країнах світу широко застосовують геоінформаційні системи військового призначення (ГІС ВП) для моделювання ситуацій, бойових операцій та прийняття рішень, витрачаючи при цьому до 75-80 % часу оперативного планування, що забезпечує більш глибоке та якісне опрацювання задумів, оптимізує заходи бойового та логістичного забезпечення, мінімізує втрати на полі бою.

Тому, на нашу думку, першочерговими завданнями розбудови сучасної української армії повинні стати розробка концепції ГІС ВП, підходів щодо її створення, інтеграція ГІС ВП із технологіями ДЗЗ, розробка моделей інтероперабельності інформаційних систем, що використовуються в ЗС України, розробка алгоритмів кластеризації та моніторингу інформаційного простору, розробка алгоритмів прогнозування для моделювання сценаріїв розвитку бойових дій в умовах невизначеності.

Список використаних джерел

1. Назарчук А. В. Сетевое общество и его философское осмысление. *Вопросы философии*. 2008. № 7. С. 61–75.

2. Сучасні технології автоматизації управління. URL: http://opk.com.ua/сучасні-технології-автоматизації-управління.

3. Буренок В. М., Ляпунов В. М., Мудров В. И. Теория и практика планирования и управления развитием вооружения / под ред. А. М. Московского. Москва : Изд-во «Вооружение. Политика. Конверсия», 2005. 418 с.

4. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века : монография. Санкт-Петербург : Наукоемкие технологии, 2017. 546 с.

5. Ярош С. П. Завдання дослідження та шляхи створення єдиного інформаційного простору при організації управління військами. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2010. № 3(9). С. 34–41.

6. Кингстон-Макклори Э. Дж. Руководство войной. Анализ роли политического руководства и высшего военного командования / пер. с англ. Н. П. Павлова и Е. М. Михайлова. Москва : Издательство иностранной литературы, 1957. 342 с.

7. Опыт применения беспилотной авиации в вооруженном конфликте на Украине. URL: https://general-skokov.livejournal.com/tag/сетецентрическая%20война.

8. Ковалев В., Малинецкий Г., Матвиенко Ю. Концепция «сетецентрической» войны для армии России: «множитель силы» или ментальная ловушка? URL: http://www.inesnet.ru/wp-content/mag_archive/2013_05/ES2013-05-Kovalev_Malinetsky_Matvienko.Pdf.

9. Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Современные тенденции развития теории и практики управления в вооруженных силах США. Москва : ЛЕНАНД, 2009. 272 с.

10. Слипченко В. И. Войны нового поколения: дистанционные и бесконтактные. Москва : ОЛМА-ПРЕСС образование, 2004. 380 с.

11. Информационные, специальные, воздушно-десантные и аэромобильные операции армий ведущих зарубежных государств: Информационно-аналитический сборник / А. Н. Сидорин и др. Москва : Воениздат, 2011. 344 с.

12. Требин М. П. Войны XXI века. Москва : АСТ, 2005. 608 с.

13. Барышев А. П. Современная стратегия США и НАТО (в контексте проблем национальной безопасности России). Москва : ОГИ, 2011. 248 с.

14. Карякин В. В. Военная политика и стратегия США в геополитической динамике современного мира : монография. Москва : Граница, 2011. 283 с.

15. Попов И. М. «Сетецентрическая война»: готова ли к ней Россия? URL: http://www.milresource.ru/NCW.html.

16. Alberts D. S., Garstka J. J., Stein F. P. Network Centric Warfare: Developing and Leveraging Information Superiority. 2-nd Edition (Revised). US Department of Defense, C4ISR Cooperative Research Program Publications Series, 2001. 292 p. URL: http://www.dodccrp.org/files/Alberts_NCW.pdf.

17. Макаренко А. В. Введение в сетецентрические информационно-управляющие системы. *Конструктивная кибернетика. Исследования. Разработки. Консалтинг*. URL: http://www.rdcn.ru/estimation/2010/03042010.shtml.

18. Слюсаренко А. В. Досвід ведення бойових дій у локальних війнах кінця XX – початку XXI століть, та його використання у підготовці ЗС України. URL http://ena.lp.edu.ua/bitstream/ntb/30909/1/30.pdf.

19. Пермяков О. Ю., Сбітнєв А. І. Інформаційні технології та сучасна збройна боротьба. Луганськ : Знання, 2008. 204 с.,

20. Василенко О. В. Основні світові тенденції розвитку озброєння та військової техніки для ведення війн у майбутньому. *Наука і оборона*. 2009. № 4. С. 18–22.

21. Куприянов А. А. Сетецентрические военные действия и вопросы интероперабельности автоматизированных систем. *Автоматизация процессов управления.* 2011. № 3(25). С. 83-97. URL: http://apu.npomars.com/images/pdf/25_14.pdf.

22. Зайцев Д. В., Шарий В. І., Добровольський В. Б. Розвиток загальної тактики за досвідом локальних війн і збройних конфліктів сучасності, які велись регулярними військами проти іррегулярних збройних формувань. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2015. Вип. 49. С. 117-124. URL: http://nbuv.gov.ua/UJRN/Znpviknu_2015_49_20.

23. Поліщук Л. І., Філімонов С. М. Аналіз деяких систем управління збройними силами країн НАТО та інших держав. *Військовий збірник.* 2009. № 1. С. 85–94.

24. Макаренко С. И. Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями. URL: https://cyberleninka.ru/article/n/podavlenie-setetsentricheskih-sistem-upravleniya-radioelektronnymi-informatsionno-tehnicheskimi-vozdeystviyami/viewer.

25. Arquilla J., Ronfeldt D. The Advent of Netwar. Santa Monica, CA: RAND, 1996. P. 47.

26. Сетецентрическая война. Дайджест по материалам открытых изданий и СМИ. Москва : ВАГШ ВС РФ, 2010.

27. Мережево-центричні військові дії: майбутнє української армії. URL: https://tsn.ua/blogi/themes/o_voine/merezhevo-centrichna-viyna-maybutnye-ukrayinskoyi-armiyi-1258350.html.

28. Слюсар В. И. Военная связь стран НАТО: проблемы современных технологий. *Электроника: Наука, Технология, Бизнес*. 2008. № 4. С. 66-71.

29. Трахтенгерц Э. А. Сетецентрические методы компьютерного противодействия катастрофам и рискам. *Управление большими системами*. 2013. Вып. 41. С. 162–248. URL: http://elib.fa.ru/art2017/bv798.pdf/download/bv798.pdf.

30. Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Современные тенденции развития теории и практики управления в вооруженных силах США. Москва : ЛЕНАНД, 2009. 272 с.

31. Коли почнеться третя світова війна. URL: http://jak.bono.odessa.ua/articles/koli-pochnetsja-tretja-svitova-vijna-news-nsk.php.

32. Тактика сухопутних військ. URL: http://www.dogswar.ru/forum/viewtopic.php?f=30&t=958&hilit=канчуков&start=80.

33. Ефремов А. Ю., Максимов Д. Ю. Сетецентрическая система управления – что вкладывается в это понятие? *Технические и программные средства систем управления, контроля и измерения* : Труды III Всероссийской конференции с международным участием (УКИ-2012, Москва). Москва : ИПУ РАН, 2012. С. 158–161.

34. Кузьмин И. Future Combat System – революция или эволюция? URL: http://www.3dnews.ru/editorial/future_combat_system.

35. Информационные, специальные, воздушно-десантные и аэромобильные операции армий ведущих зарубежных государств: Информационно-аналитический сборник / А. Н. Сидорин и др. Москва : Воениздат, 2011. 344 с.

36. Савин Л. В. Сетецентричная и сетевая война. Введение в концепцию. Москва : Евразийское движение, 2011. 130 с.

37. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.

38. Глушков В. О. Основи новітньої теорії ведення сучасних війн. *Актуальні проблеми політики.* 2015. Вип. 56. С. 12–21. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/3031/ Глушков%20APP 56.pdf?sequence=1&isAllowed=y.

39. Пермяков О. Ю., Сбітнєв А. І. Інформаційні технології та сучасна збройна боротьба. Луганськ : Знання, 2008. 204 с.

40. Fadok, David S. John Boyd and John Warden. Airpower's Quest for Strategic Paralysis. *The Paths of Heaven: The Evolution of Airpower Theory*, Maxwell AFB, AL: Air University Press, 1997. 30 April 2008. URL: http://aupress.maxwell.af.mil/saas_Theses/Fadok/fadok.pdf.

41. Революция в военном деле и «армейские операции вне условий войны». URL: https://magazines.gorky.media/oz/2005/5/revolyucziya-v-voennom-dele-i-armejskie-operaczii-vne-uslovij-vojny-oboyudoostroe-oruzhie.html.

References

1. Nazarchuk, A. V. (2008). Setevoe obschestvo i ego filosofskoe osmyislenie [Network society and its philosophical understanding]. *Voprosyi filosofii – Problems of philosophy,* 7, pp. 61–75.

2. *Suchasni tekhnolohii avtomatyzatsii upravlinnia [Modern technologies of control automation]*. (n.d.). http://opk.com.ua/suchasni-tekhnolohii-avtomatyzatsii-upravlinnia/.

3. Burenok, V. M., Lyapunov, V. M., Mudrov, V. I., Moskovskyi, A. M. (ed.). (2005). Teoriia i praktika planirovaniia upravleniia razvitiem vooruzheniia *[Theory and practice of planning and management of weapondevelopment]*. Izd-vo «Vooruzhenie. Politika. Konversiya».

4. Makarenko, S. I. (2017). *Informatsionnoe protivoborstvo i radioelektronnaya borba v setetsentricheskih voynah nachala XXI veka [Information confrontation and electronic warfare in network-centric wars at the beginning of the XXI century].* Naukoemkie tehnologii.

5. Iarosh, S. P. (2010). Zavdannia doslidzhennia ta shliakhy stvorennia yedynoho informatsiinoho prostoru pry orhanizatsii upravlinnia viiskamy [Research tasks and ways to create a uniform information space at the organization of management of armies]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony – Modern information technologies in the sphere of security and defense*, 3(9), pp. 34–41.

6. Kingston-Makklori, E. Dzh. (1957). *Rukovodstvo voynoy. Analiz roli politicheskogo rukovodstva i vyisshego voennogo komandovaniya [War leadership. Analysis of the role of political leadership and the highest military command]*. (N. P. Pavlova i E. M. Mihaylova, Trans.). Izdatelstvo inostrannoy literaturyi.

7. Opyit primeneniya bespilotnoy aviatsii v vooruzhennom konflikte na Ukraine [Experience in the use of unmanned aircraft in the armed conflict in Ukraine]. https://general-skokov.livejournal.com/tag/setetsentricheskaya voyna.

8. Kovalev, V., Malinetskiy, G., Matvienko, Yu. (n.d.). Kontseptsiya «setetsentricheskoy» voynyi dlya armii Rossii: «mnozhitel silyi» ili mentalnaya lovushka? [Concept of "network-centric" war for the Russian army: "force multiplier" or a mental trap?]. http://www.inesnet.ru/wp-content/mag archive/2013 05/ES2013-05-Kovalev Malinetsky Matvienko.Pdf.

9. Parshin, S. A., Gorbachev, Yu. E., Kozhanov, Yu. A. (2009). *Sovremennyie tendentsii razvitiya teorii i praktiki upravleniya v vooruzhennyih silah SShA [Modern trends in the development of the theory and practice of management in the US armed forces]*. LENAND.

10. Slipchenko, V. I. (2004). *Voiny novogo pokoleniia: distantsionnye i beskontaktnye [New generation wars: remote and non-contact].* OLMA-PRESS obrazovanie.

11. Sidorin, A. N., Ryabchenko, I. A., … Gerasimov, V. P. (2011). *Informatsionnye, spetsialnye, vozdushno-desantnye i aeromobilnye operatsii armii veduschikh zarubezhnykh gosudarstv: Informatsionno-analiticheskii sbornik [Information, special, airborne and airmobile operations in the armies of the leading foreign states: Information and analytical collection]*. Voenizdat.

12. Trebin, M. P. (2005). *Voynyi XXI veka [Wars of the XXI century]*. AST.

13. Baryishev, A. P. (2011). *Sovremennaia strategiia SShA i NATO (v kontekste problem natsionalnoy bezopasnosti Rossii) [Modern strategy of the USA and NATO (in the context of Russian national security problems)]*. OGI.

14. Karyakin, V. V. (2011). *Voennaia politika i strategiia SShA v geopoliticheskoi dinamike sovremennogo mira [Military policy and strategy of the United States in the geopolitical dynamics of the modern world].* Granitsa.

15. Popov, I. M. (n.d.). «Setetsentricheskaya voyna»: gotova li k ney Rossiya? ["Network-centric war": is Russia ready for it?]. http://www.milresource.ru/NCW.html.

16. Alberts, D. S., Garstka, J. J., Stein, F. P. (2001). *Network Centric Warfare: Developing and Leveraging Information Superiority* (2nd edition (revised)). US Department of Defense, C4ISR Cooperative Research Program Publications Series. Retrieved 19.12.2019 from http://www.dodccrp.org/files/Alberts_NCW.pdf.

17. Makarenko, A. V. (n.d.). Vvedenie v setetsentricheskie informatsionno-upravliaiuschie sistemyi [Introduction to network-centric information and control systems]. In *Konstruktivnaia kibernetika. Issledovaniia. Razrabotki. Konsalting – Constructive cybernetics. Research. Developments. Consulting.* http://www.rdcn.ru/estimation/2010/03042010.shtml.

18. Sliusarenko, A. V. (n.d.). *Dosvid vedennia boiovykh dii u lokalnykh viinakh kintsia XX – pochatku XXI stolit, ta yoho vykorystannia u pidhotovtsi ZS Ukrainy [Experience of warfare in local wars of the late XX - early XXI centuries, and its use in the training of the Armed Forces of Ukraine].* http://ena.lp.edu.ua/bitstream/ntb/30909/1/30.pdf.

19. Permiakov, O. Iu., Sbitniev, A. I. (2008). *Informatsiini tekhnolohii ta suchasna zbroina borotba [Information technology and modern warfare].* Znannia.

20. Vasylenko, O. V. (2009). Osnovni svitovi tendentsii rozvytku ozbroiennia ta viiskovoi tekhniky dlia vedennia viin u maibutnomu [The main world trends in the development of weapons and military equipment for future wars]. *Nauka i oborona – Science and defense,* 4, pp. 18–22.

21. Kupriyanov, A. A. (2011). Setetsentricheskie voennyie deystviya i voprosyi inteoprabelnosti avtomatizirovannyih sistem [Network-centric military actions and issues of interoperability of automated systems]. *Avtomatizatsiia protsessov upravleniia – Automation of control processes,* 3(25), pp. 83-97. http://apu.npomars.com/images/pdf/25_14.pdf.

22. Zaitsev, D. V., Sharyi, V. I., Dobrvolskyi, V. B. (2015). Rozvytok zahalnoi taktyky za dosvidom lokalnykh viin i zbroinykh konfliktiv suchasnosti, yaki velys rehuliarnymy viiskamy proty irrehuliarnykh zbroinykh formuvan [Development of general tactics based on the experience of local wars and armed conflicts of today, which were conducted by regular troops against irregular armed groups]. *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka – Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv*, 49, pp. 117–124. http://nbuv.gov.ua/UJRN/Znpviknu_2015_49_20.

23. Polishchuk, L. I., Filimonov, S. M. (2009). Analiz deiakykh system upravlinnia zbroinymy sylamy krain NATO ta inshykh [Analysis of some management systems of the armed forces of NATO and other countries]. *Viiskovyi zbirnyk – Military collection*, 1, pp. 85–94.

24. Makarenko, S. I. (n.d.). *Podavlenie setetsentricheskikh sistem upravleniia radioelektronnymi informatsionno-tehnicheskimi vozdeistviiami [Suppression of network-centric control systems for electronic information and technical effects].* URL: https://cyberleninka.ru/article/n/podavlenie-setetsentricheskih-sistem-upravleniya-radioelektronnymi-informatsionno-tehnicheskimi-vozdeystviyami/viewer.

25. Arquilla, J., Ronfeldt D. (1996). *The Advent of Netwar*. Santa Monica, CA: RAND.

26. *Setetsentricheskaia voina. Daidzhest po materialam otkryityih izdanii i SMI [Network-centric warfare. Digest based on materials from open publications and media].* (2010). VAGSh VS RF.

27. *Merezhevo-tsentrychni viiskovi dii: maibutnie ukrainskoi armii [Network-centric military action: the future of the Ukrainian army]* (n.d.). https://tsn.ua/blogi/themes/o_voine/merezhevo-centrichna-viyna-maybutnye-ukrayinskoyi-armiyi-1258350.html.

28. Slyusar, V. I. (2008). Voennaya svyaz stran NATO: problemyi sovremennyih tehnologiy [Military communications of NATO countries: problems of modern technologies]. *Elektronika: Nauka, Tehnologiya, Biznes – Electronics: Science, Technology, Business,* 4, pp. 66–71.

29. Trahtengerts, E. A. (2013). Setetsentricheskie metodyi kompyuternogo protivodeystviya katastrofam i riskam [Network-centric methods of computer counteraction to disasters and risks]. *Upravlenie bolshimi sistemami – Large-Scale Systems Control,* 41, pp. 162–248. http://elib.fa.ru/art2017/bv798.pdf/download/bv798.pdf.

30. Parshin, S. A., Gorbachev, Yu. E., Kozhanov, Yu. A. (2009). *Sovremennye tendentsii razvitiia teorii i praktiki upravleniia v vooruzhennykh silah SShA [Modern trends in the development of theory and practice of management in the US armed forces]*. LENAND.

31. *Koly pochnetsia tretia svitova viina [When the Third World War begins].* (n.d.). http://jak.bono.odessa.ua/articles/koli-pochnetsja-tretja-svitova-vijna-news-nsk.php.

32. *Taktyka sukhoputnykh viisk [Tactics of Ground Forces]*. (n.d.). http://www.dogswar.ru/forum/viewtopic.php?f=30&t=958&hilit=kanchukov&start=80.

33. Efremov, A. Yu., Maksimov, D. Yu. (2012). Setetsentricheskaya sistema upravleniya – chto vkladyivaetsya v eto ponyatie? [Network-centric control system - what is included in this concept?]. *Tehnicheskie i programmnyie sredstva sistem upravleniya, kontrolya i izmereniya: Trudyi III Vserossiyskoy konferentsii s mezhdunarodnyim uchastiem – Hardware and software for control, monitoring and measurement systems: Proceedings of the 3rd All-Russian conference with international participation* (UKI-2012, Moscow) (pp. 158–161). IPU RAN.

34. Kuzmin, I. (n.d.). Future Combat System – revolyutsiia ili evoliutsiia? [Future Combat System – revolution or evolution?]. http://www.3dnews.ru/editorial/future_combat_system.

35. Sidorin, A. N., Ryabchenko, I. A., … Gerasimov, V. P. (2011). *Informatsionnye, spetsialnye, vozdushno-desantnye i aeromobilnye operatsii armii veduschikh zarubezhnykh gosudarstv: Informatsionno-analiticheskiy sbornik [Information, special, airborne and airmobile operations of the armies of leading foreign countries: Information and analytical collection].* Voenizdat.

36. Savin, L. V. (2011). *Setetsentrichnaia i setevaia voina. Vvedenie v kontseptsiiu [Network-centric and network warfare. Introduction to the concept].* Evraziyskoe dvizhenie.

37. Sashchuk, H. (n.d.). *Informatsiina bezpeka v systemi zabezpechennia natsionalnoi bezpeky [Information security in the system of national security].* http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.

38. Hlushkov, V. O. (2015). Osnovy novitnoi teorii vedennia suchasnykh viin [Fundamentals of the latest theory of modern wars]. *Aktualni problemy polityky – Actual Problems of Politics,* 56, pp. 12-21. http://dspace.onua.edu.ua/bitstream/handle/11300/3031/Hlushkov%20APP_56.pdf?sequence=1&isAllowed=y.

39. Permiakov, O. Iu., Sbitniev, A. I. (2008). *Informatsiini tekhnolohii ta suchasna zbroina borotba [Information technology and modern armed struggle].* Znannia.

40. Fadok, David S. John Boyd and John Warden (1997). Airpowers Quest for Strategic Paralysis. *The Paths of Heaven: The Evolution of Airpower Theory, Maxwell AFB, AL*: Air University Press, 30 April 2008. http://aupress.maxwell.af.mil/saas_Theses/Fadok/fadok. pdf.

Revoliutsiia v vennom dele i «armeiskie operatsii vne uslovii voiny» [Revolution in military affairs and “army operations outside the conditions of war”]. (n.d.). https://magazines.gorky.media/oz/2005/5/revolyucziya-v-voennom-dele-i-armejskie-operaczii-vne-uslovij-vojny-oboyudoostroe-oruzhie.html.*UDC 316.259+355.01*

UDC 316.259+355.01

Vitalii Zatserkovnyi, Pavlo Savkov, Igor Pampukha, Iryna Syniavska

ASSESSMENT OF THE ADVANTAGES OF NETWORK-CENTRISM AND NETWORK-CENTRIC TECHNOLOGIES FOR DEVELOPMENT OF THE ARMED FORCES OF UKRAINE

Urgency of the research. *Given the changes of the nature of modern wars and ways to achieve informational advantage over the enemy, the study of network-centric technologies is extremely relevant. Increasing the maneuverability of units, their ability to perform combat missions on the basis of continuous information support, makes it possible to gain a significant advantage over the enemy, to prevent and neutralize real and potential threats to national security.*

Target setting. *The current level of automation, informatization and control system of the Armed Forces of Ukraine on the set of values of the characteristics of its main components does not meet modern requirements.*

Actual scientific researches and issues analysis. *The problems of external information influences and information aspects of ensuring the national security of the state, the conceptual problems of war and peace and the problem of network-centric wars are considered.*

Uninvestigated parts of general matters defining. *The main problem in applying the principles of network-centrism in the organization of modern combat is insufficiently effective and unadapted to modern requirements information systems.*

The research objective. *The priority is to form an effective information system based on network-centric technologies, which will reduce the time for decision-making, and predict possible scenarios and prevent possible consequences.*

The statement of basic materials. *Advances in information and communication technologies (ICTs) have given rise to new models of high-precision weapons, modern intelligence, and automatic and automated control systems (ACS) for troops and weapons. Computer technology made it possible to control weapons at a distance of several thousand kilometers, to form high-precision point strikes, to correct the actions of military units, to carry out actions of military formations in several directions to destroy enemy objects or capture its territory, to achieve results in a short period time, etc. The need to make the most of all available reconnaissance and combat platforms led to a shift from a platform-centric model of troop and arms control, with the main emphasis on the number of weapons and military equipment, to a network-centric one.*

Conclusions. *The role of network-centric wars and their influence on the development of the Armed Forces of the economically advanced countries is determined. The use of network-centric approaches has led to the emergence of many new non-traditional forms and methods of armed struggle, such as "special operation", "three-dimensional air-ground form of attack on the enemy", "long-range fire", etc., during which ships and submarines, aircraft, space aircraft, unmanned aerial vehicles (UAVs), tanks, field radios and laptops, etc. shared information through common interfaces, standards and protocols. The components of high efficiency of network-centric wars are determined.*

Keywords: *information advantage; single information space; network centrism; network-centric control system; network-centric war.*

Fig.: 8. References: 42.

Зацерковний Віталій Іванович – доктор технічних наук, професор, завідуючий кафедри геоінформатики, Навчально-науковий інститут «Інститут геології» Київського національного університету імені Тараса Шевченка (вул. Васильківська, 90, м. Київ, 03022, Україна).
Zatserkovnyi Vitalii – Doctor of Technical Sciences, Professor, Chair of the Department of Geoinformatics, Institute of Geology of Taras Shevchenko National University of Kyiv (90 Vasylkivska Str., 03022 Kyiv, Ukraine).
E-mail: vitalii.zatserkovnyi@gmail.com
SCOPUS Author ID: 57200165109
ORCID: https://orcid.org/0000-0003-2346-9496
ResearcheriD: AAE-6191-2019

Савков Павло Анатолійович – кандидат технічних наук, доцент, начальник кафедр геоінформаційних систем та технологій, Військовий інститут Київського національного університету імені Траса Шевченка (вул. Ломоносова,81, м. Київ, 03189, Україна).
Savkov Pavlo – PhD in Technical Sciences, Associate Professor, Chair of the Department of Geoinformation System and Tachnologies, Military Institute of Taras Shevchenko National University of Kyiv (81 Lomonosova Str., 03189 Kyiv, Ukraine).
E-mail: savkovpa@gmail.com
SCOPUS Author ID: 57210749931
ORCID: https:// orcid.org/0000-00020127-0610

Пампуха Ігор Володимирович – кандидат технічних наук, доцент, начальник науково-дослідного центру, Військовий інститут Київського національного університету імені Траса Шевченка (вул. Ломоносова,81, м.Київ, 03189, Україна).
Pampukha Igor – PhD in Technical Sciences, Associate Professor, Chair of the Reaseacher Centre, Military Institute of Taras Shevchenko National University of Kyiv (81 Lomonosova Str., 03189 Kyiv, Ukraine).
E-mail: pamp@ukr.net
SCOPUS Author ID: 57195922711
ORCID: http://orcid.org/0000-0002-4807-3984

Синявська Ірина Костянтинівна – ад'юнкт науково-організаційного відділення, Військовий інститут Київського національного університету імені Траса Шевченка (вул. Ломоносова, 81, м. Київ, 03189, Україна).
Syniavska Iryna – PhD Student, Military Institute of Taras Shevchenko National University of Kyiv (81 Lomonosova Str., 03189 Kyiv, Ukraine).
E-mail: irinashatkovska@gmail.com
SCOPUS Author ID: 57218568662
ORCID: https://orcid.org/0000-0002-2645-994X

Зацерковний В., Савков П., Пампуха І., Синявська І. Оцінка переваг мережецентризму та мережецентричних технологій для розбудови Збройних Сил України. *Технічні науки та технології.* 2020. № 3 (21). С. 163-184.