

УДК 355.422:004.7

[https://doi.org/ 10.31652/2786-6068-2026-7-113-126](https://doi.org/10.31652/2786-6068-2026-7-113-126)

Віктор Петров

Національного університету оборони України,
доктор філософії, старший викладач кафедри військової підготовки, полковник,
e-mail: vitalygavlitsky@gmail.com
<https://orcid.org/0000-0001-7966-2020>

Оксана Зелінська

Вінницький державний педагогічний університет імені Михайла Коцюбинського,
кандидат технічних наук, доцент кафедри публічного управління та
менеджменту
e-mail: zeloksanavlad@gmail.com
<https://orcid.org/0000-0002-9069-1428>

Віталій Гавліцький

Національного університету оборони України,
слухач кафедри комунікаційних технологій та кіберзахисту, майор
e-mail: vitalygavlitsky@gmail.com
<https://orcid.org/0009-0002-9749-7465>

**КОНЦЕПТУАЛЬНІ ЗАСАДИ МЕРЕЖЕЦЕНТРИЧНОЇ
ТРАНСФОРМАЦІЇ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКАМИ В УМОВАХ
ЦИФРОВІЗАЦІЇ ПОЛЯ БОЮ**

Анотація. У статті досліджено трансформацію систем управління військами від традиційної ієрархічної до мережецентричної моделі в умовах цифровізації, динамічної зміни обстановки та зростання вимог до швидкості прийняття рішень. Обґрунтовано, що мережецентричний підхід не передбачає повної відмови від військової ієрархії, а формує її поєднання з горизонтальними зв'язками, цифровою інтеграцією та децентралізацією повноважень. Визначено недоліки ієрархічної системи: часові затримки передачі інформації, перевантаження органів управління, обмежена гнучкість та залежність від централізованих рішень. Розкрито сутність мережецентричної системи як моделі, що ґрунтується на інтеграції інформаційних ресурсів у єдиний інформаційний простір та забезпечує взаємодію елементів системи в режимі реального часу. Проаналізовано ключові характеристики її ефективності: швидкість управлінського циклу, повноту й достовірність інформації, рівень інтеграції, стійкість до зовнішніх впливів та адаптивність. Розглянуто цикл OODA, C4ISR, ситуаційну обізнаність та самосинхронізацію підрозділів. На основі досвіду російсько-української війни розглянуто практичне застосування цифрових систем управління, безпілотних комплексів, цифрових каналів зв'язку та систем типу DELTA, які сприяють скороченню часу реагування та узгодженості дій. Визначено основні ризики мережецентричного управління,
© Петров В., Зелінська О., Гавліцький В.

зокрема залежність від каналів зв'язку, кіберзагрози, інформаційне перевантаження та вразливість до радіоелектронної боротьби. Запропоновано основні напрями трансформації: технологічний, організаційний, доктринальний, кадровий та безпековий. Обґрунтовано доцільність використання гібридної моделі на перехідному етапі, яка поєднує єдність управління з гнучкістю дій нижчих рівнів. Подальші дослідження доцільно спрямувати на оцінювання готовності військових частин до мережецентричного середовища, стійкості цифрових систем та інтеграції штучного інтелекту. Підкреслено, що технології мають підтримувати командира, не замінювати його відповідальність. саму.

Ключові слова: мережецентричне управління, система управління військами, цифрова трансформація, ситуаційна обізнаність, місійне командування, децентралізація управління, бойова стійкість.

Viktor Petrov, Oksana Zelinska, Vitalii Havlitskyi

CONCEPTUAL FOUNDATIONS OF THE NETWORK-CENTRIC TRANSFORMATION OF MILITARY COMMAND AND CONTROL SYSTEMS UNDER THE CONDITIONS OF BATTLEFIELD DIGITALIZATION

Abstract. The article explores the transformation of military command and control systems from a traditional hierarchical model to a network-centric one amid digitalization, rapidly changing operational environments, and increasing demands for decision-making speed. It is substantiated that the network-centric approach does not imply a complete rejection of military hierarchy, but rather forms its combination with horizontal links, digital integration, and decentralization of authority. The drawbacks of the hierarchical system are identified: information transmission delays, C2 body overload, limited flexibility, and reliance on centralized decision-making. The essence of the network-centric system is revealed as a model based on integrating information resources into a unified information space, ensuring real-time interaction among system components. Key performance characteristics are analyzed: management cycle speed, information completeness and accuracy, level of integration, resilience to external influences, and adaptability. The study considers the OODA loop, C4ISR, situational awareness, and self-synchronization of units. Based on the experience of the Russo-Ukrainian War, the practical application of digital command and control systems, unmanned aerial systems, digital communication channels, and systems like DELTA is examined, which contribute to reduced response times and coordinated action. Major risks of network-centric warfare are identified, including reliance on communication channels, cyber threats, information overload, and vulnerability to electronic warfare. Primary transformation vectors are proposed: technological, organizational, doctrinal, personnel, and security. The expediency of employing a hybrid model during the transition phase, combining unity of command with lower-level operational flexibility, is justified. Future research should focus on assessing unit readiness for the network-centric environment, the resilience of digital systems, and the integration of artificial intelligence. It is emphasized that technology must support the

commander without replacing their responsibility.

Keywords: network-centric management, troop management system, digital transformation, situational awareness, combat command, decentralization of management, combat sustainability.

Постановка проблеми. Мережецентричні моделі управління стрімко набрали актуальності у сучасному мультидоменному середовищі, що формуються під впливом цифрової трансформації сучасного поля бою. В цей же час ієрархічні системи управління військами з часом та динамічними змінами на полі бою розпочали моральне старіння.

Все частіше на полі бою використовують нові технологічні рішення, які дозволяють швидше, надійніше, безпечніше та економно досягати очікуваних результатів.

Під час виконання бойових завдань здебільшого користуються різними сенсорами, безпілотними системами, цифровими платформами, засобами радіоелектронної боротьби, системами супутникового зв'язку та автоматизованими засобами обробки інформації.

Теоретичні дані з керівних документів та практичне підтвердження відповідно до бойового досвіду за 2022-2025 роки дають чітке розуміння, що лише за умов швидшого виявлення противника, оперативного прийняття рішень, детальнішої оцінки обстановки та вмілого, якісного, централізованого та безперервного управління діями підрозділів можна забезпечити перевагу над противником у різнодоменній війні сьогодення.

Класична ієрархічна модель управління, побудована на послідовному проходженні інформації через різні ланки командування з затримкою часу на сам процес виконання та зі збереженням значущості прийнятого рішення командира без можливості діяти оперативно на місці. Така модель має ряд недоліків, що можуть значно вплинути на ефективність виконання, серед яких є такі як затримка управлінського циклу, перевантаження штабів, уразливість командних пунктів, обмежена ситуаційна обізнаність тактичної ланки та складність швидкої адаптації до змін оперативної обстановки.

Мережецентрична модель стала актуальним сучасним та революційним рішенням для класичної моделі управління завдяки горизонтальному обміну даними, цифровій інтеграції сенсорів, засобів ураження, штабів і командирів різних рівнів у єдине інформаційно-бойове середовище.

З розвитком інформаційних технологій та цифрових систем обробки даних з'явилися передумови для вирішення зазначеної проблеми шляхом переходу до нової моделі управління - мережецентричної. Основною її особливістю є інтеграція всіх елементів бойової системи в єдиний інформаційний простір, що забезпечує оперативний обмін даними та підвищує швидкість прийняття рішень.

Впровадження мережецентричних систем управління супроводжується новими викликами, пов'язаними з їх залежністю від інформаційних технологій та вразливістю до кібернетичних загроз. Дослідження показують, що порушення функціонування інформаційних систем може призвести до дезорганізації управління військами та зниження ефективності бойових дій. Це обумовлює

необхідність врахування факторів кібербезпеки та стійкості систем управління при їх побудові.

Таким чином, наукова проблема дослідження полягає у необхідності обґрунтування концептуальних засад переходу від ієрархічних до мережецентричних систем управління військами з урахуванням сучасних умов ведення бойових дій, розвитку інформаційних технологій та загроз кіберпростору.

Сучасний бій набуває рис високодинамічного, інформаційно-насиченого та багатодоменого середовища, де швидкість прийняття рішень, точність оцінки обстановки та стійкість комунікацій стають вирішальними чинниками успіху. Ієрархічні системи управління військами, що домінували в ХХ столітті, виявляються недостатньо гнучкими для реагування на загрози в реальному масштабі часу. Водночас цифровізація поля бою – розгортання захищених мереж, застосування безпілотних систем, супутникової розвідки, штучного інтелекту та edge-обчислень – створює технологічне підґрунтя для переходу до мережецентричного управління (NetCentric Warfare). Проте більшість наявних наукових праць зосереджена або на технічних аспектах (C4ISR, захист каналів), або на загальних концепціях, не враховуючи комплексності трансформації: поєднання технологічних, організаційних, доктринальних, кадрових та безпекових викликів. Особливо гостро ця проблема стоїть для Збройних Сил України, які здобувають унікальний бойовий досвід в умовах інтенсивної радіоелектронної боротьби, кібератак та обмежених ресурсів.

Отже, невирішеною частиною загальної проблеми є відсутність цілісних концептуальних засад поетапної трансформації систем управління військами від ієрархічно-центральної моделі до мережецентричної, яка б одночасно враховувала: реальний стан технічної інфраструктури та її вразливість до засобів РЕБ; необхідність збереження стійкості управління в умовах деградації зв'язку; культурні та доктринальні бар'єри (децентралізація повноважень, довіра до автоматизованих систем).

Аналіз останніх досліджень. Проблематика розвитку систем управління військами в умовах інформаційного протистояння та цифрової трансформації поля бою посідає важливе місце як у вітчизняних, так і в зарубіжних наукових дослідженнях. Особлива увага приділяється переходу від традиційних ієрархічних моделей управління до мережецентричних систем, які забезпечують інтеграцію інформаційних ресурсів, підвищення швидкості обміну даними та оперативності прийняття рішень.

Теоретичні основи мережецентричної війни були сформовані у працях David S. Alberts, John J. Garstka та F.P.Stein, які обґрунтували твердження про те, що інформаційна перевага здатна трансформуватися у реальну бойову перевагу лише за умов об'єднання сил і засобів у спільну інформаційну мережу [1]. У цих дослідженнях мережецентрична війна розглядається не як окремий технологічний елемент, а як нова концепція організації бойових дій, у якій вирішального значення набувають швидкість обміну інформацією, рівень ситуаційної обізнаності та здатність сил до самосинхронізації.

Подальший розвиток концепції мережецентричного управління знайшов

відображення у праці «Power to the Edge», де Д. Альбертс та Р. Гейс акцентували увагу на необхідності передавання частини управлінських повноважень безпосередньо виконавцям, які перебувають у районі виконання бойових завдань та володіють більш актуальною інформацією про обстановку [2]. Автори підкреслюють, що надмірна централізація управління в умовах високодинамічного бою призводить до втрати темпу операції та зниження ефективності реагування.

Значний вплив на сучасні підходи до військового управління справила концепція циклу OODA, запропонована John Boyd [3]. Її сутність полягає у здатності сторони швидше проходити етапи спостереження, орієнтування, прийняття рішення та дії, нав'язуючи противнику власний темп ведення бойових дій. У сучасному цифровому бойовому середовищі ефективність проходження циклу OODA безпосередньо залежить від рівня розвитку систем зв'язку, цифрових платформ, автоматизованої обробки даних та ситуаційної обізнаності.

У доктринальних документах НАТО та армії США значна увага приділяється питанням оперативного планування, організації управління, забезпечення взаємодії та децентралізованого виконання завдань [7,] [12]. Особливе місце займає концепція mission command, відповідно до якої підлеглі командири повинні не лише отримувати наказ, але й розуміти загальний замисел старшого начальника, мету операції та межі власної ініціативи [8]. Такий підхід дозволяє забезпечити гнучкість управління та адаптивність підрозділів без втрати єдності управління.

Окремий напрям досліджень присвячений розвитку систем C4ISR, ситуаційної обізнаності та багатосенсорної інтеграції даних [3], [5], [9]. У працях зазначається, що сучасні системи управління повинні забезпечувати інтеграцію розвідки, зв'язку, автоматизованої обробки інформації, спостереження, рекогносцировки та засобів вогневого ураження в єдине інформаційно-бойове середовище. Саме така інтеграція дозволяє суттєво скоротити часовий цикл «виявлення – рішення – ураження» та підвищити ефективність застосування сил і засобів.

У вітчизняних наукових дослідженнях значна увага приділяється ролі інформаційних технологій у системі військового управління. Зокрема, у працях Ю. Г. Даника обґрунтовано, що мережецентрична концепція ведення бойових дій базується на досягненні інформаційної переваги шляхом інтеграції розвідувальних, інформаційних та ударних компонентів у єдину систему [16], [17]. Автор підкреслює, що саме інтеграція інформаційних ресурсів забезпечує підвищення рівня ситуаційної обізнаності та ефективності управлінських рішень.

Дослідження сучасного бойового досвіду, зокрема російсько-української війни, представлені у працях українських та зарубіжних аналітичних центрів, таких як Royal United Services Institute, Institute for the Study of War та RAND Corporation [6], [10], [13], [15]. У цих дослідженнях наголошується, що використання безпілотних систем, цифрових платформ управління, сучасних засобів зв'язку та автоматизованих систем обробки даних дозволяє значно скоротити цикл реагування та підвищити результативність бойового

застосування військ. Особлива увага приділяється інтеграції розвідувальних і ударних компонентів у єдину систему управління.

Водночас значна кількість досліджень присвячена питанням кібербезпеки та забезпечення стійкості систем управління в умовах інформаційного впливу та радіоелектронної боротьби [11], [14]. Дослідники зазначають, що мережецентричні системи, попри свої переваги, залишаються вразливими до кібератак, порушення каналів зв'язку та впливу засобів РЕБ, що може призвести до дезорганізації управління військами. Це обумовлює необхідність розроблення комплексних підходів до захисту інформаційних систем та забезпечення їх функціональної стійкості.

Аналіз сучасних наукових публікацій свідчить, що, незважаючи на значний обсяг наукових досліджень, низка питань залишається недостатньо опрацьованою. Зокрема, потребують подальшого дослідження питання формалізації ефективності систем управління, кількісної оцінки впливу цифровізації на швидкість прийняття рішень, а також інтеграції теоретичних моделей мережецентричного управління з практичним досвідом сучасних бойових дій. Таким чином, проведений аналіз підтверджує актуальність проблематики та необхідність подальшого розвитку теоретичних і прикладних засад переходу від традиційних ієрархічних до мережецентричних систем управління військами в умовах цифрової трансформації сучасного поля бою.

Метою статті є обґрунтування теоретичних і практичних засад мережецентричної трансформації систем управління військами в умовах цифровізації поля бою.

Виклад основного матеріалу. Провівши детальне дослідження слід зрозуміти, що перехід від ієрархічних до мережецентричних систем управління військами не потрібно сприймати як заміну однієї моделі управління на іншу. Вони поєдналися в симбіоз і стали більш якіснішою та швидшою моделю управління, що значно покращила діяльність на всіх рівнях системи.

Відбулася трансформація логіки прийняття рішень, де керівники відповідних структурних підрозділів зберігають своє право своєчасно приймати рішення та керувати підрозділами у режимі реального часу.

Основними недоліками ієрархічної системи є:

- значні часові затримки при передачі інформації;
- перевантаження органів управління;
- обмежена гнучкість та адаптивність;
- залежність від централізованих рішень.

У формалізованому вигляді час управління в ієрархічній системі може бути представлений як сума часових витрат на кожному рівні:

$T_{\text{hier}} = \sum_{i=1}^n (T_{\text{receive},i} + T_{\text{process},i} + T_{\text{transfer},i})$, де:

T_{hier} — загальний час управління в ієрархічній системі;

n — кількість рівнів управління;

$T_{\text{receive},i}$ — час отримання інформації на i -му рівні;

$T_{\text{process},i}$ — час обробки інформації на i -му рівні;

$T_{\text{transfer},i}$ — час передачі інформації з i -го на $(i+1)$ -й рівень (або між рівнями).

Збільшення кількості рівнів призводить до пропорційного зростання часу прийняття рішень, що є критичним недоліком у сучасних умовах.

Засоби комунікації також відіграють значну роль у розвитку мережецентричних систем управління через свій вагомий вплив зі зміною у часі. Основними засобами комунікації були голосовий зв'язок, письмові накази, доповіді та штабні документи. Однак сучасне поле бою є розосередженим, насиченим цифровими засобами спостереження, прозорим для розвідки та водночас дуже нестабільним через постійний вплив РЕБ, кібератак і вогневого ураження.

Основним недоліком ієрархічної моделі в таких умовах є затримка управлінського циклу. При використанні старих моделей управління інформація проходила декілька рівнів, на який кожен виконавець обробляв інформацію та приймав рішення, на що витрачався деякий час, і після декількох етапів управлінського циклу затримка часу могла збільшуватися експоненціально, що в подальшому, з великою ймовірністю, могло б призвести до кризової ситуації великого масштабу. Але і перенавантаженість штабів може призвести до такого ж ефекту через великі потоки даних, які потрібно аналізувати та велику кількість засобів, що генерують дану інформацію.

Мережецентрична модель пропонує інший підхід. Її головна ідея полягає в тому, що інформація має бути доступною не лише вищому командирові, а й тим учасникам бойових дій, які можуть безпосередньо її використати. Сенсор, який виявив ціль, вогневий засіб, який може її уразити і командир, який відповідає за ділянку бойових дій, повинні бути пов'язані не тільки через довгий цикл штабних доповідей, а й через єдине цифрове середовище.

Мережецентрична система управління є новою моделлю організації управлінських процесів, яка базується на інтеграції інформаційних ресурсів у єдиний інформаційний простір та забезпечує взаємодію всіх елементів системи в режимі реального часу.

До основних характеристик входять децентралізація управління, наявність горизонтальних зв'язків, висока швидкість обміну інформацією, можливість автономного прийняття рішень на нижчих рівнях управління.

Оцінка ефективності систем управління здійснюється за такими основними критеріями: швидкість прийняття управлінських рішень; повнота та достовірність інформації; рівень інтеграції інформаційних ресурсів; стійкість системи до зовнішніх впливів; здатність до адаптації в умовах зміни обстановки.

Ключовою ідеєю мережецентричного підходу є досягнення інформаційної переваги шляхом об'єднання розвідувальних, інформаційних та ударних компонентів у єдину мережу. Це дозволяє підвищити швидкість прийняття рішень та забезпечити узгодженість дій підрозділів.

Мережецентрична система (МЦС) базується на протилежних принципах: кожний абонент (сенсор, вогневий засіб, командир тактичної групи) має прямий логічний зв'язок з будь-яким іншим за умови дотримання прав доступу.

Ефективність мережецентричної системи можна описати як функцію інформації, швидкості та інтеграції:

$$\Sigma_{net} = I \times M / T_{cycle}$$

T_{cycle} - час повного циклу управління (обернено пропорційний швидкості S),

I та M - нормовані величини від 0 до 1.

Одним із ключових елементів теоретичної моделі є цикл прийняття рішень, відомий як OODA (Observe–Orient–Decide–Act).

У межах цього циклу ефективність управління визначається швидкістю проходження всіх його етапів, де скоротити час тривалості циклу за допомогою автоматизації збору інформації, інтеграції даних з різних джерел, децентралізації прийняття рішень. Скорочення часу проходження циклу OODA забезпечує отримання переваги над противником, який діє у більш повільному інформаційному контурі.

Збільшення кількості взаємодій між елементами системи призводить до зростання її загальної ефективності за рахунок покращення обміну інформацією та координації дій. Ключову роль у цьому процесі відіграє C4ISR. Саме поєднання командування, управління, зв'язку, комп'ютерних систем, розвідки, спостереження та рекогносцировки формує основу сучасного інформаційно-бойового контуру.

Ситуаційна обізнаність означає не просто наявність великої кількості даних, а здатність правильно розуміти їх значення зі збереженням структури логіки та суті для прийняття рішення командиром начальником.

Досвід російсько-української війни підтверджує, що перевага у швидкості управління може компенсувати нестачу окремих матеріальних ресурсів. Українські підрозділи в багатьох випадках демонстрували високу адаптивність, завдяки використанню безпілотних систем, цифрових карт, захищених каналів зв'язку, гнучких схем взаємодії та ініціативи командирів нижчої ланки управління. Саме поєднання технології та ініціативи створює практичний зміст мережецентричного підходу. Перехід від ієрархічних до мережецентричних систем управління військами є складним багаторівневим процесом, що охоплює технологічні, організаційні та функціональні зміни. На відміну від модернізації окремих елементів системи, дана трансформація передбачає формування нової моделі управління, заснованої на інтеграції інформаційних ресурсів та децентралізації прийняття рішень. Основною передумовою переходу є розвиток інформаційних технологій, які забезпечують можливість створення єдиного інформаційного простору та організації взаємодії між різними елементами системи управління. У таких умовах змінюється роль органів управління, які поступово переходять від функцій безпосереднього керування до координації та забезпечення взаємодії. Цифровізація є ключовим чинником трансформації систем управління. Результатом цифровізації є суттєве скорочення часу обробки інформації та підвищення її достовірності, що безпосередньо впливає на ефективність управління [5], [7].

Одним із ключових механізмів переходу є інтеграція інформаційних систем у єдиний інформаційний простір. У традиційній системі управління інформаційні потоки є фрагментованими та ізольованими, що ускладнює процес прийняття рішень. Мережецентричний підхід передбачає об'єднання різних джерел інформації, зокрема: розвідувальних систем; безпілотних комплексів;

засобів зв'язку; інформаційно-аналітичних платформ. Інтеграція цих елементів дозволяє сформувати єдину картину обстановки та забезпечити оперативний доступ до інформації на всіх рівнях управління, а горизонтальні зв'язки дозволяють формувати гнучкі мережеві структури, які адаптуються до змін обстановки та забезпечують більш ефективну координацію дій. Децентралізація є необхідною умовою функціонування мережецентричної системи, оскільки дозволяє скоротити час прийняття рішень та підвищити гнучкість управління. У результаті інтеграції інформаційних систем та розвитку горизонтальних зв'язків формується здатність підрозділів до самосинхронізації.

Сутність цього явища полягає у тому, що підрозділи, маючи доступ до єдиної інформаційної бази, є одним із ключових факторів підвищення ефективності мережецентричних систем управління.

Незважаючи на значні переваги, процес переходу до мережецентричних систем управління супроводжується рядом обмежень:

- залежність від інформаційних технологій;
- вразливість до кіберзагроз;
- необхідність значних ресурсів;
- складність інтеграції різних систем.

Ці фактори необхідно враховувати при плануванні та реалізації трансформації систем управління тому що вони висвітлюють проблематику створення нових ризиків.

Перший ризик - залежність від каналів зв'язку. Якщо цифрова система втрачає зв'язок, а особовий склад не здатний діяти автономно, то перевага швидко перетворюється на слабкість.

Другий ризик - кіберзагрози. Будь-яка цифрова платформа може стати об'єктом атаки, спроби підміни даних або дезорганізації управління.

Третій ризик - інформаційне перевантаження. Забагато сигналів без належної фільтрації, може призвести до втрати здатності швидко ухвалювати рішення.

Саме тому перехід до мережецентричного управління має бути не хаотичним, а концептуально впорядкованим.

Визначимо декілька взаємопов'язаних напрямів такої трансформації:

Перший напрям - технологічний. Він передбачає створення захищених цифрових платформ, розвиток тактичних мереж зв'язку, впровадження автоматизованих систем управління, інтеграцію БПЛА, сенсорів, артилерійських засобів, логістики та штабних систем. Особливе значення має сумісність цих рішень між собою та з підходами НАТО.

Другий напрям - організаційний. Він полягає в перегляді ролі штабів і командирів різних рівнів. Штаб у мережецентричному середовищі має бути не лише місцем збирання доповідей, а центром аналізу, координації та підтримки рішень. Командири нижчих рівнів повинні отримати більше простору для ініціативи в межах загального задуму.

Третій напрям - доктринальний. Він вимагає оновлення статутів, настанов і бойових документів з урахуванням принципів mission command, цифрової взаємодії, горизонтального обміну даними та багатодоменого управління.

Доктрина має не лише дозволяти децентралізоване виконання, а й навчати командирів правильно користуватися цією свободою.

Четвертий напрям - кадровий. Він є одним із найскладніших. Техніку можна закупити швидше, ніж змінити мислення. Командир мережецентричної епохи має бути не тільки носієм військової дисципліни, а й лідером, здатним працювати з даними, довіряти підлеглим, діяти в умовах невизначеності та ухвалювати рішення без очікування детального наказу на кожен крок.

П'ятий напрям - безпековий. Він охоплює кіберзахист, криптографічний захист інформації, резервування каналів зв'язку, протидію РЕБ, захист даних і здатність системи функціонувати навіть у разі втрати окремих вузлів. Мережецентрична система повинна бути не лише швидкою, а й живучою.

У цьому контексті доцільно говорити про гібридну модель управління на перехідному етапі. Така модель не руйнує військову ієрархію, але поступово доповнює її мережевими елементами. Старший командир визначає мету, задум, ресурси, обмеження та критерії успіху. Командири нижчих рівнів отримують можливість самостійно обирати способи виконання завдань залежно від конкретної обстановки. Саме так досягається баланс між єдністю управління та гнучкістю дій.

Особливої уваги потребує питання штучного інтелекту та edge computing. Штучний інтелект може використовуватися для попередньої обробки великих масивів розвідувальних даних, виявлення закономірностей, пріоритезації цілей і підтримки прийняття рішень. Edge computing дозволяє обробляти інформацію ближче до місця її отримання, зменшуючи залежність від центральних серверів і підвищуючи стійкість системи. Водночас ці технології не повинні підміняти командира. Їхнє завдання - допомагати людині швидше й точніше оцінювати ситуацію, а не забирати в неї відповідальність за рішення.

Російсько-українська війна стала одним із найбільш показових прикладів практичного впровадження елементів мережецентричного управління, де інтеграція розвідувальних, інформаційних та ударних компонентів забезпечує підвищення ефективності бойових дій. Одним із ключових інструментів реалізації такого підходу у Збройних Силах України є впровадження цифрових систем управління, що забезпечують формування єдиної картини обстановки. Зокрема, використання систем типу DELTA дозволяє інтегрувати дані з різних джерел - розвідки, безпілотних комплексів та підрозділів на місцях - у єдине інформаційне середовище. Це забезпечує командирам можливість оперативно оцінювати ситуацію та приймати рішення в умовах обмеженого часу. Важливу роль у цій системі відіграють безпілотні літальні апарати, які забезпечують безперервний моніторинг обстановки та оперативне виявлення цілей. Наприклад, у ході бойових дій на сході України широке застосування отримали БПЛА для коригування артилерійського вогню, що дозволило значно підвищити точність ураження та зменшити витрати боєприпасів. Іншим прикладом є використання FPV-дронів, які інтегруються у систему управління, як засоби безпосереднього ураження, скорочуючи час реагування до мінімальних значень.

З досвіду на полі бою, скорочення кожного з цих етапів досягається за рахунок інтеграції БПЛА, цифрових каналів передачі даних та делегування

повноважень на нижчій рівні. Наприклад, у ряді операцій артилерійські підрозділи отримують координати цілей безпосередньо від операторів БПЛА, минаючи проміжні ланки управління, що дозволяє суттєво скоротити час відкриття вогню. Суттєвим фактором забезпечення стійкості управління є використання сучасних засобів зв'язку, зокрема супутникових систем. Практика показує, що їх застосування дозволяє підтримувати управління навіть в умовах активного впливу засобів радіоелектронної боротьби, що особливо важливо при веденні бойових дій на великих територіях та в умовах порушення наземної інфраструктури.

У результаті впровадження мережецентричних підходів у Збройних Силах України спостерігається формування ефекту самосинхронізації підрозділів. Наприклад, у бойових епізодах, де задіяні розвідувальні БПЛА, артилерійські підрозділи та штурмові групи, їх дії часто координуються не через жорстку вертикаль управління, а через спільний інформаційний простір, що дозволяє оперативно адаптуватися до змін обстановки. Разом з тим, практичний досвід свідчить, що ефективність мережецентричних систем значною мірою залежить від їх стійкості до зовнішніх впливів. Зокрема, застосування противником засобів радіоелектронної боротьби та кібернетичних атак може призводити до порушення інформаційних зв'язків, що негативно впливає на процес управління. Противник активно застосовує засоби радіоелектронної боротьби, для подавлення каналів зв'язку, порушення роботи навігаційних систем та впливу на безпілотні комплекси. Наприклад, у ряді випадків фіксується зниження ефективності застосування БПЛА, внаслідок глушіння сигналів управління або спотворення координат, що безпосередньо впливає на процес прийняття рішень. Сучасний підхід до забезпечення стійкості систем управління передбачає поєднання технологічних і організаційних заходів. До них належать резервування каналів зв'язку, використання альтернативних засобів передачі даних, підвищення рівня захисту інформації, а також підготовка персоналу до дій в умовах порушення функціонування систем.

Важливим аспектом є також інтеграція кібернетичного та фізичного вимірів бойових дій. Порушення інформаційних процесів може безпосередньо впливати на результати застосування військ, що підтверджується сучасною практикою. У зв'язку з цим кіберзахист стає невід'ємною складовою системи управління, а його ефективність визначає загальний рівень боєздатності.

Таким чином, концептуальна сутність переходу до мережецентричного управління полягає у зміні самої філософії військового управління. Якщо традиційна модель була зорієнтована на контроль інформації, то мережецентрична - на її доцільне поширення. Якщо раніше головним було передати наказ, то тепер не менш важливо забезпечити спільне розуміння обстановки. Якщо класична система вимагала передусім слухняності, то сучасна - поєднання дисципліни, ініціативи та відповідальності.

Висновки. Отримані результати дослідження підтверджують, що трансформація систем управління військами від ієрархічної до мережецентричної моделі є об'єктивним наслідком розвитку інформаційних технологій та зміни характеру сучасних бойових дій. Встановлено, що ключовим

фактором ефективності управління є не стільки організаційна структура, скільки швидкість циркуляції інформації та здатність системи забезпечувати оперативне прийняття рішень. Доведено, що мережецентрична система управління не заперечує військову ієрархію, а доповнює її горизонтальним обміном даними, цифровою інтеграцією сил і засобів, розширенням ситуаційної обізнаності та можливістю децентралізованого прийняття рішень у межах загального задуму старшого командира.

Практичний досвід Збройних Сил України підтверджує, що впровадження мережецентричних підходів дозволяє досягти суттєвого скорочення часу реагування, підвищення точності ураження та забезпечення гнучкості управління навіть в умовах обмежених ресурсів. Водночас встановлено, що ефективність таких систем значною мірою залежить від рівня їх стійкості до зовнішніх впливів, зокрема кіберзагроз та засобів радіоелектронної боротьби.

Перспективи подальших досліджень доцільно спрямувати на розроблення методики оцінювання готовності військових частин і органів управління до роботи в мережецентричному середовищі, дослідження стійкості цифрових систем управління в умовах радіоелектронної боротьби, інтеграцію штучного інтелекту в процес підтримки прийняття рішень, а також створення моделей багатодоменого управління з урахуванням українського бойового досвіду та підвищенням рівня кіберзахисту мережецентричних систем.

Список використаних джерел:

1. Alberts D.S., Garstka J.J., Stein F.P. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington : *CCRP Publication Series*, 1999. 284 p.
2. Alberts D.S., Hayes R.E. *Power to the Edge: Command and Control in the Information Age*. Washington : *CCRP Publication Series*, 2003. 259 p.
3. Alberts D.S. *Information Age Transformation: Getting to a 21st Century Military*. Washington : *CCRP Publication Series*, 2002. 172 p.
4. Boyd J.R. *The Essence of Winning and Losing*. *Unpublished briefing*, 1995.
5. Cebrowski A.K., Garstka J. J. *Network-Centric Warfare: Its Origin and Future*. *Proceedings Magazine*, 1998. Vol. 124/1/1139.
6. Davis L. E. et al. *Russia's War in Ukraine: Identity, History and Conflict*. Santa Monica : RAND Corporation, 2023. 214 p.
7. Department of the Army. *FM 6-0 Commander and Staff Organization and Operations*. Washington : *Headquarters Department of the Army*, 2022. 384 p.
8. Department of the Army. *ADP 6-0 Mission Command: Command and Control of Army Forces*. Washington : *Headquarters Department of the Army*, 2019. 64 p.
9. Endsley M.R. *Toward a Theory of Situation Awareness in Dynamic Systems*. *Human Factors*. 1995. Vol. 37, No. 1. P. 32–64.
10. Kofman M., Lee R. *Not Built for Purpose: The Russian Military's Ill-Fated Force Design*. Arlington : CNA, 2022. 45 p.
11. Libicki M. C. *Cyberdeterrence and Cyberwar*. Santa Monica : RAND Corporation, 2009. 238 p.
12. NATO Standardization Office. *AJP-5 Allied Joint Doctrine for the Planning of Operations*. Brussels : NATO, 2019. 456 p.
13. *Russian Offensive Campaign Assessment*. Washington : *Institute for the Study of War*, 2022–2025.
14. Singer P.W., Friedman A. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford : *Oxford University Press*, 2014. 312 p.

15. Watling J., Reynolds N. Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. London : *RUSI*, 2023. 58 p.
16. Даник Ю. Г. Основи мережецентричної концепції ведення бойових дій. *Наука і оборона*, 2018. № 2. С. 12–18.
17. Даник Ю.Г., Писарчук О.О. Інформаційні технології в системах військового управління. *Збірник наукових праць ЖВІ*, 2020. № 3. С. 45–53.

References:

1. Alberts, D.S., Garstka, J.J. & Stein, F.P. (1999). Network centric warfare: Developing and leveraging information superiority. Washington, DC: *CCRP Publication Series*. 284 p.
2. Alberts, D.S. & Hayes, R.E. (2003). Power to the Edge: Command and Control in the Information Age. Washington : *CCRP Publication Series*. 259 p.
3. Alberts, D.S. (2002). *Information age transformation: Getting to a 21st century military*. Washington, DC: *CCRP Publication Series*. 172 p.
4. Boyd, J.R. (1995). The Essence of Winning and Losing. Unpublished briefing.
5. Cebrowski, A.K. & Garstka, J.J. (1998). Network-Centric Warfare: Its Origin and Future. *Proceedings Magazine*. 124/1/1139.
6. Davis, L.E. (2023). Russia's War in Ukraine: Identity, History and Conflict. *Santa Monica : RAND Corporation*. 214 p.
7. Department of the Army. (2022). FM 6-0 Commander and Staff Organization and Operations. Washington : *Headquarters Department of the Army*. 384 p.
8. Department of the Army. (2019). ADP 6-0 Mission Command: Command and Control of Army Forces. *Washington : Headquarters Department of the Army*. 64 p.
9. Endsley, M.R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*. 37 (1). Ss. 32–64.
10. Kofman, M. & Lee R. (2022). Not Built for Purpose: The Russian Military's Ill-Fated Force Design. *Arlington : CAN*. 45 p.
11. Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. *Santa Monica : RAND Corporation*. 238 p.
12. NATO Standardization Office. (2019). AJP-5 Allied Joint Doctrine for the Planning of Operations. *Brussels : NATO*. 456 p.
13. Russian Offensive Campaign Assessment. (2022-2025). *Washington : Institute for the Study of War*.
14. Singer, P.W. & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. *Oxford : Oxford University Press*. 312 p.
15. Watling, J. & Reynolds, N. (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. *London : RUSI*. 58 p.
16. Danyk, YU.H. (2018). Osnovy merezhetsentrychnoyi kontseptsiiy vedennya boyovykh diy [Fundamentals of the network-centric concept of warfare]. *Nauka i oborona*. 2. Ss. 12–18.
17. Danyk, YU.H. & Pysarchuk, O.O. (2020). Informatsiyni tekhnolohiyi v systemakh viys'kovoho upravlinnya [Information technologies in military command and control systems]. *Zbirnyk naukovykh prats' ZHVI*. 3. Ss. 45–53.