Формування єдиного інформаційного простору Міністерства оборони України на основі принципів мережецентричної війни та цифрової трансформації

Formation of a Unified Information Space for the Ministry of Defense of Ukraine Based on the Principles of Network-Centric Warfare and Digital Transformation

Вадим Колотухін
науковий співробітник науково-дослідного відділу проблем системної інтеграції, захисту інформації та технологічної підтримки інформаційних систем, e-mail: vv.vasilich1@gmail.com, ORCID ID: https://orcid.org/0000-0002-6065-4896

Андрій Дядечко
Corresponding author: доктор філософії, начальник науково-дослідної лабораторії проблем технологічної підтримки інформаційних систем, e-mail: andrewvvs@gmail.com, ORCID ID: http://orcid.org/0000-0003-0191-8326

Микола Петрушен
старший науковий співробітник науково-дослідного відділу проблем системної інтеграції, захисту інформації та технологічної підтримки інформаційних систем, e-mail: nik-petrushen@ukr.net, ORCID ID: http://orcid.org/0000-0002-7448-2765

Національний університет оборони України, м. Київ, Україна

Vadym Kolotukhin
Researcher of the Research Department for Problems of System Integration, Information Protection and Information Systems Technological Support, e-mail: vv.vasilich1@gmail.com, ORCID ID: https://orcid.org/0000-0002-6065-4896

Andrii Diadechko
Corresponding author: PhD, Head of the Research Laboratory for Problems of Information Systems Technological Support, e-mail: andrewvvs@gmail.com, ORCID ID: http://orcid.org/0000-0003-0191-8326

Mykola Petrushen
Senior Researcher of the Research Department for Problems of System Integration, Information Protection and Information Systems Technological Support, e-mail: nik-petrushen@ukr.net, ORCID ID: http://orcid.org/0000-0002-7448-2765

National Defense University of Ukraine, Kyiv, Ukraine

Received: April 11, 2026 | Revised: April 24, 2026 | Accepted: April 30, 2026

УДК 004.77:355.41:004.056

DOI: https://doi.org/10.33445/sds.2026.16.2.25

Мета роботи. Обґрунтування підходів до формування єдиного інформаційного простору Міністерства оборони України на основі принципів мережецентричної війни та цифрової трансформації, а також визначення ключових напрямів його реалізації.

Метод дослідження. Використано методи системного аналізу, узагальнення, порівняльного аналізу концепцій мережецентричності та цифрової трансформації, а також структурно-функціональний підхід для дослідження архітектури інформаційних систем оборонного відомства.

Результати дослідження. Визначено основні проблеми функціонування інформаційних систем Міністерства оборони України, зокрема їх фрагментованість, обмежену сумісність та вразливість до кіберзагроз. Обґрунтовано необхідність формування єдиного інформаційного простору та визначено ключові принципи його побудови, включаючи інтеграцію систем управління, використання захищених комунікацій, впровадження хмарних технологій і стандартів сумісності з НАТО. Запропоновано практичні напрями реалізації відповідної архітектури.

Теоретична цінність дослідження. Розвинено наукові підходи до формування єдиного інформаційного простору оборонного відомства шляхом інтеграції концепцій мережецентричної війни та цифрової трансформації.

Практична цінність дослідження. Отримані результати можуть бути використані при розробленні архітектури інформаційних систем, програм цифрової трансформації та нормативного забезпечення створення єдиного інформаційного простору Міністерства оборони України.

Оригінальність дослідження. Оригінальність полягає у комплексному обґрунтуванні підходів до формування єдиного інформаційного простору Міністерства оборони

Purpose. To substantiate approaches to the formation of a unified information space of the Ministry of Defense of Ukraine based on the principles of network-centric warfare and digital transformation, as well as to identify key directions for its implementation.

Method. The study employs methods of system analysis, generalization, and comparative analysis of the concepts of network-centric warfare and digital transformation. A structural and functional approach is used to analyze the architecture of information and communication systems of the defense sector.

Findings. The main problems of the functioning of information and communication systems of the Ministry of Defense of Ukraine are identified, including their fragmentation, limited interoperability, and vulnerability to cyber threats. The necessity of forming a unified information space is substantiated, and key principles of its development are defined, including system integration, secure communications, implementation of cloud technologies, and compliance with NATO interoperability standards. Practical directions for implementing the corresponding architecture are proposed.

Theoretical implications. The study develops scientific approaches to the formation of a unified information space of the defense sector through the integration of network-centric warfare and digital transformation concepts.

Practical value of the study. The results can be used in the development of architectures of information and communication systems, digital transformation programs, and regulatory support for the creation of a unified information space of the Ministry of Defense of Ukraine.

Originality. The originality of the study lies in the comprehensive substantiation of approaches to forming a unified information space of the Ministry of Defense of Ukraine, taking into account modern conditions of network-centric

України з урахуванням сучасних умов ведення мережецентричної війни та цифровізації.
Тип статті. Аналітично-прикладна стаття.

Ключові слова: мережецентрична війна; цифрова трансформація; єдиний інформаційний простір; Міністерство оборони України; інформаційно-комунікаційні системи; кібербезпека; сумісність з НАТО; ситуаційна обізнаність; інтеграція даних; оборонні інформаційні технології.

warfare and digitalization.
Paper type. Analytical and applied article.

Key words: Network-Centric Warfare; Digital Transformation; Unified Information Space; Ministry of Defense of Ukraine; Information and Communication Systems; Cybersecurity; NATO Interoperability; Situational Awareness; Data Integration; Defense Information Technologies.

Вступ

Сучасні воєнні конфлікти характеризуються стрімким зростанням ролі інформації, цифрових технологій та швидкості обміну даними між усіма елементами системи управління військами. Традиційні підходи до ведення бойових дій поступово трансформуються у високотехнологічні форми протиборства, де визначальним фактором досягнення переваги стає здатність забезпечити ефективну інтеграцію інформаційно-комунікаційних систем (ІКС), своєчасне отримання, оброблення та використання інформації в режимі реального часу.

У цьому контексті особливого значення набуває концепція мережецентричної війни, яка передбачає створення єдиного інформаційного простору (ЄІП), що об’єднує сили і засоби різних рівнів управління, забезпечує їхню взаємодію та підвищує рівень ситуаційної обізнаності. Реалізація таких підходів дозволяє значно скоротити час прийняття рішень, підвищити точність управління військами та забезпечити синергію дій підрозділів у складних умовах сучасного бою.

Паралельно з розвитком мережецентричних підходів відбувається активна цифрова трансформація оборонних відомств провідних держав світу, яка передбачає впровадження сучасних інформаційно-комунікаційних технологій, автоматизацію процесів управління, розвиток хмарних рішень, а також підвищення рівня кібербезпеки. Зазначені процеси формують основу для створення єдиного інформаційного середовища, здатного забезпечити ефективне функціонування сектору безпеки і оборони.

Для Міністерства оборони України (МОУ) питання формування ЄІП набуває особливої актуальності в умовах протидії російській збройній агресії та необхідності забезпечення сумісності з інформаційними системами держав-членів НАТО. Наявність розрізнених ІКС, різнорідність технологічних рішень, обмежена інтеграція та підвищені кіберзагрози ускладнюють реалізацію сучасних підходів до управління військами та потребують системного вирішення.

Водночас досвід застосування сучасних цифрових рішень, зокрема автоматизованих систем управління військами та систем ситуаційної обізнаності, свідчить про значний потенціал впровадження мережецентричних принципів у Збройних Силах (ЗС) України . Це зумовлює необхідність наукового обґрунтування підходів до формування ЄІП МОУ, що має забезпечити інтеграцію ІКС, підвищення ефективності управління військами та стійкість до сучасних викликів і загроз.

Таким чином, актуальність дослідження визначається потребою у розробленні науково обґрунтованих підходів до формування ЄІП МОУ на засадах мережецентричної війни та цифрової трансформації, що є необхідною умовою підвищення обороноздатності держави та ефективності функціонування сектору безпеки і оборони.

Теоретичні основи дослідження

Теоретичну основу дослідження становлять сучасні підходи до організації інформаційного забезпечення військових операцій, концепція мережецентричної війни, а також положення цифрової трансформації оборонного сектору, які визначають напрям розвитку ІКС у збройних силах провідних держав світу.

Концепція мережецентричної війни базується на ідеї досягнення інформаційної переваги шляхом інтеграції всіх елементів бойової системи в єдину інформаційну мережу. Її

ключовими положеннями є забезпечення безперервного обміну даними, підвищення ситуаційної обізнаності, скорочення циклу прийняття рішень та досягнення синергетичного ефекту від узгоджених дій різнорідних сил і засобів. В основі цієї концепції лежить принцип об'єднання сенсорів, засобів ураження та органів управління в інтегроване інформаційне середовище, що функціонує в режимі реального часу.

Подальший розвиток зазначених підходів реалізується через концепції C4ISR та C5ISR, які передбачають інтеграцію функцій управління, зв'язку, комп'ютерних систем, розвідки, спостереження та рекогносцировки. Застосування таких підходів забезпечує формування єдиної інформаційної картини бойових дій та створює передумови для ефективного управління військами на всіх рівнях.

Водночас цифрова трансформація оборонного сектору розглядається як комплексний процес впровадження сучасних інформаційно-комунікаційних технологій у всі сфери діяльності Міністерства оборони, що охоплює автоматизацію управлінських процесів, розвиток цифрової інфраструктури, використання хмарних обчислень, великих даних та штучного інтелекту. Цифрова трансформація створює технологічну основу для реалізації мережецентричних підходів, забезпечуючи інтеграцію інформаційних ресурсів, підвищення їх доступності та надійності.

Важливим теоретичним аспектом є поняття ЄІП, який визначається як сукупність взаємопов'язаних ІКС, інформаційних ресурсів та технологій, що забезпечують збір, оброблення, зберігання та обмін інформацією між усіма суб'єктами управління в єдиному стандартизованому середовищі. Формування такого простору передбачає уніфікацію протоколів обміну даними, стандартизацію форматів інформації, забезпечення інтероперабельності систем та впровадження єдиних принципів управління даними.

Окрему роль у формуванні ЄІП відіграє забезпечення кібербезпеки, яка розглядається як невід'ємна складова функціонування ІКС. Сучасні підходи передбачають створення багаторівневих систем захисту інформації, впровадження механізмів криптографічного захисту, систем виявлення та реагування на кіберінциденти, а також забезпечення стійкості інформаційної інфраструктури до зовнішніх впливів.

З урахуванням досвіду держав-членів НАТО, важливим елементом теоретичної бази є принципи інтероперабельності, що передбачають сумісність ІКС на технічному, семантичному та організаційному рівнях. Це досягається шляхом застосування уніфікованих стандартів обміну даними, протоколів зв'язку та архітектурних підходів до побудови інформаційних систем.

Таким чином, теоретичні основи дослідження формуються на перетині концепцій мережецентричної війни та цифрової трансформації, які у взаємозв'язку визначають підходи до формування ЄІП МОУ як інтегрованого, захищеного та адаптивного середовища функціонування ІКС.

Постановка проблеми

У сучасних умовах ведення бойових дій ефективність функціонування ЗС України значною мірою визначається здатністю забезпечити своєчасний, достовірний та захищений обмін інформацією між різними рівнями управління, підрозділами та союзниками. В умовах високої динаміки бойових дій та зростання ролі інформаційного чинника ключового значення набуває формування ЄІП МОУ, який забезпечує інтеграцію ІКС, підвищення ситуаційної обізнаності та ефективність управління військами [1, 2].

Разом з тим, на сьогодні існує низка проблем, що суттєво ускладнюють реалізацію зазначеного завдання. Насамперед це фрагментованість ІКС, які створювалися в різний час, за різними стандартами та без урахування необхідності їх подальшої інтеграції [3, 4]. Значна частина інфраструктури залишається застарілою, що обмежує можливості впровадження сучасних цифрових технологій та знижує рівень кіберзахисту [5]. Крім того, недостатній рівень

сумісності з інформаційними системами держав-членів НАТО ускладнює ефективну взаємодію з партнерами, а зростання кіберзагроз потребує впровадження комплексних підходів до захисту інформації [2, 6]. Важливим стримуючим фактором також залишаються обмежені фінансові та кадрові ресурси.

Аналіз наукових досліджень і публікацій свідчить, що проблематика мережецентричної війни та цифрової трансформації оборонного сектору активно розглядається як у вітчизняних, так і в зарубіжних джерелах. Зокрема, у працях вітчизняних науковців розкрито сутність та принципи мережецентричної війни, особливості її реалізації в сучасних умовах, а також підходи до забезпечення інформаційної переваги [1, 7, 8]. Значна увага приділяється питанням розвитку інформаційно-аналітичних систем, інтеграції інформаційних ресурсів та застосування сучасних технологій у військовій сфері [9, 10].

У зарубіжних дослідженнях, зокрема в доктринальних документах США та країн НАТО (Joint Vision 2010, Joint Vision 2020, Digital Modernization Strategy), сформовано концептуальні засади мережецентричного підходу та цифрової трансформації оборонних відомств, що передбачають створення інтегрованих інформаційних середовищ, розвиток стандартів інтероперабельності та забезпечення кіберстійкості інформаційної інфраструктури [2].

Приклад мережецентричної військової операції згідно [11] наведений на рисунку 1.

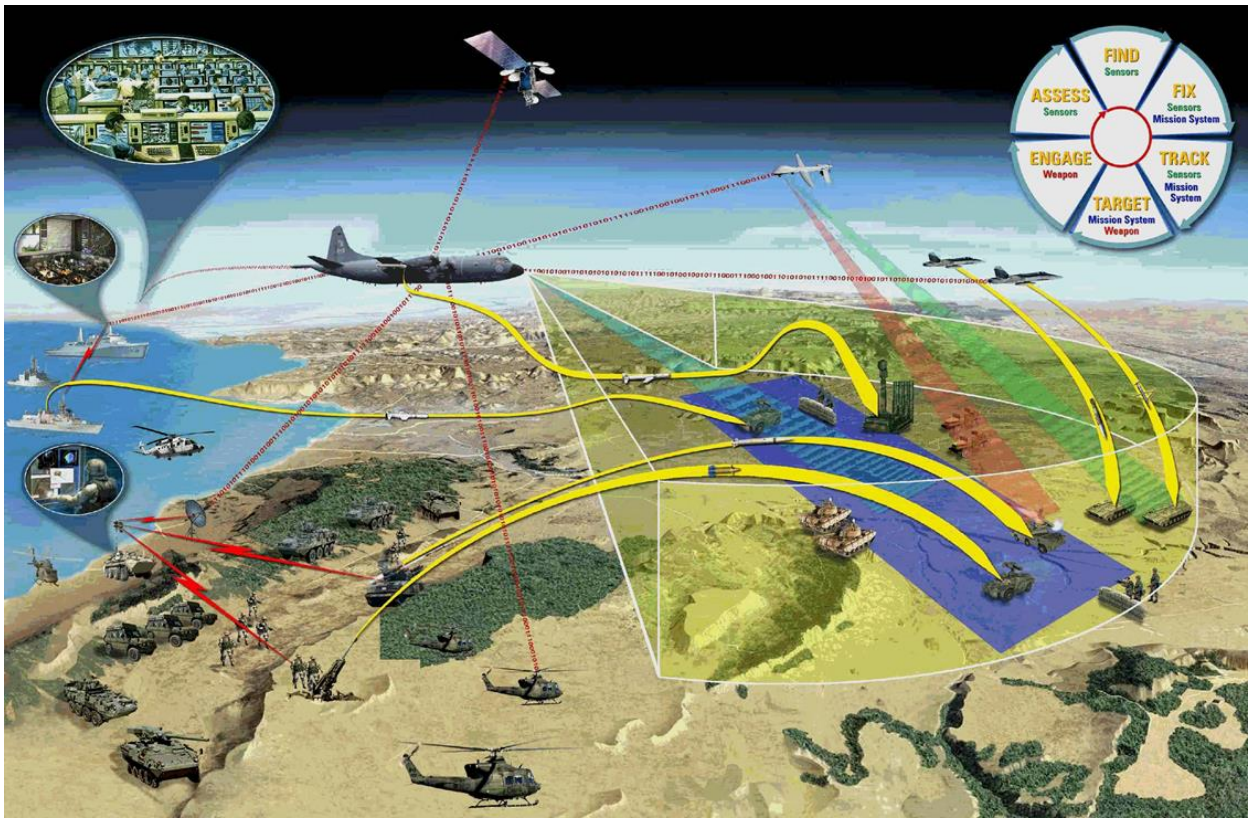

Рисунок 1: Приклад мережецентричної військової операції [11]

Незважаючи на значну кількість досліджень, питання формування ЄІП МОУ з урахуванням одночасного впливу концепцій мережецентричної війни та цифрової трансформації залишається недостатньо опрацьованим. Існуючі підходи, як правило, розглядають зазначені концепції окремо або без урахування специфіки функціонування ІКС у секторі безпеки і оборони України [9, 10].

Практичний досвід застосування сучасних ІКС, зокрема систем ситуаційної обізнаності та автоматизованих систем управління військами, підтверджує ефективність впровадження

мережецентричних принципів [5]. Водночас відсутність цілісної архітектури ЄІП, узгоджених стандартів та комплексного підходу до інтеграції систем обмежує досягнення максимального ефекту від їх використання.

Концепція ЄІП оборонного відомства за версією Digital Modernization Strategy (DMS) Міністерства оборони Сполучених Штатів Америки [12] представлена на рисунку 2.

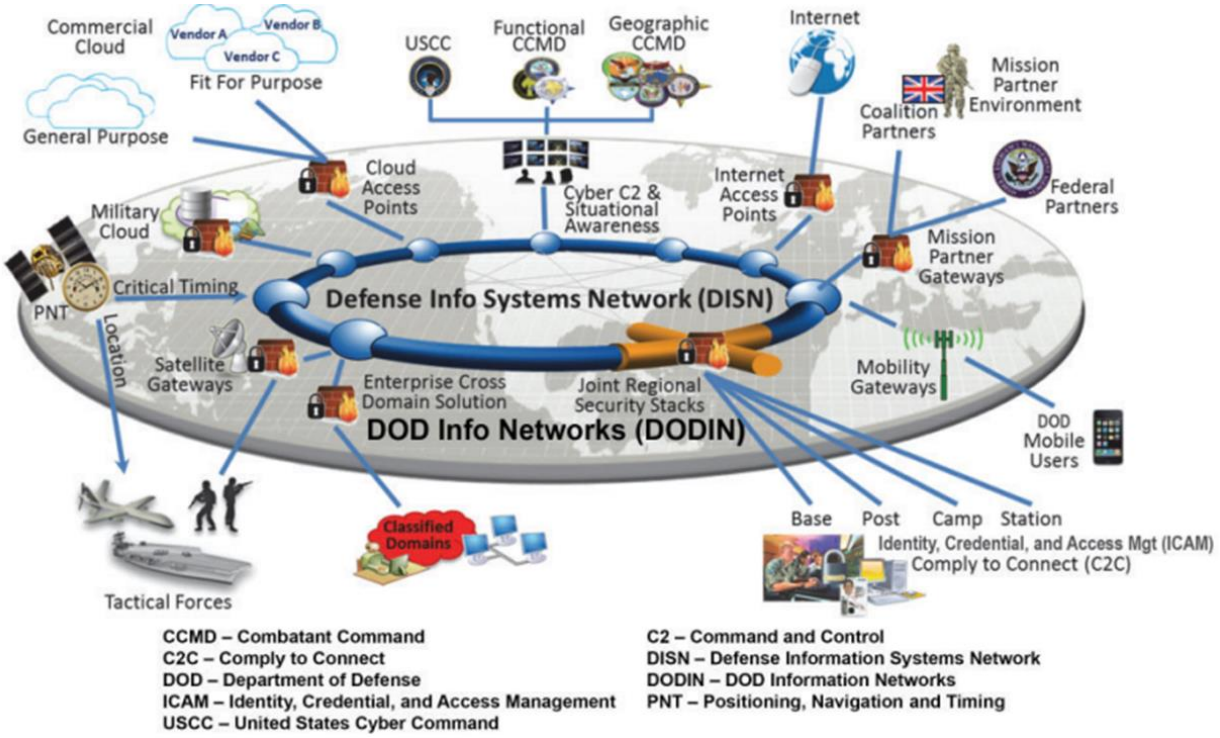

Рисунок 2: Бачення єдиного інформаційного простору оборонного відомства [12]

Таким чином, існує науково-практична проблема, яка полягає у необхідності обґрунтування підходів до формування ЄІП МОУ, що забезпечить інтеграцію ІКС, підвищення ефективності управління військами, сумісність із системами партнерів та стійкість до сучасних кіберзагроз.

Методологія дослідження

Методологічною основою дослідження є сукупність загальнонаукових та спеціальних методів, що забезпечують комплексне вивчення процесів формування ЄІП МОУ в умовах мережецентричної війни та цифрової трансформації.

У ході дослідження використано системний підхід, який дозволяє розглядати ЄІП як складну інтегровану систему, що об’єднує ІКС, інформаційні ресурси, засоби оброблення даних та організаційні механізми управління. Застосування системного підходу забезпечило можливість визначення взаємозв’язків між окремими елементами системи, а також оцінювання їх впливу на загальну ефективність функціонування.

Метод структурно-функціонального аналізу використано для дослідження архітектури ІКС МОУ, визначення їх функціональних можливостей, рівня інтеграції та відповідності сучасним вимогам. Це дозволило виявити основні проблеми, пов’язані з фрагментованістю систем, обмеженою інтероперабельністю та недостатнім рівнем кіберзахисту.

Порівняльний аналіз застосовано для зіставлення вітчизняних підходів до розвитку ІКС із концепціями мережецентричної війни та цифрової трансформації, що використовуються в

країнах-членах НАТО. Це дало змогу визначити ключові відмінності, а також напрями адаптації міжнародного досвіду до умов функціонування сектору безпеки і оборони України.

Метод узагальнення використано для систематизації наукових положень, результатів досліджень і практичного досвіду впровадження сучасних цифрових рішень у військовій сфері, зокрема автоматизованих систем управління військами та систем ситуаційної обізнаності. На основі цього сформовано узагальнені підходи до формування ЄІП.

Крім того, у дослідженні застосовано елементи експертно-аналітичного підходу, що дозволило врахувати сучасні тенденції розвитку інформаційно-комунікаційних технологій, кіберзагроз та вимог до забезпечення інтероперабельності з інформаційними системами партнерів.

Застосування зазначених методів у сукупності забезпечило отримання обґрунтованих результатів дослідження та дозволило сформулювати практичні рекомендації щодо формування ЄІП МОУ як інтегрованого, захищеного та адаптивного середовища функціонування ІКС.

Результати

У результаті проведеного дослідження, на основі аналізу сучасних підходів до розвитку ІКС, концепцій мережецентричної війни та цифрової трансформації, а також оцінювання стану ІКС МОУ, визначено ключові проблеми, тенденції та напрями формування ЄІП.

Отримані результати дозволили систематизувати існуючі підходи, виявити обмеження функціонування ІКС та обґрунтувати необхідність їх інтеграції в єдине інформаційне середовище, що забезпечує ефективне управління військами, підвищення ситуаційної обізнаності та стійкість до сучасних загроз.

1. Аналіз сучасного стану інформаційно-комунікаційних систем Міністерства оборони України.

Аналіз сучасного стану ІКС МОУ свідчить про наявність суттєвих проблем, що обмежують ефективність їх функціонування в умовах ведення мережецентричних бойових дій.

Однією з ключових проблем є фрагментованість ІКС, які створювалися в різні періоди, із застосуванням різних технологічних підходів і стандартів, що призвело до їх низького рівня інтеграції.

Під фрагментованістю ІКС у даному дослідженні розуміється стан, за якого окремі системи функціонують ізольовано або частково інтегровано, мають різнорідні програмно-технічні платформи, несумісні формати даних та відсутність уніфікованих протоколів обміну інформацією. Такий стан характеризується відсутністю єдиного центру управління даними, дублюванням функціональних можливостей систем, а також обмеженою можливістю обміну інформацією між підрозділами в режимі реального часу.

Фрагментованість проявляється на кількох рівнях:

технічному – використання різнорідних апаратно-програмних платформ і каналів зв’язку;

інформаційному – відсутність уніфікованих форматів даних і стандартів їх оброблення;

організаційному – відсутність єдиних підходів до управління інформаційними ресурсами та взаємодії між підрозділами.

Це ускладнює обмін даними між підрозділами, знижує швидкість прийняття рішень та негативно впливає на загальну ефективність управління військами [3, 4, 9].

Значна частина наявної інфраструктури базується на застарілих технічних і програмних рішеннях, що не відповідають сучасним вимогам до швидкості оброблення інформації, масштабованості та кіберзахисту. Це обмежує можливості впровадження новітніх цифрових технологій, таких як хмарні обчислення, обробка великих даних та штучний інтелект [5].

Суттєвою проблемою є також недостатній рівень інтероперабельності ІКС із системами держав-членів НАТО, що ускладнює ефективну взаємодію з міжнародними партнерами. Відсутність уніфікованих стандартів обміну даними, протоколів зв'язку та узгоджених архітектурних рішень знижує можливості інтеграції в ЄІП союзників [2].

Разом з тим, сучасні умови ведення бойових дій характеризуються зростанням кіберзагроз, що спрямовані на порушення функціонування критично важливих ІКС. Це вимагає впровадження комплексних підходів до забезпечення кібербезпеки, включаючи використання криптографічного захисту, систем виявлення та реагування на інциденти, а також підвищення стійкості інформаційної інфраструктури до зовнішніх впливів [6].

Водночас, незважаючи на зазначені проблеми, у ЗС України вже впроваджуються сучасні інформаційно-комунікаційні рішення, що відповідають принципам мережецентричної війни. Зокрема, застосування автоматизованих систем управління військами та систем ситуаційної обізнаності, наприклад система «Дельта», дозволяє інтегрувати дані з різних джерел (розвідки, безпілотних систем, артилерії тощо) та забезпечувати їх відображення в режимі реального часу. Використання супутникових комунікацій, зокрема Starlink, забезпечує стійкий зв'язок між підрозділами навіть у складних умовах бойових дій.

Такі рішення сприяють підвищенню рівня ситуаційної обізнаності, скороченню часу прийняття рішень та покращенню координації дій підрозділів. Водночас їх ефективність значною мірою обмежується відсутністю єдиної архітектури інформаційного простору, яка б забезпечувала повноцінну інтеграцію всіх ІКС.

Отже, результати аналізу свідчать, що сучасний стан ІКС МОУ характеризується наявністю як суттєвих обмежень, так і значного потенціалу розвитку. Це зумовлює необхідність переходу від фрагментованих рішень до формування ЄІП, який забезпечить інтеграцію систем, підвищення ефективності управління військами та відповідність сучасним вимогам мережецентричної війни.

2. Концептуальні засади формування єдиного інформаційного простору Міністерства оборони України.

Формування ЄІП МОУ в умовах мережецентричної війни та цифрової трансформації потребує застосування комплексного підходу, що поєднує технологічні, організаційні та функціональні аспекти розвитку ІКС.

У рамках даного дослідження під ЄІП пропонується розуміти інтегроване середовище функціонування ІКС, яке забезпечує уніфікований збір, оброблення, зберігання та обмін інформацією між усіма суб'єктами управління в режимі, близькому до реального часу, на основі єдиних стандартів, протоколів та правил взаємодії.

Ключовою умовою формування такого простору є забезпечення інтероперабельності ІКС. Інтероперабельність у даному контексті розглядається як здатність різнорідних систем взаємодіяти між собою шляхом обміну даними та їх коректної інтерпретації незалежно від використовуваних технологій і платформ. Вона реалізується на трьох рівнях:

технічному – забезпечення сумісності апаратних і програмних засобів та каналів зв'язку;

семантичному – уніфікація форматів даних, їх структури та змісту;

організаційному – узгодження процедур, правил та регламентів обміну інформацією.

Формування ЄІП повинно базуватися на таких концептуальних засадах:

1. Інтеграційність – об'єднання всіх ІКС у єдину мережу з можливістю централізованого та децентралізованого доступу до інформаційних ресурсів.

2. Модульність архітектури – побудова системи за принципом відкритої архітектури, що дозволяє інтегрувати нові компоненти без необхідності повної перебудови системи.

3. Масштабованість – здатність системи адаптуватися до зростання обсягів даних, кількості користувачів та функціональних завдань.

4. Стійкість та відмовостійкість – забезпечення безперервності функціонування системи навіть в умовах впливу зовнішніх загроз або пошкодження окремих елементів.

5. Кіберзахищеність – впровадження багаторівневих механізмів захисту інформації, включаючи криптографічний захист, багатофакторну автентифікацію, системи виявлення та реагування на кіберінциденти [6].

6. Сумісність із системами партнерів – забезпечення відповідності стандартам НАТО щодо обміну даними та взаємодії ІКС [2].

Важливим елементом реалізації зазначених засад є впровадження сучасних цифрових технологій, зокрема хмарних обчислень, які забезпечують гнучкість розгортання інфраструктури та доступ до обчислювальних ресурсів, а також технологій оброблення великих даних і штучного інтелекту, що дозволяють здійснювати оперативний аналіз інформації та підтримку прийняття рішень.

Особливе значення у формуванні ЄІП має використання автоматизованих систем управління військами та систем ситуаційної обізнаності, які забезпечують інтеграцію даних з різних джерел (розвідки, безпілотних систем, засобів ураження) та їх візуалізацію в режимі реального часу. Це дозволяє значно підвищити ефективність управління військами, скоротити цикл прийняття рішень та забезпечити координацію дій підрозділів.

Крім того, формування ЄІП передбачає створення централізованих органів управління інформаційними ресурсами та процесами їх оброблення, що забезпечить узгодженість функціонування ІКС, їх розвиток та адаптацію до сучасних викликів.

Таким чином, концептуальні засади формування ЄІП МОУ базуються на інтеграції принципів мережецентричної війни та цифрової трансформації, що у сукупності забезпечують створення ефективного, захищеного та адаптивного середовища функціонування ІКС.

3. Практичні рекомендації щодо формування єдиного інформаційного простору Міністерства оборони України.

На основі проведеного дослідження, аналізу сучасного стану ІКС МОУ та визначених концептуальних засад їх розвитку сформовано практичні рекомендації щодо формування ЄІП.

1. Розроблення єдиної архітектурної моделі інформаційного простору. Необхідно сформувати багаторівневу архітектуру ЄІП, яка включатиме мережевий рівень, рівень даних та рівень прикладних сервісів. Така модель має базуватися на використанні відкритих стандартів і протоколів обміну даними, що забезпечить інтеграцію різнорідних ІКС та їх подальший розвиток.

2. Інтеграція та уніфікація інформаційно-комунікаційних систем. Доцільно здійснити поетапну модернізацію та об’єднання існуючих ІКС у єдину платформу із забезпеченням їх взаємодії через захищені канали зв’язку. Особливу увагу слід приділити усуненню дублювання функцій та забезпеченню узгодженості інформаційних потоків.

3. Забезпечення інтероперабельності із системами партнерів. Необхідно впровадити стандарти обміну даними та протоколи зв’язку, що використовуються в країнах-членах НАТО, з метою досягнення сумісності ІКС та забезпечення ефективної взаємодії з міжнародними партнерами [2].

4. Розвиток хмарної інфраструктури та технологій оброблення даних. Доцільно розширити використання захищених хмарних технологій для забезпечення гнучкості розгортання інформаційних ресурсів, підвищення відмовостійкості систем та оброблення великих обсягів даних. Це дозволить підвищити ефективність функціонування ІКС в умовах динамічних змін обстановки.

5. Посилення кібербезпеки інформаційного простору. Формування ЄІП повинно супроводжуватися впровадженням комплексної системи кіберзахисту, що включає шифрування каналів передачі даних, багатофакторну автентифікацію, системи виявлення та

запобігання вторгненням, а також створення механізмів оперативного реагування на кіберінциденти [6].

6. Впровадження технологій штучного інтелекту та аналітики даних. Рекомендується застосовувати технології штучного інтелекту для аналізу великих масивів даних, прогнозування розвитку бойової обстановки та підтримки прийняття управлінських рішень. Це дозволить підвищити швидкість та обґрунтованість управлінських процесів.

7. Інтеграція безпілотних і роботизованих систем. Необхідно забезпечити включення безпілотних літальних апаратів та роботизованих платформ до ЄІП для отримання розвідувальної інформації, коригування вогню та логістичного забезпечення, що відповідає принципам мережецентричної війни.

8. Створення централізованої системи управління інформаційним простором. Доцільно створити єдиний центр управління інформаційними ресурсами (за аналогією з функціональними структурами типу J6 у країнах НАТО), який забезпечуватиме координацію розвитку ІКС, управління інцидентами та контроль їх функціонування.

9. Підготовка та розвиток кадрового потенціалу. Необхідно посилити підготовку фахівців у сфері інформаційно-комунікаційних технологій та кібербезпеки, а також забезпечити підвищення цифрових компетенцій військовослужбовців для ефективного використання сучасних систем.

10. Поетапне впровадження та апробація рішень. Рекомендується реалізовувати формування ЄІП поетапно, починаючи з пілотних проєктів, з подальшим масштабуванням і адаптацією рішень з урахуванням досвіду їх практичного застосування.

Таким чином, в результаті дослідження встановлено, що сучасний стан ІКС МОУ характеризується фрагментованістю, обмеженою інтероперабельністю та наявністю кіберзагроз, що знижує ефективність управління військами в умовах мережецентричних бойових дій. Водночас визначено наявність значного потенціалу розвитку, пов’язаного із впровадженням сучасних цифрових технологій та автоматизованих систем управління.

Обґрунтовано концептуальні засади формування ЄІП, що базуються на принципах інтеграційності, модульності, масштабованості, кіберзахищеності та сумісності з системами партнерів. На цій основі сформовано комплекс практичних рекомендацій, спрямованих на інтеграцію ІКС, розвиток цифрової інфраструктури та підвищення ефективності управління військами.

Обговорення

Отримані результати дослідження підтверджують, що формування ЄІП Міністерства оборони України є системною та багаторівневою проблемою, яка не може бути вирішена виключно шляхом технічної модернізації інформаційно-комунікаційних систем. Як показано у роботі, ключовим обмеженням залишається не лише фрагментованість ІКС, але й відсутність узгодженої архітектури та єдиних стандартів управління даними, що знижує ефективність навіть сучасних цифрових рішень.

У контексті порівняння з підходами держав-членів НАТО слід відзначити, що запропоновані у статті концептуальні засади загалом відповідають сучасним тенденціям розвитку мережецентричних систем, зокрема щодо забезпечення інтероперабельності та використання хмарних технологій. Водночас існує ризик певного спрощення причинно-наслідкових зв’язків: впровадження технологій саме по собі не гарантує досягнення синергетичного ефекту без відповідних організаційних змін, включаючи реформування процесів управління та підготовку персоналу.

Особливої уваги потребує теза про визначальну роль цифрової трансформації як основи формування ЄІП. Такий підхід є обґрунтованим, однак частково ігнорує обмеження ресурсного характеру та інституційну інерцію, які можуть суттєво впливати на темпи і

результати трансформації. Крім того, питання кібербезпеки у роботі розглянуто переважно як технічне завдання, тоді як сучасні дослідження підкреслюють його комплексний, у тому числі організаційно-поведінковий характер.

Сильним аспектом дослідження є поєднання теоретичних положень із практичними рекомендаціями, що підвищує його прикладну цінність. Водночас запропоновані рекомендації мають переважно загальний характер і потребують подальшої формалізації у вигляді конкретних моделей, показників ефективності та механізмів оцінювання результатів впровадження.

Таким чином, результати дослідження створюють підґрунтя для подальшого розвитку науково-методичного забезпечення формування ЄІП МОУ, однак потребують поглиблення в частині кількісного аналізу, верифікації запропонованих підходів та врахування інституційних і ресурсних обмежень.

Висновки

У статті розглянуто актуальне науково-практичне завдання – формування ЄІП МОУ в умовах мережецентричної війни та цифрової трансформації.

За результатами дослідження встановлено, що ефективність функціонування ЗС України значною мірою залежить від рівня інтеграції ІКС, забезпечення їх інтероперабельності та стійкості до кіберзагроз. Виявлені проблеми, зокрема фрагментованість систем, застарілість інфраструктури та обмежена сумісність із системами партнерів, потребують системного вирішення.

У роботі розвинено підходи до формування ЄІП як інтегрованого середовища функціонування ІКС, що забезпечує ефективний обмін інформацією, підвищення ситуаційної обізнаності та підтримку прийняття управлінських рішень.

Практичним результатом дослідження є сформований комплекс рекомендацій щодо розвитку архітектури інформаційного простору, інтеграції систем, впровадження сучасних цифрових технологій, підвищення рівня кібербезпеки та забезпечення сумісності з інформаційними системами держав-членів НАТО.

Реалізація запропонованих підходів дозволить підвищити ефективність управління військами, забезпечити стійкість інформаційної інфраструктури до сучасних загроз та сприятиме досягненню технологічної переваги ЗС України в умовах сучасних збройних конфліктів.

Перспективи подальших досліджень полягають у розробленні формалізованої архітектурної моделі ЄІП МОУ, удосконаленні методів забезпечення інтероперабельності ІКС, а також у дослідженні підходів до застосування штучного інтелекту для підтримки прийняття рішень у системах управління військами. Окремого опрацювання потребують питання створення нормативного забезпечення функціонування ЄІП та оцінювання ефективності його впровадження в умовах реальної експлуатації.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Опрощенко Ю. О. Мережецентрична війна: основні риси, особливості та принципи ведення. Соціально-політичні студії: наук. альманах, ОНУ імені І. І. Мечникова, № 2, 2018, с. 7-11. URL: https://dspace.onu.edu.ua/server/api/core/bitstreams/ee58b2b4-c91f-4b9f-9a37-dd4709b38ca2/content. (Дата звернення: 09.03.2026).

2. Концепція мережецентричної війни. Доктрина США – «Спільне бачення» розвитку збройних сил США (версії «Joint Vision 2010» і «Joint Vision 2020»). URL: https://apps.dtic.mil/sti/tr/pdf/ADA377926.pdf. (Дата звернення: 09.03.2026).
3. Молодцов В. А., Писарєв А. В., Радченко І. О., Тузіков С. А., Лисенко О. В. Сутність і зміст електромагнітної війни в асиметричних діях повномасштабної мережецентричної війни за поглядами командування збройних сил США. Збірник наукових праць ХНУПС, № 1(71), 2022, с. 13-21. DOI: https://doi.org/10.30748/zhups.2022.71.02.
4. Трофименко О.Г., Дубовий Я.В. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства. Порівняльно-аналітичне право, № 1, 2017, с. 189–192. URL: https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/bab9d235-b6fb-4cb4-b25b-40203d54c039/content. (Дата звернення: 11.03.2026).
5. Олександр Ян. Як українська армія збирає бойовий досвід: від штучного інтелекту до нової структури ВВД. Інформаційний портал «Мілітарний». URL: https://militarnyi.com/uk/articles/shtuchnyj-intelekt-forumy-ta-ofitsery-vvd-yak-ukrayinska-armiya-zbyraye-bojovyj-dosvid/. (Дата звернення: 12.03.2026).
6. Молодцов В. А., Писарєв А. В., Радченко І. О. Можливості асиметричної протидії у мережецентричній війні. Збірник тез доповідей VI Всеукраїнської науково-практичної конференції. Харків: НАНГУ, 2021.
7. Ярош С.П. Способи асиметричної протидії збройним силам, побудованим для ведення мережецентричної війни. Збірник наукових праць Харківського університету Повітряних сил, Вип. 1, 2012, с. 20-28. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2012_1_8. (Дата звернення: 12.03.2026).
8. Ярош С. П. Аналіз ведення бойових дій, тактики застосування засобів повітряного нападу і використання нових інформаційних технологій у ході воєнного конфлікту в Лівії в 2011 році. Наука і техніка Повітряних Сил Збройних Сил України, Харків, № 2 (6), 2011, с. 19-25. URL: http://nbuv.gov.ua/UJRN/Nitps_2011_2_8. (Дата звернення: 12.03.2026).
9. Головін О. О., Стрижак О. Є. Окремі технологічні аспекти впровадження принципів мережецентричності в перспективні знання – орієнтовані інформаційно-аналітичні системи управління розвитком озброєння та військової техніки. Озброєння та військова техніка, Київ, ЦНДІ ОВТ ЗС України, № 4 (20), 2018, с. 19-25. DOI: https://doi.org/10.34169/2414-0651.2018.4(20).19-25.
10. Головін О. О., Стрижак О. Є. Побудова мережецентричної системи підтримки процесів оснащення і розвитку озброєння та військової техніки на основі використання трансдисциплінарних процедур інтеграції інформаційних ресурсів. Системи озброєння і військова техніка, № 4(56), 2018, с. 81-91. DOI: https://doi.org/10.30748/soivt.2018.56.12.
11. Network Centric Operation. URL: https://www.bsipk.net/solution_networkcentric.html. (Дата звернення: 23.03.2026).
12. Digital Modernization Strategy – Related Enterprise Information Technology Initiatives. United States Department of Defense, 2020, p. 36-40. URL: https://www.dote.osd.mil/Portals/97/pub/reports/FY2022/dod/2022dms.pdf?ver=eYBu_u4mMHS6qY5gCsl4CQ%3D%3D. (Дата звернення 23.03.2026).

References

1. Oproshchenko, Yu. O. (2018). *Merezhetsentrychna viina: Osnovni rysy, osoblyvosti ta pryntsypy vedennia* [Network-centric warfare: Main features, characteristics and principles]. *Sotsialno-politychni studii*, (2), 7–11. Retrieved March 9, 2026, from https://dspace.onu.edu.ua/server/api/core/bitstreams/ee58b2b4-c91f-4b9f-9a37-dd4709b38ca2/content

2. Joint Vision 2010 and Joint Vision 2020. (n.d.). *Concept of network-centric warfare*. Retrieved March 9, 2026, from https://apps.dtic.mil/sti/tr/pdf/ADA377926.pdf
3. Molodtsov, V. A., Pysariev, A. V., Radchenko, I. O., Tuzikov, S. A., & Lysenko, O. V. (2022). *Sutnist i zmist elektromahnitnoi viiny v asymetrychnykh diiakh povnomasshtabnoi merezhetsentrychnoi viiny za pohliadamy komanduvannia Zbroinykh syl SShA* [The essence and content of electromagnetic warfare in asymmetric actions of full-scale network-centric warfare according to the views of the U.S. Armed Forces command]. *Zbirnyk naukovykh prats KhNUPS*, 1(71), 13–21. https://doi.org/10.30748/zhups.2022.71.02
4. Trofymenko, O. H., & Dubovyi, Ya. V. (2017). *Evoliutsiia pohliadiv na informatsiini viiny v epokhu informatsiinoho suspilstva* [Evolution of views on information warfare in the information society era]. *Porivnialno-analitychne pravo*, (1), 189–192. Retrieved March 11, 2026, from https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/bab9d235-b6fb-4cb4-b25b-40203d54c039/content
5. Yan, O. (n.d.). *Yak ukrainska armiia zbyraie boiovyi dosvid: Vid shtuchnoho intelektu do novoi struktury VVD* [How the Ukrainian army accumulates combat experience: From artificial intelligence to a new VVD structure]. *Militarnyi*. Retrieved March 12, 2026, from https://militarnyi.com/uk/articles/shtuchnyj-intelekt-forumy-ta-ofitsery-vvd-yak-ukrayinska-armiya-zbyraye-bojovyj-dosvid/
6. Molodtsov, V. A., Pysariev, A. V., & Radchenko, I. O. (2021). *Mozhlyvosti asymetrychnoi protydii u merezhetsentrychnii viini* [Possibilities of asymmetric counteraction in network-centric warfare]. In *Proceedings of the VI All-Ukrainian Scientific and Practical Conference*. Kharkiv: NANGU.
7. Yarosh, S. P. (2012). *Sposoby asymetrychnoi protydii zbroinym sylam, pobudovanym dlia vedennia merezhetsentrychnoi viiny* [Methods of asymmetric counteraction to armed forces designed for network-centric warfare]. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh syl*, (1), 20–28. Retrieved March 12, 2026, from http://nbuv.gov.ua/UJRN/ZKhUPS_2012_1_8
8. Yarosh, S. P. (2011). *Analiz vedennia boiovykh dii, taktyky zastosuvannia zasobiv povitrianoho napadu i vykorystannia novykh informatsiinykh tekhnolohii u khodi voiennoho konfliktu v Livii v 2011 rotsi* [Analysis of combat operations, air attack tactics, and the use of new information technologies during the 2011 Libya conflict]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy*, 2(6), 19–25. Retrieved March 12, 2026, from http://nbuv.gov.ua/UJRN/Nitps_2011_2_8
9. Holovin, O. O., & Stryzhak, O. Ye. (2018). *Okremi tekhnolohichni aspekty vprovadzhennia pryntsypiv merezhetsentrychnosti v perspektyvni znannia-oriientovani informatsiino-analitychni systemy upravlinnia rozvytkom ozbroiennia ta viiskovoi tekhniky* [Technological aspects of implementing network-centric principles in knowledge-oriented information-analytical systems for armament development management]. *Ozbroiennia ta viiskova tekhnika*, (4(20)), 19–25. https://doi.org/10.34169/2414-0651.2018.4(20).19-25
10. Holovin, O. O., & Stryzhak, O. Ye. (2018). *Pobudova merezhetsentrychnoi systemy pidtrymky protsesiv osnashchennia i rozvytku ozbroiennia ta viiskovoi tekhniky na osnovi vykorystannia transdystsyplinarnykh protsedur intehratsii informatsiinykh resursiv* [Development of a network-centric system for supporting armament development processes based on transdisciplinary integration of information resources]. *Systemy ozbroiennia i viiskova tekhnika*, (4(56)), 81–91. https://doi.org/10.30748/soivt.2018.56.12
11. Network centric operation. (n.d.). Retrieved March 23, 2026, from https://www.bsipk.net/solution_networkcentric.html
12. United States Department of Defense. (2020). *Digital modernization strategy: Related enterprise information technology initiatives* (pp. 36–40). Retrieved March 23, 2026, from https://www.dote.osd.mil/Portals/97/pub/reports/FY2022/dod/2022dms.pdf