

**ВІЙСЬКОВИЙ ІНСТИТУТ КИЇВСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА**

ЗБІРНИК НАУКОВИХ ПРАЦЬ

**ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА**

Виходить 4 рази на рік

№ 89

Згідно з наказом МОН №1188 від 24.09.2020, п. №156 Додатку 5 "Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка" включено до категорії "Б" за спеціальностями:

- F4 Системний аналіз та наука про дані (124);
- F6 Інформаційні системи і технології (126);
- K6 Забезпечення військ (сил) (254);
- K7 Озброєння та військова техніка (255).

**MILITARY INSTITUTE OF TARAS SHEVCHENKO NATIONAL
UNIVERSITY OF KYIV**

**COLLECTION OF SCIENTIFIC WORKS
OF THE MILITARY INSTITUTE OF TARAS SHEVCHENKO NATIONAL
UNIVERSITY OF KYIV**

It comes out 4 times a year

№ 89

According to the Order of the Ministry of Education and Science No. 1188 from 09/24/2020, item No. 156 of Appendix 5 "Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv" is included in category "B" by specialties:

- F4 System analysis and data science (124);
- F6 Information systems and technologies (126);
- K6 Supply of troops (forces) (254);
- K7 Armament and military equipment (255).

KYIV – 2025

УДК 621.43
ББК 32-26.8-68.49
Збірник наукових праць Військового інституту Київського національного університету імені
Тараса Шевченка. К.: ВІКНУ, 2025. № 89. 95 с.

Голова редакційної колегії:

Ленков С.В. доктор технічних наук, професор, ВІКНУ;

Члени редакційної колегії:

Анісімов А.В.	доктор фізико-математичних наук, професор, член-кор. НАНУ,
Барабаш О.В.	доктор технічних наук, професор, НТУУ КПІ;
Гунченко Ю.О.	доктор технічних наук, професор, ОНУ;
Жиров Г.Б.	кандидат технічних наук, старший науковий співробітник, КНУ;
Заславський В.А.	доктор технічних наук, професор, КНУ;
Карпінський	доктор технічних наук, професор, УНТ, Краків (Польща)
Лепіх Я.І.	доктор фізико-математичних наук, професор, ОНУ;
Петров О.С.	доктор технічних наук, професор, УНТ, Краків (Польща);
Погорілий С.Д.	доктор технічних наук, професор, КНУ;
Толок І.В.	кандидат педагогічних наук, доцент, НУЦЗУ;
Хайрова Н.Ф.	доктор технічних наук, професор, Університет Умеа (Швеція);
Хлапонін Ю.І.	доктор технічних наук, професор, КНУБА;
Шаронова Н.В.	доктор технічних наук, професор, НТУ ХПІ.

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень і побажань.

Зареєстровано Міністерством юстиції України, свідоцтво про державну реєстрацію друкованого засобу масової інформації – серія КВ № 11541 – 413Р від 21.07.2006 р.

Відповідно до наказу МОН України від 24.09.2020 № 1188 "Збірник наукових праць ВІКНУ імені Тараса Шевченка" внесено до категорії "Б" (технічні науки).

Затверджено на засіданні Вченої ради ВІКНУ від 18.12.25 р., протокол № 5.

Відповідальна за макет:
Петренко М.М.

Відповідальність за новизну і достовірність наведених результатів, тактико-технічних та економічних показників і коректність висловлювань несуть автори. Точка зору редколегії не завжди збігається з позицією авторів. Усі матеріали надруковані в авторській редакції.

Усі статті, що публікуються в збірнику, проходять обов'язкове рецензування, яке здійснюється за анонімною формою як для авторів, так і для рецензентів. Незважаючи на перевірку статей на антиплагіат, остаточну відповідальність за плагіат несуть автори.

Видання безкоштовне.

Примірники збірників знаходяться у: Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, бібліотеці Військового інституту та в наукових бібліотеках України згідно зі списком МОН. Електронна версія збірника розміщена на відповідних сайтах.

Видання індексується Google Scholar.

Адреса редакції: 03189, м. Київ, вул. Ю. Здановської, 81, тел./факс +38 (044) 521 – 33 – 82
Наклад 50 прим. Ел. адреса редактора: lenkov_s@ukr.net
Офіційний сайт журналу: <http://miljournals.knu.ua>

UDC 621.43
LBC 32-26.8-68.49
Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv. K.: VIKNU, 2025. № 89. 95p.

Chairman of the editorial board:

Lienkov S.V. doctor of technical sciences, professor, VIKNU;

Members of the editorial board:

Anisimov A.V. doctor of physics and mathematics, professor, corresponding member of. NASU, KNU;
Barabash O.V. doctor of technical sciences, professor, NTUU KPI;
Gunchenko doctor of technical sciences, professor, ONU;
Zhyrov G.B. candidate of technical sciences, senior researcher, KNU;
Zaslavsky V.A. doctor of technical sciences, professor, KNU;
Karpinski M.P. doctor of technical sciences, professor, UNT, Krakow (Poland)
Lepikh Ya.I. doctor of physics and mathematics, professor, ONU;
Petrov O.S. doctor of technical sciences, professor, UNT, Krakow (Poland);
Pogorilyy S.D. doctor of technical sciences, professor, KNU;
Tolok I.V. candidate of pedagogical sciences, docent, NUCP
Khairova N.F. doctor of technical sciences, professor, Umea University (Sweden);
Khlaponin Yu.I. doctor of technical sciences, professor, KNUBA;
Sharonova N.V. doctor of technical sciences, professor, NTU KhPI.

The editorial board strives to improve the content and quality of the publication and will be grateful to the authors and readers for their comments and wishes.

Registered by the Ministry of Justice of Ukraine, certificate of state registration of printed mass media – KV series No. 11541 – 413P from 07/21/2006.

In accordance with the Order of the Ministry of Education and Science of Ukraine from September 24, 2020 No. 1188, "Collection of Scientific Works of the Military Institute of Taras Shevchenko National University of Kyiv" is included in category "B" (technical sciences).

Approved at the meeting of the Scientific Council of VIKNU from 18.12.2025, prot. №5

Responsible for the layout:
Petrenko M.

The authors are responsible for the novelty and reliability of the given results, tactical-technical and economic indicators and the correctness of statements. The point of view of the editorial board does not always coincide with the position of the authors. All the materials are printed in the author's edition.

All articles published in the collection undergo a mandatory review, which is carried out anonymously for both authors and reviewers. Despite checking the articles for anti-plagiarism, the final responsibility for plagiarism lies with the authors.

The publication is free.

Copies of the collections are in the National Library of Ukraine named after V.I. Vernadsky, in the scientific library named after M. Maksymovych, in the library of the Military Institute and in the scientific libraries of Ukraine according to the list of the Ministry of Education and Science. The electronic version of the collection is posted on the relevant websites.

The publication is indexed by Google Scholar.

Address of the editorial office: 03189, Kyiv, str. Y. Zdanovska, 81, phone/fax +38 (044) 521 – 33 – 82 Edition of 50 copies. E-mail address of the editor: lenkov_s@ukr.net
Official website of the journal: <http://miljournals.knu.ua>

ЗМІСТ

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Пампуха І.В., Яцук П.П., Тищук С.О., Савков П.А., Поздняк В.П. Електромагнітний простір у сфері оборони	7
Лоза В.М., Мірошніченко О.В., Іценко Д.С. Застосування методу просторової фільтрації з використанням сукупності матричних фільтрів-проекторів для визначення складу групової цілі у межах одного імпульсного об'єму радіолокаційної станції	18

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Машков О.А. Застосування інформаційних аерокосмічних технологій для підтримки прийняття управлінських рішень з використанням штучного інтелекту в системі контролю над звичайними озброєннями в Європі	26
Коренець О.В., Лукіяничук А.А. Удосконалення технології створення карт змін місцевості за допомогою програмного забезпечення ArcGIS	37
Коваль М.О., Кравченко О.І., Карпенко А.О., Шамрай Н.М. Аналіз вразливостей та кібератак на інформаційні ресурси, що обробляються в інформаційних системах	47

ЗАГАЛЬНІ ПИТАННЯ

Богданович В.Ю., Цибізов А.Л., Гуляк О.В. Спрощена методика обґрунтування рекомендацій щодо коригування політики національної безпеки держави за результатами стратегічного аналізу геополітичної та військової могутності недружніх держав	58
Гурковський В.І. ОБСЄ як інституційний механізм формування довіри, військової транспарентності, контролю над озброєннями та запобігання конфліктам у Європі	64
Ситник Г.П. Діалектична взаємозумовленість феноменів "безпека" та "небезпека" у контексті взаємодії системи різної природи	74
Зубчик О.А., Линченко М.М. Інституційна інерція та стійкість політичної системи України в умовах війни: аналіз через призму path dependence	90
Дейнека О.В. Середовищно-центрична парадигма управління безпекою: Концептуальна засада розвитку контрдронних систем	104
Зайцев Д.В., Мельник Я.І., Миколайчук О.М. Елементи програмно-проектного менеджменту як основа оборонного планування та оцінювання ефективності організаційних структур підрозділів	115

Дані про авторів	122
Алфавітний покажчик	124
Редакційна політика та етичні норми	125
Якісні показники членів редакційної колегії.	127
Порядок подання і оформлення статей до "Збірника наукових праць Військового інституту Київського національного університету імені Тараса Шевченка"	127

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

Pampukha I., Yatsuk P., Tyshchuk S., Savkov P., Pozdniak V. Electromagnetic space in the sphere of defense	7
Loza V., Miroshnichenko O., Itsenko D. Application of the spatial filtering method using a set of matrix filters -projectors to determine the composition of a group target within a single pulse volume of a radar station	18

INFORMATION TECHNOLOGIES

Mashkov O. Application of aerospace information technologies in the system of supporting management decisions using artificial intelligence in the system of control of conventional	26
Korenets O., Lukianchuk A. Improvement of the technology for creating terrain change maps using ArcGIS software	37
Koval M., Kravchenko O., Karpenko A., Shamraii N. Analysis of vulnerabilities and cyberattacks on information resources processed within information systems	47

GENERAL QUESTIONS

Bohdanovych V., Tsybizov A., Huliak O. Simplified methodology for substantiating recommendations on adjusting the state's national security policy based on the results of strategic analysis of the geopolitical and military power of unfriendly states	58
Gurkovskiy V. Osce as an institutional mechanism for confidence-building, military transparency, arms control and conflict prevention in europe	64
Sytnyk H. Dialectical interdependence of the concepts 'security' and 'danger' in the context of interaction between systems of different natures	74
Zubchuk O., Lynchenko M. Institutional inertia and the resilience of ukraine's political system under wartime conditions: a path dependence perspective	90
Deineka O. An environment-centric paradigm of security governance: a conceptual basis for development of counter-drone systems	104
Zaitsev D., Melnyk Y., Mikolayichuk O. Elements of program and project management as a basis for defense planning and assessment of the efficiency of organizational structures of units	115

Data on Authors	122
Alphabetical Index	125
Editorial policy and ethical standard	127
The order of submission and registration of articles to the "Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv"	127

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

УДК: 355/359

к.т.н., доц. Пампуха І.В. (ВІКНУ)
к.т.н., доц. Яцук П.П. (МСУ)
к.т.н., доц. Тищук С.О. (НУОУ)
к.т.н., доц. Савков П.А. (КНУ)
Поздняк В. П. (ХНУПС)

DOI: <https://doi.org/10.17721/2519-481X/2025/89-01>

ЕЛЕКТРОМАГНІТНИЙ ПРОСТІР У СФЕРІ ОБОРОНИ

У статті розглянуто сутність електромагнітного простору та його зміст як нового виміру сучасної війни, що інтегрує усі інші бойові простори – сухопутний, морський, повітряний, космічний та кіберпростір. Проведено аналітичний огляд регламентованих визначень щодо електромагнітного простору, що дозволило виявити відсутність єдиного узгодженого підходу до його трактування. Здійснено упорядкування понятійно-термінологічної основи застосування електромагнітного простору для сил оборони у сучасних воєнних конфліктах, що є важливим для формування доктринальних положень та розробки нормативно-правових актів. Окрему увагу приділено місцю електромагнітного простору в умовах відсічі збройної агресії. Розглянуто основні характеристики електромагнітних хвиль та електромагнітних засобів, що стосуються сфери оборони. Показано, що ефективність застосування сил оборони залежить від здатності здійснювати електромагнітну боротьбу в електромагнітному просторі, та що ефективність застосування електромагнітної боротьби в електромагнітному просторі є одним із ключових чинників досягнення переваги над противником. Електромагнітну боротьбу в сучасних умовах відсічі збройної агресії розглянуто як цілісну систему взаємопов'язаних складових, що забезпечують комплексне застосування сил і засобів електромагнітної боротьби в електромагнітному просторі. Показано змістовну трансформацію ключових термінів "радіоелектронна боротьба" в "електромагнітну боротьбу" та вузького технічного розуміння "електромагнітний спектр" у багатовимірну категорію "електромагнітний простір". Окремо розглянуто можливе місце електромагнітного простору у законодавстві України, зокрема перспективи нормативно-правового врегулювання його застосування в інтересах оборони. Підкреслено, що упорядкування термінологічного апарату та встановлення правових норм щодо застосування електромагнітного простору створює основу для підвищення ефективності практичних дій сил оборони та забезпечення національної безпеки.

Ключові слова: електромагнітний простір, електромагнітний засіб, електромагнітна боротьба, електромагнітна розвідка, електромагнітний вплив, електромагнітний захист, управління електромагнітним спектром.

Вступ та постановка проблеми. Сучасні воєнні конфлікти дедалі більше характеризуються використанням електромагнітного простору (ЕМП), як поєднуючого усі інші простори протиборства [1]. ЕМП охоплює широкий спектр заходів, які визначають ефективність застосування засобів сил оборони [2]. Водночас у науковій та нормативно-правовій площині відсутнє єдине узгоджене розуміння термінів, яке б забезпечувало цілісне сприймання змісту ЕМП та його ролі у сфері оборони [3]. Це створює труднощі у формуванні доктринальних положень, розробці законодавчих актів та практичному застосуванні електромагнітних засобів у військовій діяльності [4, 6].

Аналіз останніх досліджень і публікацій. У сучасній науково-публіцистичній літературі дослідження електромагнітного простору у сфері оборони охоплюють два ключові напрями. Перший напрям зосереджений на висвітленні значущості ЕМП та складових електромагнітної боротьби, включно з електромагнітним впливом, розвідкою та захистом [5].

Другий напрям стосується розвитку питань управління електромагнітним спектром та електромагнітної сумісності, що є критично важливим для забезпечення ефективної взаємодії сил оборони [6, 7, 8]. Попри наявності окремих досліджень, упорядкування понятійно-термінологічного апарату залишається недостатньо розробленим, що актуалізує потребу у його науковому осмисленні та нормативному впорядкуванні [9].

Метою статті є: розгляд визначення сутності та змісту електромагнітного простору у сфері оборони, упорядкування його понятійно-термінологічної основи, окреслення можливого місця електромагнітного простору у законодавстві України в контексті забезпечення відсічі агресії.

Виклад основного матеріалу. Розуміння електромагнітного простору пройшло тривалий шлях розвитку: від теоретичної основи, закладеної Джеймсом Максвеллом (1861), та практичного підтвердження існування електромагнітних хвиль Генріхом Герцем (1888), до розробки ключових принципів і патентів на радіопередавачі Ніколою Теслою (1894), першої демонстрації радіозв'язку Олександром Поповим (1895) та комерціалізації радіо Гульєльмо Марконі (1897).

Подальший розвиток привів до формування стратегій планування об'єднаних операцій і командування та управління (Command and Control, C2) на стратегічному, оперативно-стратегічному та тактичному рівнях у всіх бойових просторах через електромагнітний простір (рис. 1). Зокрема це реалізується через концепцію Joint All-Domain Command and Control (JADC2) [10].



Рисунок 1 – Об'єднане командування та управління у сухопутному, морському, повітряному, космічному та кіберпросторах через електромагнітний простір

У цьому розвитку можна виділити два основних напрямки трансформації: лінійної шкали радіочастот у всеохоплюючий електромагнітний простір, радіоелектронної боротьби, з основним завданням створення перешкод засобам управління військами та зброєю противника, у електромагнітну боротьбу, з основним завданням досягнення переваги над противником в електромагнітному просторі [11].

Перший напрямок розвивається на основі стратегічно-доктринальних документів [10, 11].

Другий напрямок розвивається на основі бойових статутів і настанов [12, 13] та набутого досвіду дій військових сил та засобів.

Задля прискорення впровадження сучасних підходів до застосування електромагнітного простору в інтересах оборони, доцільно розглянути такі питання:

- сутність та зміст електромагнітного простору,
- аналітичний огляд регламентованих визначень щодо електромагнітного простору.

Сутність електромагнітного простору. Електромагнітний простір у фізичному розумінні – це всеосяжна широчінь (обшир, просторінь), у якій електромагнітні хвилі поширюються без застосування штучних хвилеводів, в різних фізичних субстанціях (грунт, вода, гази, космічний вакуум), які водночас є просторами ведення бойових дій та здійснення діяльності людини [10, 11, 20]. Особливості використання електромагнітного спектра в кожному з цих середовищ визначаються його фізичними властивостями та технічними обмеженнями (табл. 1) [5, 9, 19].

Таблиця 1 - Застосування електромагнітних хвиль у бойових просторах

Простір	Застосування електромагнітних хвиль		У смузі частот
	Поширення	Обсяги (глибина, відстань)	
Сухопутний	на поверхні	увесь простір	$0-10^{24}$ Гц
	у товщі ґрунту	до 100 м	10–100 кГц
Водний	на поверхні	увесь простір	$0-10^{24}$ Гц
	у товщі морської / прісної води	сотні / тисячі м	10-300 Гц
		до 200 м	430-770 ТГц (видиме світло)
Повітряний	по всьому простору	увесь простір	$0-10^{24}$ Гц
Космічний	у межах місцезнаходження штучних супутників Землі	близько 36 тис. км	$0-10^{24}$ Гц
	у межах місцезнаходження штучних дослідницьких зондів	десятки млрд. км	2-8 ГГц
	у межах місцезнаходження природних космічних об'єктів	близько 46 млрд. світлових років (межа спостереження Всесвіту)	$0-10^{24}$ Гц
Кібер	у межах безпроводових ліній, мереж електронних комунікацій	безпроводова частина кіберпростору	$0-10^{17}$ Гц

З точки зору питань оборони, електромагнітний простір – це бойовий простір, який є частиною традиційних бойових просторів – сухопутного, морського, повітряного, космічного, а також порівняно нового – кіберпростору, в яких різноманітні електромагнітні засоби застосовуються для виконання завдань щодо оборони [4, 12, 13, 14]. Водночас електромагнітний простір є єдиним у всіх бойових просторах, він не має умовних військових меж (наприклад, ліній розмежування районів проведення військових операцій) [3, 8, 15]. Таким чином, ЕМП виконує роль об'єднуючого простору, у якому електромагнітні засоби різних видів, родів військ взаємодіють при виконанні завдань оборони [1, 6, 18]. Іншими словами ЕМП є узагальнюючим простором, який поєднує всі бойові простори щодо діяльності із застосуванням електромагнітних хвиль.

Підсумкова сутність ЕМП. Електромагнітний простір – це частина космічного, повітряного, сухопутного, водного (підводного) та кібер просторів, у якій електромагнітні хвилі поширюються без штучного хвилеводу [7, 11, 16, 21].

Зміст електромагнітного простору визначається сукупністю об'єктів, що перебувають у ньому, та їх діяльністю [5, 6, 9, 17]. До об'єктів електромагнітного простору відносяться зокрема електромагнітні хвилі, електромагнітні засоби, природні джерела електромагнітної енергії, об'єкти, на які впливає електромагнітне випромінювання тощо [2, 4, 19]. Діяльність в електромагнітному просторі (електронна комунікація, навігація, локація, електромагнітна боротьба тощо) здійснюється шляхом випромінювання та/або приймання електромагнітних хвиль електромагнітними засобами, поглинання та/або відбиття електромагнітних хвиль цілями або сторонніми об'єктами. [12, 13, 14, 18]. Взаємодія електромагнітних хвиль та живих істот зокрема людини не є предметом цієї статті, за винятком впливу електромагнітного випромінювання на стан особового складу.

Розглянемо основні характеристики електромагнітних хвиль та електромагнітних засобів, що стосуються сфери оборони.

Основні характеристики електромагнітних хвиль:

- смуга частот – визначає місце хвилі на шкалі електромагнітного спектру в просторі та часі [6, 11, 20],
- щільність потоку енергії – визначає рівень енергії електромагнітної хвилі в просторі та часі [5, 18],
- тип модуляції – визначає спосіб зміни параметрів хвилі при передаванні інформації [8, 19].

Основні характеристики електромагнітних засобів:

- призначення – визначається завданнями, які виконує електромагнітний засіб [4, 14],
- місцезнаходження – визначає розташування електромагнітного засобу в просторі та часі [2, 6, 15].

Розглянемо основні види діяльності в електромагнітному просторі, що стосуються сфери оборони.

Основні види діяльності в електромагнітному просторі:

- електронна комунікація – передавання та/або приймання інформації у вигляді електромагнітних хвиль із застосуванням електромагнітних засобів [12, 18],
- електромагнітна боротьба – діяльність щодо досягнення перемоги над противником в електромагнітному просторі [13, 16, 21].

Основні складові електромагнітної боротьби:

- електромагнітна розвідка – збір, розгляд та обробка інформації про дії противника в електромагнітному просторі [4, 5, 15],
- електромагнітний вплив – дія, у тому числі фізичне знищення, щодо унеможливлення застосування за призначенням електронних та/або електромагнітних засобів, а також виконання службових обов'язків особовим складом противника [2, 6, 19],
- електромагнітний захист – захист електронних та/або електромагнітних засобів, особового складу від електромагнітного впливу противника [7, 14],
- управління та регулювання в сфері електромагнітного простору для цілей оборони – дії щодо застосування за призначенням сил та засобів електромагнітної боротьби і досягнення електромагнітної сумісності електромагнітних засобів (унеможливлення створення електромагнітних завад електромагнітним засобам) [8, 11, 17, 20].

Аналітичний огляд регламентованих визначень щодо електромагнітного простору. Вперше у США розуміння електромагнітного спектра як окремого простору було визнано у 2007 році [22]. Починаючи з 2020 року електромагнітний простір визначено одним із основних бойових просторів, що поєднує основні бойові простори (сухопутний, морський, повітряний, космічний, кібер) [10, 11, 12].

Водночас у міжнародних документах та нормативних актах країн-членів НАТО простежується більш консервативне розуміння (табл. 2) [7].

Таблиця 2 - Особливості використання електромагнітного простору (спектра)

Держава	Національне законодавство, яке регулює ЕМП (спектра)	Нормативне визначення поняття ЕМП (спектра)	Уповноважений державний регулятор у сфері управління використанням ЕМП (спектра)	Наявність ЕМП
США	Федеральний закон "Про телекомунікації", Федеральний закон "Про допомогу правоохоронним органам у сфері зв'язку"	Смуга усіх частот / видів електромагнітного випромінювання	Національна адміністрація з питань телекомунікацій та інформації (NTIA) Федеральна комісія з питань зв'язку (FCC)	+
Велика Британія	Закон "Про комунікації", Закон "Про бездротову телеграфію"	Повна і впорядкована сукупність електромагнітних хвиль відповідно до їх частоти або довжини хвилі	Офіс із комунікацій (Ofcom)	+
Іспанія	Закон "Про телекомунікації"	Розподіл енергії електромагнітного випромінювання, яке поширюється з меншою довжиною випромінювання (гамма-промені) до випромінювання з більшою довжиною хвилі (радіохвилі)	Комісія ринку телекомунікацій	+
Норвегія	Закон "Про електронні комунікації"	Усі типи електромагнітних хвиль, упорядкованих за довжиною хвилі та відповідною частотою	Міністерство транспорту та комунікацій, Телекомунікаційний концерн (TELENOR)	+
Туреччина	Закон "Про електронні комунікації"	Смуга частот електромагнітних хвиль від 9 кГц до 3 ТГц, які використовуються для електронних комунікацій	Управління з питань інформаційних технологій та зв'язку	+
Франція	Кодекс про поштові послуги та електронні комунікації	1) Окремий простір для ведення бойових дій 2) Нематеріальне оперативне поле, яке складається з фотонів, електронів і магнітних полів	Національне агентство з питань радіочастот (ANFR)	+

Для нашого часу актуальним щодо окремого бойового простору (domain/space/battlespace) є використання у закордонних джерелах сфери оборони двох термінів – "електромагнітний спектр" та "електромагнітний простір". Причому у терміні "електромагнітний спектр" слово "спектр" розуміється не лише як послідовна шкала частот (одновимірна модель), і не лише як ресурс (чотиривимірна модель: широта, довгота, висота/глибина, шкала частот), а як простір, тобто необмежена протяжність (великий обшир, просторінь) у багатьох вимірах – щонайменше сім основних: широта, довгота, висота/глибина, час, шкала частот, потужність, модуляція, у якому плануються та здійснюються військові операції [10, 11, 12, 13].

Змістовну трансформацію пройшли також терміни "радіоелектронна боротьба" (electronic warfare) [22] та "управління частотами" (frequency management) [23], які раніше розглядалися як два взаємодіючих, але окремих напрямки. Сучасний термін "electromagnetic warfare" поєднує складові традиційної РЕБ із напрямком управління спектром, складовою якої є управління частотами [10, 11, 12, 13].

Еволюція поняття "електромагнітний простір" демонструє поступовий перехід від вузького технічного розуміння спектра до багатовимірної категорії, що охоплює планування та ведення операцій (бойових дій). Таким чином, у США електромагнітний простір (спектр) має статус окремого бойового простору (domain), на відміну від міжнародного права та

документів НАТО, що потребує подальшої гармонізації для забезпечення єдиного підходу до питань управління, регулювання та користування електромагнітним простором у сфері оборони.

Упорядкування понятійно-термінологічної основи застосування електромагнітного простору. У багатовимірному бойовому електромагнітному просторі (спектрі) здійснюється планування та ведення операцій (бойових дій) електромагнітної боротьби. Водночас засоби зокрема електронних комунікацій активно застосовуються при плануванні та веденні операцій в інших бойових просторах, що зумовлює потребу гармонізації термінології.

З метою забезпечення уникнення термінологічних розбіжностей доцільно обґрунтувати та систематизувати низку понять, притаманних цій сфері оборони. На підставі адаптації міжнародних документів та їх критичного осмислення щодо вітчизняних умов, упорядковано терміни щодо електромагнітного простору (спектру) у сфері оборони.

Електромагнітний простір (спектр) (electromagnetic spectrum) – частина космічного, повітряного, сухопутного, водного (підводного) та кіберпросторів, у якій електромагнітні хвилі поширюються без штучного хвилеводу [24].

Електромагнітна (радіоелектронна) боротьба (electromagnetic warfare) – сукупність організаційно-технічних заходів, що проводяться з метою стримування та/або відсічі збройної агресії проти України у електромагнітному просторі [24].

Електромагнітна розвідка (electromagnetic support) – комплекс заходів щодо збору, обробки та зберігання інформації про іноземні джерела електромагнітного випромінювання із застосуванням сил, засобів та способів електромагнітної боротьби для забезпечення подальшого аналізу, оцінки та прийняття рішень.

Електромагнітний вплив (electromagnetic attack) – комплекс заходів щодо послаблення, знешкодження або знищення спроможностей та/або введення в оману агресора із застосуванням вогневого ураження, електромагнітного випромінювання, сил, засобів та способів електромагнітної боротьби.

Електромагнітний захист (electromagnetic protection) – комплекс заходів щодо забезпечення захисту власних (дружніх) електричних, електронних та електромагнітних засобів, матеріальних об'єктів та особового складу від електромагнітного впливу ворога, із застосуванням сил, засобів та способів електромагнітної боротьби.

Управління електромагнітним спектром (spectrum management) – комплекс заходів щодо збору, обробки та зберігання інформації про джерела електромагнітного випромінювання у межах державного кордону та в районах виконання бойових завдань, управління (в особливий період та в умовах надзвичайного або воєнного стану) та регулювання користування електромагнітним спектром (зокрема розподіл, виділення, присвоєння смуг частот, державний нагляд, радіочастотний моніторинг, забезпечення електромагнітної сумісності та міжнародне співробітництво щодо електромагнітних засобів Збройних Сил України та інших спеціальних користувачів радіочастотного (електромагнітного) спектра) із застосуванням сил, засобів та способів електромагнітної боротьби.

Електромагнітна обстановка (electromagnetic environment) – це сукупність усіх електромагнітних випромінювань та їх джерел у певному районі електромагнітного простору протягом визначеного терміну.

Оперативна електромагнітна обстановка (operational electromagnetic environment) – електромагнітна обстановка у межах оперативної (операційної) зони, яка включає сукупність приймальних електромагнітних засобів та об'єктів впливу електромагнітної боротьби.

Операція в електромагнітному просторі (спектрі) (electromagnetic spectrum operation) – це взаємоузгоджене застосування сил, засобів та способів електромагнітної боротьби у ході проведення окремих або багатопросторових операцій для досягнення оперативних та/або стратегічних цілей.

Електромагнітний засіб (electromagnetic equipment/device/asset/mean) – технічний пристрій, що призначений для випромінювання та/або приймання електромагнітних хвиль [24].

Засіб електромагнітної боротьби (electromagnetic warfare device/system/equipment/asset/mean) – технічний пристрій, що застосовується для виконання завдань електромагнітної боротьби [24].

Упорядкування термінів здійснено з огляду на їх логічну та лінгвістичну узгодженість зокрема з урахуванням логіки натовських стандартів, але українськими словами, що забезпечить українським військовослужбовцям діяти звично і професійно, а Альянсу – бачити в Україні передбачуваного та зрозумілого партнера. Інакше кажучи зміст термінів чітко визначений, позбавлений двозначності, зрозумілий командирів і підлеглим, а при перекладі на англійську – ідентичний натівському за суттю.

Електромагнітний простір (спектр) в умовах відсічі збройної агресії. Електромагнітний простір є невід’ємною складовою сучасних операцій (бойових дій) в усіх бойових просторах, насичених електромагнітними засобами. В умовах відсічі збройної агресії ефективність застосування сил оборони залежить від здатності здійснювати електромагнітну боротьбу (ЕМБ) в електромагнітному просторі.

Електромагнітна боротьба в сучасних умовах відсічі збройної агресії розглядається як цілісна система взаємопов’язаних складових, що забезпечують комплексне застосування сил і засобів ЕМБ в електромагнітному просторі.

Електромагнітна розвідка виступає первинною ланкою системи, забезпечуючи командування інформацією про електромагнітні засоби ворога, їхні характеристики та вразливості. Вона створює інформаційний фундамент для планування та реалізації наступних заходів.

Електромагнітний вплив реалізує практичні дії щодо зниження або знищення спроможностей ворога.

Електромагнітний захист забезпечує стійкість та живучість власних електромагнітних засобів за умови електромагнітного впливу ворога.

Управління спектром формує організаційний порядок у користуванні частотами, що дозволяє уникати хаотичного застосування засобів, забезпечує електромагнітну сумісність, а також узгодженість дій із союзниками.

ЕМБ має стратегічний, оперативний і тактичний рівні застосування:

- на стратегічному рівні – державне управління та регулювання спектру, формування політики його користування та інтеграція із союзниками,

- на оперативному рівні – узгоджене застосування сил і засобів у межах угруповань, що забезпечує досягнення оперативних цілей,

- на тактичному рівні – безпосереднє застосування засобів ЕМБ на полі бою.

Сучасні бойові дії характеризуються багатовимірністю, де жоден простір не функціонує автономно. Операції у просторах завжди супроводжуються застосуванням електромагнітних засобів, що зумовлює необхідність узгодження з операціями в електромагнітному просторі. Поєднання операцій у просторах з операціями в електромагнітному просторі формує єдиний багатовимірний театр бойових дій, де перемога у спектрі стає значущим чинником успіху.

Розробка, виробництво, постачання та закупівля засобів електромагнітної боротьби мають здійснюватися не лише за критерієм технологічної новизни. Основним принципом має бути ціна – якість або вартість/витрати – ефективність (cost-benefit ratio), тобто співвідношення витрат до бойового результату в актуальних смугах частот протиборства. Такий підхід гарантує воєнно-економічну раціональність та оптимальне планування, дозволяє спрямовувати інвестиції на ті засоби, які реально забезпечують перемогу у спектрі.

Сумісність процедур управління та термінології відповідно до стандартів НАТО є умовою інтеграції України з союзниками та гарантує узгодженість дій у багатонаціональних операціях.

Таким чином, ЕМБ постає як багаторівнева та інтегрована система, де її ефективність визначається не лише якістю окремих складових, а й системною взаємодією між ними. Перемога в електромагнітному просторі шляхом здійснення ефективної ЕМБ значно посилює передумови досягнення стратегічних та оперативних цілей у багатовимірному бойовому просторі.

Нормативно-правове врегулювання застосування електромагнітного простору в інтересах оборони. З метою реалізації вимог статті 92 Конституції України щодо визначення виключно законами України засад використання природних ресурсів народним депутатом України О. Федієнко та іншими народними депутатами України було розроблено проєкт Закону України "Про внесення змін до деяких законів України щодо врегулювання окремих питань у сфері електромагнітного простору" (реєстраційний номер 13140 від 28.03.2025 до першого читання).

Ціллю прийняття законопроєкту є встановлення законних підстав у першу чергу щодо планування та ведення операцій, бойових дій в електромагнітному просторі силами оборони [24].

Проєктом Закону пропонується визначити основні засади використання електромагнітного простору (спектру), правовий статус та засади застосування у першу чергу силами оборони засобів електромагнітної (радіоелектронної) боротьби щодо електромагнітної розвідки, електромагнітної атаки (електромагнітних перешкод), електромагнітного захисту, управління спектром у тому числі при підготовці та веденні військових операцій в електромагнітному просторі (спектрі), зокрема Головним управлінням електромагнітної боротьби Генерального штабу Збройних Сил України [24].

Прийняття законопроєкту реєстраційний номер 13140:

- врегулює законодавчі питання забезпечення законних підстав застосування Збройними Силами України та іншими складовими сил оборони електромагнітних засобів, засобів електромагнітної боротьби в електромагнітному просторі (спектрі) для цілей безпеки та оборони України [24],

- забезпечить правову визначеність у сфері застосування електромагнітного простору для потреб оборони, закріпить компетенції відповідних органів та створить законні підстави зокрема для планування та ведення операцій,

- дозволить узгодити практику Збройних Сил України з вимогами Конституції та сучасними доктринальними підходами до ведення бойових дій в електромагнітному просторі, а також сприятиме гармонізації національного законодавства з нормативними та доктринальними стандартами НАТО.

Висновки. Визнання електромагнітного простору самостійним бойовим простором, який взаємо інтегрує сухопутний, морський, повітряний, космічний та кіберпростори, забезпечуючи комплексність при проведенні сучасних операцій передбачає упорядкування понятійно-термінологічного апарату застосування електромагнітного простору, що в свою чергу формує основу для вдосконалення нормативно-правової бази у сфері національної безпеки та оборони та підвищує ефективність практичних дій у сфері електромагнітної боротьби. Гармонізація українських термінів із міжнародними (зокрема країн-членів НАТО) стандартами усуває багатозначність і розбіжності у визначеннях, забезпечує зрозумілу та передбачувану систему для командирів, підлеглих і союзників, сприяє професійності Збройних Сил України та інтеграції у багатопросторові операції, утворюючи Україну як надійного партнера у сфері оборони. Здійснення ефективної ЕМБ в електромагнітному просторі значно посилює передумови досягнення стратегічних та оперативних цілей у багатовимірному бойовому просторі та забезпечує узгодженість дій України з країнами-членами НАТО. Прийняття законопроєкту реєстраційний номер 13140 у сфері нормативно-правового врегулювання застосування електромагнітного простору забезпечить формування чіткої правової основи для використання засобів електромагнітної боротьби силами оборони та сприятиме інтеграції України у систему багатопросторових операцій союзників.

ЛІТЕРАТУРА:

1. Бровінська М. Що таке електромагнітна зброя та чи загрожує вона Україні? dev.ua, 2025. – С. 2–4. URL: <https://dev.ua/news/shcho-take-elektromahnitna-zbroia-ta-chy-zahrozhuie-vona-ukraini-poiasniiuie-flesh-1759924407>.
2. Defense Express. Електромагнітна зброя: українські реалії. 2020. – С. 5–7. URL: https://defence-ua.com/weapon_and_tech/elektromagnitna_zbroja_ukrajinski_realii-612.html.

3. СОЮЗ "Золотий вік України". Електромагнітна зброя: від потенціалу до реалізації – ключ до підвищення обороноздатності України. 2024. – С. 10–12. URL: <https://zovu.org/elektromagnitnoye-oruzhiye-ot-potentsial/>.
4. Бибик Р., Опірський І. Електромагнітні загрози в сучасних конфліктах: аналіз характеристик джерел РЕБ та їх вплив на ефективність систем ураження. Кібербезпека: освіта, наука, техніка. 2025. – С. 748–755. DOI: 10.28925/2663-4023.2025.27.748.
5. Бибик Р., Наконечний Ю. Дослідження впливу електромагнітних перешкод на функціонування систем зв'язку та радіолокації. Вісник Львівської політехніки. 2024. – С. 1–9. DOI: 10.23939/csn2024.01.001.
6. Управління радіочастотним ресурсом: настанова. Київ: Центр учбової літератури, 2024. – С. 15–20. URL: <https://jurkniga.ua/contents/upravlinnya-radiochastotnim-resursom-nastanova.pdf>.
7. Дослідницька служба Верховної Ради України. Аналітична записка щодо застосування терміна "електромагнітний простір" у державах НАТО. 2025. – С. 3–6. URL: https://research.rada.gov.ua/documents/analyticRSmaterialsDocs/nscur_defense/analytical_notes-nb/76093.html.
8. Новіцький П., Степаняк М. Розвиток електромагнітної боротьби: інновації в домінуванні спектру, оборонних технологіях і захисних системах. Scientia. 2025. – С. 2379–2385. URL: <https://previous.scientia.report/index.php/archive/article/view/2379>.
9. Воробйов О., Мацько О., Тягай С. Перспективи використання електромагнітної зброї. Національний університет оборони України, 2024. – С. 12–18. URL: <http://sit.nuou.org.ua/article/download/37294/33466>.
10. United States Department of Defense. Summary of the Joint All-Domain Command & Control (JADC2) Strategy [Електронний ресурс]. Washington, D.C., March 2022. – С. 1–12. URL: <https://media.defense.gov/2022/Mar/17/2002953400/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF>.
11. United States Department of Defense. Electromagnetic Spectrum Superiority Strategy. Washington, D.C., 2020. – С. 1–18. URL: <https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/1/ELECTROMAGNETIC-SPECTRUM-SUPERIORITY-STRATEGY.PDF>.
12. Joint Chiefs of Staff, Department of Defense. Joint Publication JP 3-85: Joint Electromagnetic Spectrum Operations. Washington, D.C., 2020. – С. 1–112. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.
13. Department of the Army, United States Department of Defense. Field Manual FM 3-12: Cyberspace Operations and Electromagnetic Warfare. Washington, D.C., 2021. – С. 1–220. URL: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN31969-FM_3-12-000-WEB-3.pdf.
14. Ukrinform. Ukraine regulates drone and electronic warfare equipment purchases during martial law. 2024. – С. 1–3. URL: <https://www.ukrinform.net/rubric-ato/3940704-ukraine-regulates-drone-and-electronic-warfare-equipment-purchases-during-martial-law>
15. Wikipedia. Ukraine and electronic warfare. 2025. – С. 1–5. URL: https://en.wikipedia.org/wiki/Ukraine_and_electronic_warfare
16. Ministry of Defence of Ukraine. Electronic Warfare Coalition launched within Ramstein format. 2025. – С. 1–2. URL: <https://mod.gov.ua/en/news/a-newly-formed-electronic-warfare-coalition-has-been-launched-within-the-framework-of-the-ramstein-format>
17. New Geopolitics Research Network. War in the Spectrum. 2025. – С. 1–6. URL: <https://www.newgeopolitics.org/2025/07/23/war-in-the-spectrum/>
18. National Defense Magazine. Daily fight for Ukraine spectrum superiority puts electronic warfare front center. 2024. – С. 1–4. URL: <https://www.nationaldefensemagazine.org/articles/2024/3/8/daily-fight-for-ukraine-spectrum-superiority-puts-electronic-warfare-front-center>
19. Armada International. The role of the Electromagnetic Spectrum in Ukraine conflict. 2024. – С. 1–5. URL: <https://www.armadainternational.com/2024/11/the-role-of-the-electromagnetic-spectrum-in-russian-surveillance-offensive-and-defensive-operations-in-ukraine-electronic-warfare/>
20. NATO. Electromagnetic warfare. 2023. – С. 1–3. URL: <https://www.nato.int/en/what-we-do/deterrence-and-defence/electromagnetic-warfare>
21. RAND Corporation. NATO's blind spot in electromagnetic warfare could decide future conflicts. 2025. – С. 1–4. URL: <https://www.rand.org/pubs/commentary/2025/11/electromagnetic-warfare-natos-blind-spot-could-decide.html>

22. Joint Chiefs of Staff, Department of Defense. *Joint Publication 3-13.1: Electronic Warfare*. Washington, D.C., 2007. – C. 1–180. URL: https://irp.fas.org/doddir/dod/jp3_13_1.pdf
23. Joint Chiefs of Staff, Department of Defense. *Joint Publication 6-0: Joint Communications System*. Washington, D.C., 2015. – C. 1–260.
URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0.pdf
24. Верховна Рада України. Законопроект №13140 "Про внесення змін до деяких законодавчих актів України щодо електронних комунікацій". Київ, 2025. – С. 1–20.
URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/13140> (itd.rada.gov.ua in Bing)

REFERENCES:

1. Brovinska, M. (2025), "Shcho take elektromahnitna zbroia ta chy zahrozhuie vona Ukraini? " [What is electromagnetic weapon and does it threaten Ukraine?], dev.ua, pp. 2–4, dev.ua/news/shcho-take-elektromahnitna-zbroia-ta-chy-zahrozhuie-vona-ukraini-poiasniiuie-flesh-1759924407.
2. Defense Express (2020), "Elektromahnitna zbroia: ukrainski realii" [Electromagnetic weapon: Ukrainian realities], pp. 5–7, defence-ua.com/weapon_and_tech/elektromagnitna_zbroja_ukrajinski_realiji-612.html.
3. Soiuz "Zoloty vik Ukrainy" (2024), "Elektromahnitna zbroia: vid potentsialu do realizatsii – kliuch do pidvyshchennia oboronozdatnosti Ukrainy" [Electromagnetic weapon: from potential to implementation – the key to strengthening Ukraine's defense], pp. 10–12, zovu.org/elektromagnitnoye-oruzhiye-ot-potentsial/.
4. Bybyk, R. and Oprisky, I. (2025), "Elektromahnitni zahrozy v suchasnykh konfliktakh: analiz kharakterystyk dzherel REB ta yikh vplyv na efektyvnist system urazhennia" [Electromagnetic threats in modern conflicts: analysis of EW sources and their impact on effectiveness of strike systems], Cybersecurity: Education, Science, Technique, pp. 748–755, doi:10.28925/2663-4023.2025.27.748.
5. Bybyk, R. and Nakonechnyi, Yu. (2024), "Doslidzhennia vplyvu elektromahnitnykh pereshkod na funktsionuvannia system zviazku ta radiolokatsii" [Study of the influence of electromagnetic interference on communication and radar systems], Visnyk Lvivskoi Politekhniky, pp. 1–9, doi:10.23939/csn2024.01.001.
6. Tsentru uchbovoi literatury (2024), "Upravlinnia radiochastotnym resursom: nastanova" [Radio frequency resource management: manual], Kyiv, pp. 15–20, jurkniga.ua/contents/upravlinnya-radiochastotnim-resursom-nastanova.pdf.
7. Doslidnytska sluzhba Verkhovnoi Rady Ukrainy (2025), "Analichna zapyska shchodo zastosuvannia termina 'elektromahnitnyi prostir' u derzhavakh NATO" [Analytical note on the use of the term 'electromagnetic space' in NATO countries], pp. 3–6, research.rada.gov.ua/documents/analyticRSMaterialsDocs/nscur_defense/analytical_notes-nb/76093.html.
8. Novitskyi, P. and Stepaniak, M. (2025), "Rozvytok elektromahnitnoi borotby: innovatsii v dominuvanni spektru, oboronnykh tekhnolohiiakh i zachysnykh systemakh" [Development of electromagnetic warfare: innovations in spectrum dominance, defense technologies and protective systems], Scientia, pp. 2379–2385, previous.scientia.report/index.php/archive/article/view/2379.
9. Vorobiov, O., Matsko, O. and Tiahai, S. (2024), "Perspektyvy vykorystannia elektromahnitnoi zbroi" [Prospects of using electromagnetic weapons], National Defence University of Ukraine, pp. 12–18, sit.nuou.org.ua/article/download/37294/33466.
10. United States Department of Defense (2022), Summary of the Joint All-Domain Command & Control (JADC2) Strategy, Washington, D.C., pp. 1–12, media.defense.gov/2022/Mar/17/2002953400/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.
11. United States Department of Defense (2020), Electromagnetic Spectrum Superiority Strategy, Washington, D.C., pp. 1–18, media.defense.gov/2020/Oct/29/2002525927/-1/-1/1/ELECTROMAGNETIC-SPECTRUM-SUPERIORITY-STRATEGY.PDF.
12. Joint Chiefs of Staff, Department of Defense (2020), Joint Publication JP 3-85: Joint Electromagnetic Spectrum Operations, Washington, D.C., pp. 1–112, jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.
13. Department of the Army, United States Department of Defense (2021), Field Manual FM 3-12: Cyberspace Operations and Electromagnetic Warfare, Washington, D.C., pp. 1–220, armypubs.army.mil/epubs/DR_pubs/DR_a/ARN31969-FM_3-12-000-WEB-3.pdf.
14. Ukrinform (2024), "Ukraine regulates drone and electronic warfare equipment purchases during martial law", pp. 1–3, ukrinform.net/rubric-ato/3940704-ukraine-regulates-drone-and-electronic-warfare-equipment-purchases-during-martial-law.
15. Wikipedia (2025), "Ukraine and electronic warfare", pp. 1–5, en.wikipedia.org/wiki/Ukraine_and_electronic_warfare.

16. Ministry of Defence of Ukraine (2025), "Electronic Warfare Coalition launched within Ramstein format", pp. 1–2, mod.gov.ua/en/news/a-newly-formed-electronic-warfare-coalition-has-been-launched-within-the-framework-of-the-ramstein-format.
17. New Geopolitics Research Network (2025), "War in the Spectrum", pp. 1–6, newgeopolitics.org/2025/07/23/war-in-the-spectrum/.
18. National Defense Magazine (2024), "Daily fight for Ukraine spectrum superiority puts electronic warfare front center", pp. 1–4, nationaldefensemagazine.org/articles/2024/3/8/daily-fight-for-ukraine-spectrum-superiority-puts-electronic-warfare-front-center.
19. Armada International (2024), "The role of the Electromagnetic Spectrum in Ukraine conflict", pp. 1–5, armadainternational.com/2024/11/the-role-of-the-electromagnetic-spectrum-in-russian-surveillance-offensive-and-defensive-operations-in-ukraine-electronic-warfare/.
20. NATO (2023), "Electromagnetic warfare", pp. 1–3, nato.int/en/what-we-do/deterrence-and-defence/electromagnetic-warfare.
21. RAND Corporation (2025), "NATO's blind spot in electromagnetic warfare could decide future conflicts", pp. 1–4, rand.org/pubs/commentary/2025/11/electromagnetic-warfare-natos-blind-spot-could-decide.html.
22. Joint Chiefs of Staff, Department of Defense (2007), Joint Publication 3-13.1: Electronic Warfare, Washington, D.C., pp. 1–180, irp.fas.org/doddir/dod/jp3_13_1.pdf.
23. Joint Chiefs of Staff, Department of Defense (2015), Joint Publication 6-0: Joint Communications System, Washington, D.C., pp. 1–260, jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0.pdf.
24. Verkhovna Rada Ukrainy (2025), Draft Law No. 13140 "Pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo elektronnykh komunikatsii" [Draft Law No. 13140 "On amendments to certain legislative acts of Ukraine regarding electronic communications"], Kyiv, pp. 1–20, itd.rada.gov.ua/billInfo/Bills/Card/13140.

**Ph.D., A/Prof. Pampukha I., Ph.D., A/Prof. Yatsuk P.,
Ph.D., A/Prof. Tyshchuk S., Ph.D., A/Prof. Savkov P., Pozdniak V.**

ELECTROMAGNETIC SPACE IN THE SPHERE OF DEFENSE

The article examines the essence of the electromagnetic space and its significance as a new dimension of modern warfare, integrating all other combat domains – land, maritime, air, space, and cyberspace. An analytical review of normative definitions of electromagnetic space has been conducted, revealing the absence of a unified and consistent approach to its interpretation. The conceptual and terminological framework for the use of electromagnetic space by defense forces in contemporary military conflicts has been systematized, which is essential for the development of doctrinal provisions and regulatory acts. Particular attention is paid to the role of electromagnetic space in countering armed aggression. The main characteristics of electromagnetic waves and electromagnetic means relevant to defense are considered. It is demonstrated that the effectiveness of defense forces depends on their ability to conduct electromagnetic warfare within the electromagnetic space, and that the efficiency of such warfare is one of the key factors in achieving superiority over the adversary. Electromagnetic warfare under current conditions of repelling armed aggression is analyzed as an integrated system of interrelated components ensuring the comprehensive employment of forces and means in the electromagnetic space. The substantive transformation of key terms is highlighted: from "electronic warfare" to "electromagnetic warfare", and from the narrow technical understanding of "electromagnetic spectrum" to the multidimensional category of "electromagnetic space". The possible place of electromagnetic space in Ukrainian legislation is also discussed, particularly the prospects of its regulatory framework for defense purposes. It is emphasized that the systematization of terminology and establishment of legal norms for the use of electromagnetic space creates the foundation for enhancing the effectiveness of defense operations and ensuring national security.

Keywords: *electromagnetic space, electromagnetic mean, electromagnetic warfare, electromagnetic intelligence (support), electromagnetic attack, electromagnetic protection, electromagnetic spectrum management.*

ЗАСТОСУВАННЯ МЕТОДУ ПРОСТОРОВОЇ ФІЛЬТРАЦІЇ З ВИКОРИСТАННЯМ СУКУПНОСТІ МАТРИЧНИХ ФІЛЬТРІВ-ПРОЕКТОРІВ ДЛЯ ВИЗНАЧЕННЯ СКЛАДУ ГРУПОВОЇ ЦІЛІ У МЕЖАХ ОДНОГО ІМПУЛЬСНОГО ОБ'ЄМУ РАДІОЛОКАЦІЙНОЇ СТАНЦІЇ

У статті розглянуто одну з актуальних проблем сучасної радіолокації – визначення складу групових зосереджених цілей у межах імпульсного об'єму радіолокаційної станції (РЛС). Проаналізовано методи високого розрізнення, що перевищують релєйську межу, зокрема алгоритми альтернативного спектрального аналізу (MUSIC, Capon) та проекційні методи. Відзначено обмеження спектральних алгоритмів, що пов'язані з високою кореляцією сигналів від окремих цілей та значною обчислювальною складністю, що знижує їх практичну ефективність.

Запропоновано алгоритм просторової обробки сигналів на основі матричних фільтрів-проекторів (ФП), який дозволяє реалізувати процедуру квазіоптимального розрізнення без необхідності обчислення оберненої кореляційної матриці. Методологія побудована на положеннях функціонального аналізу та використанні критерію найменших квадратів, що забезпечує адаптивність алгоритму до умов невизначеності параметрів сигналів.

Розроблена структурна схема системи включає кілька фільтрів-проекторів, узгоджених із різними моделями групових цілей. Для випадку двох цілей у межах імпульсного об'єму застосовується пара ФП: один узгоджений з одиночним сигналом, інший – з парною ціллю. Рішення про кількість цілей приймається на основі порівняння вихідних сигналів цих каналів із заданим порогом, що дозволяє реалізувати процедуру, близьку за змістом до оптимального алгоритму розрізнення.

Ефективність методу підтверджено статистичними випробуваннями за методом Монте-Карло. Показано, що при відношенні сигнал/шум 16-20 дБ система високого розрізнення на основі двох узгоджених ФП забезпечує впевнене розрізнення групових цілей, удвічі перевищуючи релєйську межу.

Таким чином, стаття робить вагомий внесок у розвиток теорії та практики систем надвисокого розрізнення в радіолокації, пропонуючи технічно реалізований алгоритм, здатний працювати в умовах високої кореляції сигналів. Результати мають значне тактичне значення для задач виявлення та класифікації групових цілей у сучасних РЛС.

Ключові слова: *групова ціль, система високого розрізнення, імпульсний об'єм.*

Вступ та постановка проблеми. Зростання інтенсивності застосування засобів повітряного нападу, зокрема безпілотних літальних апаратів та високотехнологічних ракет, вимагає від радіолокаційних станцій (РЛС) Повітряних Сил Збройних Сил України здатності не лише виявляти групові цілі, але й визначати їхній чисельний склад. Визначення складу групових зосереджених цілей (ГЗЦ) є однією з проблемних завдань радіолокаційного забезпечення, вирішення якого дозволить визначити склад групової цілі в межах імпульсного об'єму РЛС, що підвищить точність та оперативність ідентифікації повітряних об'єктів у складних умовах сучасного бою.

Методологія вирішення задачі, що отримала назву "надвисока роздільна здатність", ґрунтується на фундаментальній роботі Monzingo R.A., Miller T.U. [1]. Розвитку ідей високої роздільної здатності в останній період присвячено велику кількість публікацій. Зокрема Schuessler C., Hoffmann M. та Vossiek M. запропонували використання глибинних нейронних мереж для вирішення завдання надрозрізнення повітряних цілей [2] що демонструє, як сучасні методи штучного інтелекту можуть доповнити класичні алгоритми просторової фільтрації, підвищуючи точність розрізнення. У роботі [3] Yang S. з колегами розглядають використання алгоритму MSL0 для підвищення кутового розрізнення реальної апертури радару, а Kim B.-S.,

Jin Y., Lee J., Kim S. досліджують використання комбінації методів FFT та MUSIC для зниження обчислювальних ресурсів при збереженні високого розрізнення [4].

Поряд з публікаціями останніх років у даній статті пропонується фундаментально обґрунтований та технічно реалізований алгоритм просторової обробки на основі матричних фільтрів-проекторів, що доповнює новітні підходи штучного інтелекту та оптимізаційні методи у сфері надвисокого розрізнення радіолокаційних систем.

Реалізація спектральних методів (алгоритми Capon, MUSIC та інші) обмежується у зв'язку з притаманними їм двома основними недоліками [5]:

- по-перше, можливість високої роздільної здатності лише за умови незалежності сигналів, відбитих від поодиноких цілей (для ГЗЦ такі сигнали мають високий ступінь кореляції);

- по-друге, велика складність обчислювальних процедур (обчислення оберненої кореляційної матриці, її власних значень).

Найбільш близькими прототипами за змістом задачі, що вирішується, є роботи [6] та [7]. У першій з них запропоновано алгоритм розрізнення сигналів, відбитих від цілі та перевідбитих поверхнею Землі, у другій – запропоновано алгоритм високої роздільної здатності, який орієнтований на застосування в РЛС загоризонтного типу (що відрізняються видом сигналу та діапазоном хвиль). В обох роботах використовуються фільтри-проектори.

Метою статті є теоретичне обґрунтування та практична реалізація алгоритму просторової обробки сигналів у РЛС, який дозволяє визначати склад ГЗЦ у межах імпульсного об'єму незалежно від ступеня кореляції сигналів, забезпечуючи надвисоке розрізнення понад релєйську межу.

Виклад основного матеріалу. Основи статистичної теорії розпізнавання були розроблені та опубліковані наприкінці 60-х років, засновником якої є Ширман Я.Д. [8].

Задача оптимального розпізнавання двох сигналів формулюється як прийняття рішення про наявність кожного з сигналів окремо за наявності іншого заважаючого сигналу, еквівалентного перешкоді.

Критична статистика розпізнавання полягає у обчисленні кореляційного інтеграла, в якому замість опорного сигналу (що є копією очікуваного) використовується вирішальна функція, яка виконує завдання придушення заважаючого сигналу в області перекриття. Ступінь придушення залежить від коефіцієнта кореляції сигналу, що виявляється в даний момент, із заважаючим.

$$z = y^H w, \quad (1)$$

де z – значення кореляційного інтеграла (КІ);

$y = x + v$ – вектор вхідного процесу (x – корисний сигнал, v – шум);

H – знак ермітового спряження;

w – вирішальна функція КІ, що визначається виразом:

$$w = x_1 - k \cdot x_2, \quad (2)$$

де $k = 1 - \rho \frac{q_2}{q_2 + 1}$ – коефіцієнт використання енергії виявленого сигналу;

$x = x_1 + x_2 \cdot q_2$ – відношення сигнал/шум: $c/u = \frac{\mathcal{E}}{N_0}$ (індекс опускається, оскільки для

розглянутої моделі ГЗЦ сигнали мають однакову амплітуду).

Приклад вигляду вирішальної функції при розрізненні нормованих до одиниці сигналів прямокутної форми при довільній координаті α з коефіцієнтом перекриття 0,5, показано на рис. 1.

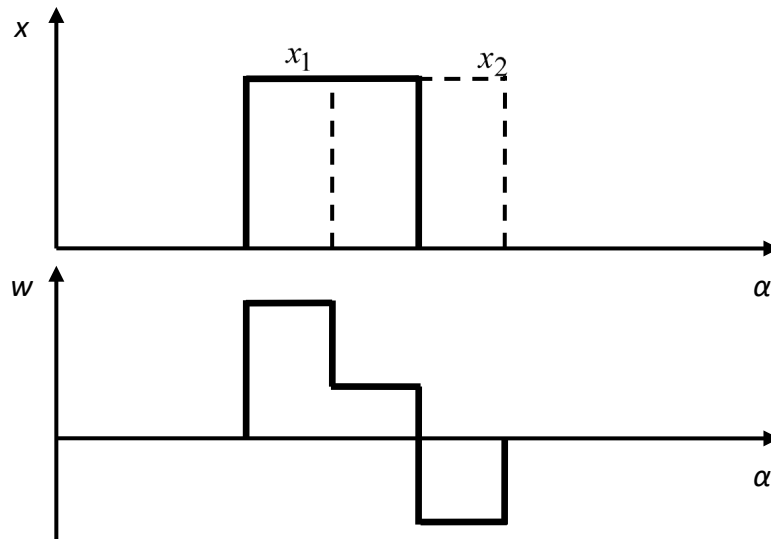


Рисунок 1 – Приклад вигляду вирішальної функції при розрізненні нормованих до одиниці сигналів прямокутної форми

Алгоритм оптимального розрізнення практично не застосовується через апіорі невідомий ступінь перекриття сигналів, хоча його реалізація можлива завдяки багатоканальності побудови системи обробки. Тому не можна повністю погодитися з висновком про непрацездатність алгоритму оптимального розрізнення, який зустрічається в окремих публікаціях.

Значно складніше реалізувати оптимальний або близький до нього за принципом обробки алгоритм розрізнення цілей за просторовими координатами, коли формування вирішальної функції має здійснюватися антенною системою або застосуванням антенної решітки (АР) з просторовими фільтрами. У той же час принцип просторового розрізнення може бути реалізований на деякій лінійній апертурі антени. Залежно від розподілу випромінювачів на апертурі створюється певний розподіл поля. На це поле накладається поле шумів теплового випромінювання, яке можна вважати ізотропним. Інформація про наявність одного з випромінювачів у присутності заважаючого, може бути отримана шляхом аналізу напруженості поля як функції двох змінних: часу та координати, що виконується додатковим інтегруванням по апертурі за допомогою багатoelementної антени типу цифрової антенної решітки (ЦЛАР) та просторовими фільтрами. Проведений аналіз показує, що задача просторового розрізнення, процедура якої наближена до алгоритму оптимального розрізнення, є цілком перспективною для розробки систем визначення складу групової парної цілі.

Для вирішення поставленої у статті мети необхідно вирішити наступні завдання:

- розробка методу квазіоптимальної просторової обробки сигналів на основі матричних фільтрів, що забезпечує обробку в реальному масштабі часу;
- розробка методу визначення кількості цілей з різними азимутами в межах імпульсного об'єму РЛС та його технічна реалізація.

При вирішенні першого завдання використовується метод синтезу детектора на основі застосування методології та положень теорії функціонального аналізу, вперше запропонований у [6].

Як критерій оптимізації обирається критерій найменших квадратів [8]. Використання даного критерію, з одного боку, не вимагає знання повних характеристик вектора (що визначає вихідні сигнали каналів прийому), з іншого боку, дозволяє застосовувати теореми та положення функціонального аналізу для спрощення задачі. У термінах функціонального аналізу задача синтезу алгоритму "виявлення – розрізнення" може бути сформульована наступним чином [6].

Існує набір базисних функцій (векторів) $V = [v_i, i = 1 \dots M]$, які належать підпростору H Гільбертового простору L^2 , і на цьому базисі необхідно сформувати вектор $U_c^\wedge$, який задовольняє умові:

$$\varepsilon = (U - U_c^\wedge)^H (U - U_c^\wedge) = \min. \quad (3)$$

З'являється можливість подання:

$$U_c^\wedge = V \cdot u_1^\wedge, \quad (4)$$

де $u_1^\wedge$ – оціночний вектор-стовпець сигналу цілі на виході першого приймального каналу. Виконуючи операцію векторного диференціювання за $u_1^\wedge$, отримаємо:

$$\frac{d\varepsilon(u_1^\wedge)}{du_1^\wedge} = V^H (U - V u_1^\wedge) = 0; \quad u_1^\wedge = V^{-1} U.$$

Розв'язуючи відносно $U_c^\wedge$, отримаємо рівняння:

$$U_c^\wedge = V(V^H V)^{-1} V^H U. \quad (5)$$

У правій частині рівності (5), використовуючи теорему проектування функціонального аналізу, виділимо вираз, що відповідає фільтру-проектору, який позначимо $Pr_M^\wedge$ і називатимемо матричним фільтром-проектором (ФП):

$$Pr_M = V(V^H V)^{-1} V^H, \quad (6)$$

де M – кількість джерел сигналів. За термінологією функціонального аналізу: проектор (6) натягнутий на стовпці матриці V .

З урахуванням (5) і (6) маємо рівність:

$$U_c^\wedge = Pr_M U. \quad (7)$$

Після фільтрації матричним ФП алгоритм передбачає обчислення норми результату і подальше порівняння з порогом. Якщо позначити вихідний сигнал системи виявлення за наявності на вході сигналів від M джерел через w_M , то алгоритм виявлення має вигляд:

$$w_M = U^H Pr_M U \geq w_0, \quad (8)$$

де w_0 – поріг виявлення (при заданому M).

Формула алгоритму випливає з однієї з властивостей проекторів: квадрат норми проекції будь-якого вектора на підпростір, утворений проектором, дорівнює квадратичній формі виду:

$$\|Pr_M U\|^2 = U^H Pr_M U.$$

За наявності в імпульсному об'ємі двох цілей N -мірний вектор-стовпець вихідних сигналів ЦЛАР має вираз:

$$U = U_{c1} + U_{c2} + U_{in}; \quad U_{c1} = v_1 s_1; \quad U_{c2} = v_2 s_2.$$

де v_1, v_2 , – вектор-стовпці, що характеризують амплітудно-фазовий розподіл на входах приймальних елементів ЦЛАР:

$$v_1^H = [1e^{-j\varphi_1} e^{-2j\varphi_1} \dots e^{-j(N-1)\varphi_1}], \quad v_2^H = [1e^{-j\varphi_2} e^{-j2\varphi_2} \dots e^{-j(N-1)\varphi_2}], \quad \varphi_{1,2} = \pi \sin \beta_{1,2};$$

s_1 та s_2 – сигнали цілей в опорному каналі.

Фільтр-проектор являє собою матричний фільтр із передавальною характеристикою $Pr_n = V \cdot (V^H V)^{-1} \cdot V^H$, де V – матриця розміром $N \times n$ (n – кількість стовпців матриці V , у нашому випадку дорівнює M). Розмірність ФП визначається кількістю стовпців V , тобто для основних моделей ГЗЦ відповідає $M = 2 \dots 3$. ФП називають узгодженим, якщо розмірність проектора n збігається з числом цілей M в імпульсному об'ємі РЛС ($n = M$).

Проектор з урахуванням кількості розрізняваних сигналів повинен здійснювати переналаштування своїх параметрів. Переналаштування необхідне для знаходження тих значень параметрів, при яких максимізується квадрат норми проекції вихідного сигналу ЦЛАР на підпростір, натягнутий на стовпці матриці V проектора, тобто досягається умова:

$$\alpha^* = \arg \max(U_i^H \cdot V \cdot (V^H V)^{-1} V^H U_i), \quad (9)$$

де α^* – вектор оцінок параметра.

Перевагою отриманого алгоритму порівняно з відомими алгоритмами високої роздільної здатності є усунення необхідності обчислення зворотної кореляційної матриці вихідних сигналів ЦЛАР і, отже, зняття обмежень, пов'язаних з її оцінкою.

Розв'язання другого завдання. При невідомих потужностях сигналів, відбитих від цілей, достовірний склад групової цілі в імпульсному об'ємі РЛС може бути встановлений тільки при включенні в систему обробки декількох ФП, число яких залежить від реального складу ГЗЦ. У разі розрізнення двох цілей у системі обробки має бути два ФП. З них: один ФП має бути "узгоджений" з одиночною ціллю (проектор позначимо Pr_1), інший "узгоджений" з груповою ціллю, що включає два повітряних об'єкти (проектор позначимо – Pr_2). За наявності цих двох фільтрів-проекторів рішення про кількість цілей в імпульсному об'ємі РЛС приймається за результатами різниці вихідних сигналів двох каналів обробки. Рішення про наявність двох цілей у складі ГЗЦ приймається тоді, коли виконується умова:

$$\Delta w = w_1 - w_2 \geq w_p, \quad (10)$$

де w_p – поріг рішення, який обирається з умовою забезпечення заданої ймовірності прийняття неправильних рішень щодо кількості цілей у групі (зазвичай приймає значення 10^{-4}).

В основу алгоритму визначення кількості цілей у ГЗЦ береться така властивість проекторів:

$$Pr_M - Pr_{M-1} = Pr_M(I_{N \times N} - Pr_{M-1}) = Pr_M \cdot Pr_{\perp(M-1)}, \quad (11)$$

де $Pr_{\perp}$ – ортогональний проектор, що формує підпростір, який є ортогональним до підпростору, що формується Pr_{M-1} .

Алгоритмічна структурна схема підсистеми визначення кількості цілей в імпульсному об'ємі РЛС представлена на рис.2.

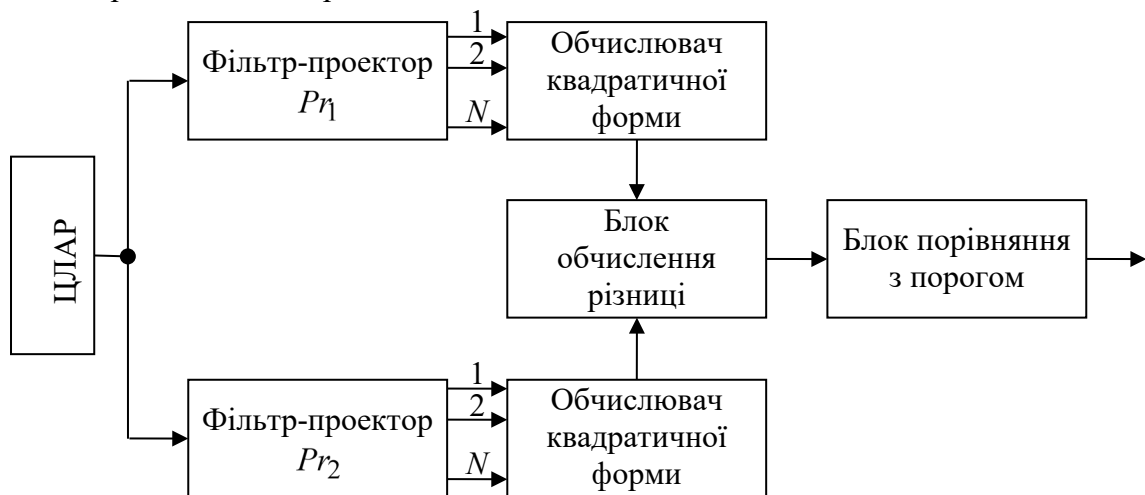


Рисунок 2 – Алгоритмічна структурна схема підсистеми визначення кількості цілей в імпульсному об'ємі РЛС

Позначення характеристик ФП на рис. 2 відповідають: $Pr_1 \Rightarrow Pr_{M_0}$, $Pr_2 \Rightarrow Pr_{M_0-1}$.

Фізичне тлумачення процедури розрізнення ілюструється при підстановці в рівняння (10) значень вихідних сигналів, виражених через характеристики проекторів, та перетворенні отриманого виразу. Після підстановки w_1 та w_2 у (10) отримаємо:

$$\Delta w = U^H (Pr_2 - Pr_1) U > w_p. \quad (12)$$

Підпростір, утворений проектором Pr_1 , належить до підпростору, що утворений Pr_2 , тому має місце співвідношення:

$$Pr_1 Pr_2 = Pr_2 Pr_1 = Pr_1, \quad (13)$$

з урахуванням чого співвідношення (12) можна представити у вигляді:

$$\Delta w = U^H Pr_2 \cdot Pr_{\perp 1} U > w_p, \quad (14)$$

де $Pr_{\perp 1} = (I - Pr_1)$ – ортогональний проектор для сигналу першої цілі.

Отримане рівняння прийняття рішення щодо розрізнення двох цілей означає, що в блоці обчислення різниці на рис. 2 здійснюється режекція сигналу однієї з цілей і забезпечується виявлення другої. Така процедура обробки сигналів при розрізненні цілком відповідає за змістом алгоритму оптимального розрізнення цілей (порівняння (2) з (12)).

Оцінка ймовірності розрізнення групової цілі, що складається з двох одиночних в імпульсному об'ємі РЛС, виконана методом статистичних випробувань Монте-Карло представлена на графіку рис. 3. Кутовий рознос цілей по азимуту становив 0,5 ширини діаграми спрямованості антени.

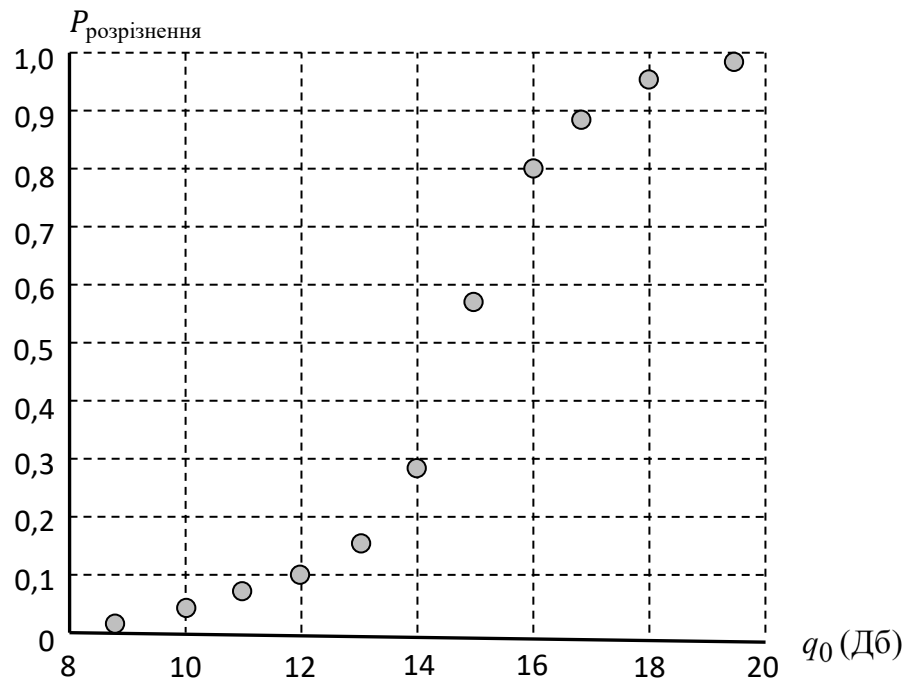


Рисунок 3 – Оцінка ймовірності розрізнення групової зосередженої цілі

Таким чином, за умови забезпечення співвідношення сигнал/шум 16–20 дБ система високої роздільної здатності на основі двох ФП, узгоджених з різними цілями, забезпечує роздільну здатність ($P_{\text{розрізнення}} > 0,8$), яка удвічі краща за релеївську.

Висновки. У результаті проведеного дослідження було науково обґрунтовано та практично реалізовано алгоритм просторової обробки сигналів, що базується на застосуванні сукупності матричних фільтрів-проекторів для ідентифікації складу ГЗЦ у межах одного імпульсного об'єму РЛС. Запропонований підхід, на відміну від класичних спектральних методів типу MUSIC або Capon, демонструє високу ефективність в умовах значної кореляції сигналів, що є характерним для щільних бойових порядків засобів повітряного нападу. Використання методології функціонального аналізу та критерію найменших квадратів дозволило мінімізувати обчислювальну складність шляхом усунення необхідності обчислення оберненої кореляційної матриці, що забезпечує можливість обробки даних у реальному масштабі часу. Результати статистичного моделювання підтвердили, що розроблена система квазіоптимального розрізнення при відношенні сигнал/шум 16-20 дБ дозволяє досягти роздільної здатності, яка вдвічі перевищує релеївську межу з ймовірністю понад 0,8.

Напрямки подальших досліджень у даній галузі доцільно зосередити на розширенні можливостей алгоритму для ідентифікації складніших конфігурацій цілей, що включають три та більше об'єктів у межах одного імпульсного об'єму РЛС. Також перспективним є поєднання методів матричної фільтрації з технологіями глибинних нейронних мереж та штучного інтелекту, що дозволить підвищити адаптивність систем до динамічних змін сигнального середовища.

ЛІТЕРАТУРА:

1. Robert A. Monzingo; Randy L. Haupt; Thomas W. Miller "Introduction to Adaptive Arrays" (2nd Edition), 2011. – 543 p. DOI: <https://doi.org/10.1049/SBEW046E>
2. C. Schuessler, M. Hoffmann, and M. Vossiek, "Super-Resolution Radar Imaging with Sparse Arrays Using a Deep Neural Network", *IEEE Journal of Microwaves*, vol. 3, no. 1, pp. 45–56, 2023. DOI: <https://arxiv.org/pdf/2306.09839>
3. S. Yang, Y. Zhao, X. Tuo, et al., "Real Aperture Radar Angular Super-Resolution Imaging Using Modified Smoothed L0 Norm", *Remote Sensing*, vol. 16, no. 2, pp. 312, 2024. <https://doi.org/10.3390/rs16010012>
4. B.-S. Kim, Y. Jin, J. Lee, and S. Kim, "FMCW Radar Estimation Algorithm with High Resolution and Low Complexity Based on Reduced Search Area," *Sensors*, vol. 22, no. 3, pp. 1456, 2022. <https://doi.org/10.3390/s22031202>
5. Raymond J. Weber; Yikun Huang "Analysis for Capon and MUSIC DOA estimation algorithms" 2009 IEEE Antennas and Propagation Society International Symposium, June 2009 DOI: <https://doi.org/10.1109/APS.2009.5171460>.
6. Бондаренко Б.Ф., Прокофьев В.П. "Применение методов функционального анализа для решения задачи синтеза системы пространственной обработки" // *Радиоэлектроника*. – 1982. – Т. 25, № 3. – С. 15-23.
7. Бондаренко Б.Ф., Сашук И.И., Тимчук В.Ю. "Предельное качество обнаружения и разрешения сигналов в обнаружителях на основе согласованных проекторов" // *Вісті вищих учбових закладів. Радиоелектроніка*, №48(3) – 2005. – С.24-33,. DOI: <https://doi.org/10.20535/S0021347005030039>
8. C. Radhakrishna Rao. "Linear Statistical Inference and its Applications" 2nd Edition, Wiley, New York, 1973. – 625p. DOI: www.doi.org/10.1002/9780470316436

REFERENCES:

1. Robert A. Monzingo; Randy L. Haupt; Thomas W. Miller "Introduction to Adaptive Arrays" (2nd Edition), 2011. – 543 p. DOI: <https://doi.org/10.1049/SBEW046E>
2. C. Schuessler, M. Hoffmann, and M. Vossiek, "Super-Resolution Radar Imaging with Sparse Arrays Using a Deep Neural Network" *IEEE Journal of Microwaves*, vol. 3, no. 1, pp. 45–56, 2023. DOI: <https://arxiv.org/pdf/2306.09839>
3. S. Yang, Y. Zhao, X. Tuo, et al., "Real Aperture Radar Angular Super-Resolution Imaging Using Modified Smoothed L0 Norm" *Remote Sensing*, vol. 16, no. 2, pp. 312, 2024. <https://doi.org/10.3390/rs16010012>
4. B.-S. Kim, Y. Jin, J. Lee, and S. Kim, "FMCW Radar Estimation Algorithm with High Resolution and Low Complexity Based on Reduced Search Area" *Sensors*, vol. 22, no. 3, pp. 1456, 2022. <https://doi.org/10.3390/s22031202>
5. Raymond J. Weber; Yikun Huang "Analysis for Capon and MUSIC DOA estimation algorithms" 2009 IEEE Antennas and Propagation Society International Symposium, June 2009 DOI: <https://doi.org/10.1109/APS.2009.5171460>.
6. Bondarenko B.F., Prokofev V.P. "Primeneniye metodov funktsyonalnoho analiza dlia resheniya zadachy synteza system prostranstvennoi obrabotky" // *Radyoelektronyka*. – 1982. – Т. 25, № 3. – С. 15-23.
7. Bondarenko B.F., Sashchuk Y.Y., Tymchuk V.Iu. "Predelnoe kachestvo obnaruzheniya y razresheniya syhnalov v obnaruzhyteliakh na osnove sohlasovannikh proektorov" // *Visti vyshchyykh uchbovykh zakladiv. Radioelektronika*, №48(3) – 2005. – С.24-33,. DOI: <https://doi.org/10.20535/S0021347005030039>
8. C. Radhakrishna Rao. "Linear Statistical Inference and its Applications" 2nd Edition, Wiley, New York, 1973. – 625p. DOI: www.doi.org/10.1002/9780470316436

APPLICATION OF THE SPATIAL FILTERING METHOD USING A SET OF MATRIX FILTERS -PROJECTORS TO DETERMINE THE COMPOSITION OF A GROUP TARGET WITHIN A SINGLE PULSE VOLUME OF A RADAR STATION

This paper addresses one of the critical challenges in modern radar systems – the determination of the composition of group concentrated targets (GCTs) within the radar’s impulse volume. The authors analyze advanced high-resolution methods that surpass the Rayleigh limit, focusing on alternative spectral analysis algorithms (such as MUSIC and Capon) and projection-based approaches. While spectral methods are limited by signal correlation and computational complexity, projection methods offer a more practical pathway to implementation.

The study proposes a spatial signal processing algorithm based on matrix projector filters (MPFs), enabling quasi-optimal resolution without the need to compute the inverse correlation matrix. The methodology is grounded in functional analysis and employs the least-squares criterion, ensuring adaptability under uncertain signal parameters. A structural scheme of the system is developed, incorporating multiple MPFs tuned to different target models. For the case of two targets within the impulse volume, the system utilizes a pair of projectors—one matched to a single target and the other to a dual-target configuration. The decision on the number of targets is made by comparing the outputs of these channels against a predefined threshold, effectively implementing a procedure close to optimal resolution.

Monte Carlo simulations confirm the efficiency of the proposed approach. Results demonstrate that at a signal-to-noise ratio of 16–20 dB, the high-resolution system based on dual MPFs achieves reliable separation of group targets, providing resolution twice as effective as the Rayleigh criterion.

In conclusion, the paper contributes significantly to the development of super-resolution radar systems, presenting a technically feasible algorithm capable of operating under conditions of high signal correlation. The findings hold substantial tactical importance for target detection and classification in contemporary radar applications. Keywords: geographic information system, geospatial data, geospatial support, ArcGIS, LiDAR, terrain change mapping, remote sensing, raster georeferencing, topographic map updating.

Keywords: group target, high-resolution system, pulse volume.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ АЕРОКОСМІЧНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМІ КОНТРОЛЮ НАД ЗВИЧАЙНИМИ ОЗБРОЄННЯМИ В ЄВРОПІ

У статті розглядаються особливості застосування інформаційних аерокосмічних технологій для підтримки прийняття управлінських рішень з використанням штучного інтелекту в системі контролю над звичайними озброєннями в Європі. Визначається, що розвиток інноваційних інформаційних аерокосмічних технологій в інтересах оборони є одним із пріоритетних завдань контролю над звичайними озброєннями в Європі. Інновації та новітні технології дозволяють розробити систему контролю над звичайними озброєннями та забезпечити національну безпеку держави. Завданням інноваційної діяльності у галузі контролю над звичайними озброєннями є виявлення, вивчення та впровадження технологій та механізмів державного управління, які забезпечать національні інтереси та національну безпеку України. При використанні систем підтримки прийняття управлінських рішень зі штучним інтелектом у сфері контролю над звичайними озброєннями в Європі можливо ефективно визначити сучасний стан та проблеми у сфері контролю над звичайними озброєннями; враховувати Європейський досвід (американський, країн НАТО) щодо застосування механізмів державного управління міжнародним співробітництвом у сфері контролю над звичайними озброєннями. Для контролю над звичайними озброєннями в Європі сьогодні доцільне використовувати сучасні інформаційні технології (використання матеріалів дистанційного зондування Землі зі супутників та літальних апаратів, а також застосування штучного інтелекту для формування управлінських рішень щодо забезпечення національної безпеки держави). Проведені дослідження свідчать про необхідність здійснення заходів щодо невідкладної організації постійного контролю за станом звичайних озброєнь в Європі та удосконалення системи контролю на основі інноваційних технологій для підвищення її ефективності. Міжнародне співробітництво України в сфері контролю над звичайними озброєннями в Європі сприяє зміцненню національної безпеки та потребує врахування як особливостей впровадження механізмів державного управління в цієї галузі так й інноваційних інформаційних аерокосмічних технологій в системі підтримки прийняття управлінських рішень з використанням штучного інтелекту. Перспективи подальших досліджень полягають у розробці апаратного та програмного забезпечення інформаційно-аналітичної системи контролю над надзвичайними озброєннями в Європі.

Ключові слова: виклики регіональній та глобальній безпеці; інформаційні аерокосмічні технології; міжнародна безпека; національна безпека; система міжнародних відносин; системи контролю над звичайними озброєннями; штучний інтелект.

Вступ та постановка проблеми.

Міжнародне співробітництво у сфері контролю над звичайними озброєннями є невід'ємною частиною сучасної системи безпеки. Комплекс міжнародних домовленостей та передбачених ними заходів з контролю над звичайними озброєннями та військовою діяльністю був вироблений у період 1975-1990 років у рамках Наради з безпеки і співробітництва в Європі (НБСЄ) у розпал "холодної війни" як один з інструментів зниження напруги у стосунках між Сходом і Заходом у рамках концепції "мирного співіснування". Подальша еволюція заходів зміцнення довіри супроводжувалась інституалізацією безпекового діалогу на майданчику НБСЄ у Відні та виходом на взаємне розуміння державами-учасницями Організації Варшавського договору (ОВД) і НАТО необхідності не лише інформаційного обміну, але й суттєвого обмеження та скорочення основних ударних озброєнь. У результаті 19 листопада 1990 р. у Парижі був підписаний Договір про звичайні збройні сили у Європі [1, 2].

У 1992 р. міжнародні моніторингові та контрольні-перевірочні механізми у військовій сфері були посилені режимом "відкритого неба", який надав державам-учасникам НАТО і колишньої ОВД можливість здійснювати з повітря безпосереднє спостереження за військовою діяльністю один одного та відвернути можливість підготовки та раптового розв'язання широкомасштабної війни [3, 4].

Побудований таким чином каркас загальноєвропейської безпеки зберігав свою ефективність упродовж майже 20 років. Основу цього механізму складали:

Договір про звичайні збройні сили в Європі (ДЗЗСЄ), який був підписаний 19 листопада 1990 р. у Парижі за Мандатом НБСЄ від 10 січня 1989 р.; набув чинності 09 листопада 1992 р.

Договір з відкритого неба (ДВН), який був підписаний 24 березня 1992 р. у м. Хельсінкі; ратифікований Україною 02 березня 2000 р.; набув чинності 01 січня 2002 р.

Віденський документ ОБСЄ про заходи зміцнення довіри і безпеки у військовій галузі у Європі, який є політично зобов'язуючою домовленістю держав-учасниць ОБСЄ.

Система контролю над звичайними озброєннями покликана забезпечити глобальну стабільність і безпеку. Однак, у світлі нових економічних і політичних реалій, виникає необхідність переосмислення існуючих механізмів контролю. Зростання військових витрат у багатьох країнах, розвиток нових технологій, а також політичні конфлікти в різних регіонах світу створюють нові загрози для міжнародної безпеки [5, 6].

Серед пріоритетів державного управління міжнародним співробітництвом України у сфері контролю над звичайними озброєннями в Європі доцільне визначити розвиток аерокосмічних технологій та штучного інтелекту в системах контролю над звичайними озброєннями. Міжнародний досвід свідчить, що аерокосмічний домен зараз активно розвивається, з'являється багато нових технологічних рішень щодо моніторингу стану озброєння та формування управлінських рішень за допомогою штучного інтелекту [7, 8].

Аналіз основних наукових досліджень і публікацій.

Питання застосування штучного інтелекту для вирішення завдань керування складними динамічними процесами розглядали Нільс Й. Нільссон, Стюарт Дж. Рассел, Пітер Норвіг [9, 10]. Парадигма обробки інформації в інтелектуальній інформаційній системі для підтримки прийняття рішень в галузі екологічної безпеки запропонована в [11, 12]. Питанням дослідження міжнародної співпраці займався багато науковців, зокрема серед дослідників проблематики міжнародного співробітництва у військовій сфері слід відзначити Богдановича В.Ю., Голопатюка Л.С., Пунда Ю.В., Ситника Г.П., Шаповалова Г.М. [4, 6]. Даалдер І. та Голдгеріе Дж. Розкривають роль НАТО в забезпеченні контролю над озброєннями та військової транспарентності. Обговорюється роль НАТО у підтримці міжнародної системи безпеки після Холодної війни. Особлива увага приділяється ролі військової транспарентності та контролю озброєнь як інструментів стримування конфліктів [13].

Проведений аналіз свідчить, що у теперішній час залишаються актуальними та не вирішеними питання застосування інформаційних аерокосмічних технологій в системі підтримки прийняття управлінських рішень з застосуванням штучного інтелекту для контролю над станом звичайного озброєння в Європі. Тому, з огляду на необхідність посилення обороноздатності України, зміцнення її міжнародних позицій та створення умов для ефективної інтеграції в європейську систему безпеки, вирішення цього завдання є актуальним.

Мета статті: дослідження механізмів застосування інформаційних аерокосмічних технологій в системі підтримки прийняття управлінських рішень з використанням штучного інтелекту в системі контролю над звичайними озброєннями в Європі.

Виклад основного матеріалу.

Аналіз тенденцій розвитку системи контролю над звичайними озброєннями в Європі.

Договір про звичайні збройні сили в Європі було узгоджено та укладено протягом останніх років Холодної війни та встановлено всеосяжні обмеження на ключові категорії звичайної військової техніки в Європі (від Атлантики до Уралу) і передбачав знищення надлишкової зброї. Договір пропонував рівні обмеження для двох "груп держав-учасниць", Організації Північноатлантичного договору (НАТО) і Варшавського пакту. Договір був

підписаний 19 листопада 1990 року в Парижі, підписи під ним поставили представники 16 держав НАТО, а також шість держав-учасниць Варшавського договору. Угода встановлювала обмеження розмір звичайних збройних сил і визначало граничні чисельності звичайних озброєнь, розгорнутих сторонами у Європі [1,2].

Україна зацікавлена у розбудові нової повоєнної безпекової архітектури у Європі відповідно до безпекових і воєнних пріоритетів.

Заходи зміцнення довіри і безпеки у військовій галузі у Європі (ЗЗДБ) були вироблені та ухвалені державами-учасницями ОБСЄ у період з 1986 по 1992 рр. з подальшим їх розвитком та модернізацією упродовж 1994-2011 рр.

Їх кодифікація здійснена у формі "Віденського документа про заходи зміцнення довіри і безпеки у військовій галузі у Європі" (ВД ЗЗДБ). Дія ЗЗДБ поширилась на територію всіх європейських держав, європейську частину Туреччини та СРСР.

У 1986 р. за результатами Стокгольмської конференції НБСЄ з заходів безпеки, механізм ЗЗДБ був доповнений зобов'язаннями щодо:

1) попереднього сповіщення один одного – за 42 дні – про військову діяльність (навчання, перекидання і зосередження військ) у регіоні "від Атлантики до Уралу", якщо кількість залучених сил налічувала 13 тис. чоловік, 300 танків (у складі одної дивізії, бригади чи полку);

2) запрошення спостерігачів на навчання, перекидання і зосередження військ, за участі у них понад 17 тис. чоловік;

3) обміну щорічними планами військової діяльності на наступний рік;

4) започаткування інспекційного режиму.

Подальша еволюція ЗЗДБ призвела до вироблення та систематизації комплексу ЗЗДБ у формі Віденського документа про заходи зміцнення довіри і безпеки у військовій галузі 1990 року (ВД-1990), який, увібравши в себе всі основні положення Стокгольмського документу, був доповнений низкою нових елементів:

- надання інформації про військові бюджети;
- інформування про так звану "надзвичайну військову діяльність" збройних сил поза місцями їх дислокації в мирний час, щодо якої виникають занепокоєння з міркувань безпеки;
- сповіщення про небезпечні інциденти військового характеру;
- демонстрація та відвідання військових авіабаз;
- започаткування практики проведення у місцях постійної дислокації військових частин "відвідувань з оцінки інформації" на додаток до здійснення інспекцій.

У цілому з 1990 р. Віденський документ оновлювався п'ять разів (у 1992, 1994, 1996, 1999 та 2011 роках) з метою уточнення/розширення – за досвідом практичного застосування – вже узгоджених заходів та доповнення їх новими елементами ЗЗДБ.

Чинний на сьогодні ВД-2011 був прийнятий на надзвичайній сесії Форуму з питань безпекового співробітництва (ФБС) ОБСЄ 30 листопада 2011р. Наразі на міжнародних переговорах у рамках ОБСЄ у Відні триває робота з подальшого оновлення/модернізації ЗЗДБ. Зоною застосування ЗЗДБ є розширена Європа, включаючи всю континентальну Європу з острівними територіями, а також територію азійських держав-учасниць (Казахстан, Киргизстан, Таджикистан, Туркменістан, Узбекистан).

Еволюція ЗЗДБ упродовж 1992-2011 р. здійснювалась відповідно до військово-політичних змін у Європі та потреб контролю за військовою діяльністю й активністю ЗС держав-учасниць. ВД, включаючи понад 30-річний період його імплементації та еволюції його положень, засвідчив свою непересічну дієвість та ефективність у якості інструменту виключно мирного часу, коли держави-учасниці прагнуть миру, зацікавлені у практичній деескалації відносин, встановленні довіри та передбачуваності у воєнній сфері.

Водночас, на тлі ознак стагнації міжнародних режимів контролю над озброєнням та військовою діяльністю, пов'язаної, серед іншого, з фактичним припиненням дії Договору про звичайні збройні сили в Європі, заходи зміцнення довіри і безпеки, посилювані можливостями Договору з відкритого неба, залишаються чи не єдиним джерелом отримання та оцінки інформації щодо військових намірів держав-учасниць, стану та характеру активності їхніх збройних сил. У

рамках Імплементації ВД-2011 здійснюється інформаційний обмін та інспекційна діяльність, а також прийняття іноземних військових інспекцій на території України.

Держави-учасники щорічно обмінюються інформацією про свої військові сили, основні системи озброєнь та військової техніки, про планування в галузі оборони та військові бюджети. Заходи раннього виявлення/попередження конфліктів включають механізм консультацій у зв'язку з незвичайною військовою діяльністю, яка може спровокувати стурбованість. Елементами довіри передбачено багатостороннє завчасне інформування про певні види військової діяльності (проведення масштабних навчань чи перекидань військ), запрошення спостерігачів та моніторингових місій, проведення інспекцій та відвідування військових формувань для оцінки правильності наданої про них інформації.

Особливе значення для України мають "Регіональні заходи", які в сучасних умовах дозволяють Україні проводити за участю іноземних військових інспекторів додаткові багатонаціональні інспекції.

Проведення таких інспекцій та відвідувань створює додатковий режим міжнародного військового моніторингу, який доповнює діяльність моніторингових місій ОБСЄ. Зокрема, лише у 2019 р. у рамках заходів "Регіонального співробітництва" за участю іноземних військових інспекторів було проведено 16 контрольно-перевірочних заходів (інспекцій та візитів) за участю Фінляндії, Грузії, Естонії, Німеччини, Норвегії, США, Канади, Румунії, Угорщини, Словаччини та інших держав, частина з яких здійснювалась в районі проведення ООС (Норвегія, Канада, США, Данія). У свою чергу, Україною здійснено 29 контрольно-перевірочних заходів на території інших держав.

Договір про звичайні збройні сили в Європі (ДЗЗСЄ) підписано 19 листопада 1990 р. у Парижі вищими представниками урядів і міністрами закордонних справ 22 країн. Головна ідея ДЗЗСЄ полягала у тому, щоб зменшити небезпечну концентрацію озброєнь, яка існувала на той час на лінії військового протистояння двох воєнно-політичних блоків в Європі. Цей документ розроблявся в умовах жорсткого протистояння двох блоків і передбачав значно зменшити наступальні потенціали колишніх держав-супротивників та забезпечити ефективний контроль за рівнем звичайних озброєнь за допомогою збройних сил Організації Варшавського договору і НАТО, через обмін інформацією та верифікацією, тобто перевірки на місцях. Договір, який був підписаний колишнім СРСР, ратифікований Верховною Радою України 1 липня 1992 р. Він є безстроковим. Район дії Договору охоплює всю сухопутну територію держав-учасниць в Європі від Атлантичного океану до Уральських гір. Для кожної держави були визначені максимальні рівні для п'яти категорій звичайних озброєнь (бойові танки, бойові броньовані машини, артистери калібру більше 100 мм, бойові літаки та ударні вертольоти).

Незважаючи на скрутне економічне становище, наша держава знайшла можливість виконати свої міжнародні зобов'язання стосовно скорочення обмежених договором озброєнь та техніки. В Україні було скорочено 1974 од. бойових танків, 1545 од. бойових броньованих машин, 550 од. бойових літаків. Для забезпечення контролю за рівнями озброєнь Договір передбачає щорічний обмін інформацією, яка готується у верифікаційних структурах і розповсюджується між державами. Для перевірки достовірності даних обмінної інформації, іноземні інспекційні групи близько 500 разів інспектували українські військові частини.

Незважаючи на те, що процес адаптації існуючого Договору почався наприкінці грудня 1996 р. в складних умовах, переговори були успішно завершені підписанням у Стамбулі 19.11.1999 р. Угоди з адаптації Договору про ЗЗСЄ. І вже 21 вересня 2000 р. Верховна Рада України ратифікувала цю Угоду як важливий документ, який відповідає сучасним умовам. Значним кроком на шляху до адаптації Договору став перегляд умов функціонування Договору щодо регулювання розміщення іноземних військ, вдосконалення системи контролю над озброєннями, забезпечення її надійного функціонування та обміну інформацією на наступні роки. Такий підхід дозволив ввести систему обмежень, яка виключає можливість неконтрольованої передачі озброєнь одній державі іншій. Встановлені обмеження (стелі) для розміщення як своїх, так і іноземних озброєнь та сил, які нейтралізують накопичення сил протиборчих сторін.

Подальше вдосконалення Договору про звичайні збройні сили в Європі після його адаптації варто проводити у наступних напрямках:

- у розширенні зони дії Договору, насамперед, за рахунок тих держав, які мають за мету приєднатися до нього. Виходячи з цього, необхідно відпрацювати механізм подальших скорочень звичайних озброєнь, щоб не допустити порушення основного принципу Договору – не збільшувати кількість озброєння та техніки на європейському континенті;

- у додатковому включенні до Договору інших видів та типів звичайних озброєнь, які характеризуються високою маневреністю, захищеністю, вогневою могутністю та мають значний бойовий потенціал;

- в удосконаленні системи обміну інформацією, яка виключала б можливість обходу положень Договору; її базовими елементами повинні стати достовірність, прозорість та точність передачі інформації;

- у подальшому розвитку та удосконаленні інспекційного режиму, ключовим елементом якого повинен стати посилений режим контролю над звичайними озброєннями.

Трансфер аерокосмічних технологій дистанційного зондування Землі в систему контролю над звичайними озброєннями в Європі.

У теперішній час космічний моніторинг широко використовується при дистанційному зондуванні Землі. За допомогою використання існуючих та нових методик оцінки стану об'єктів спостереження з використанням штучного інтелекту можливо оперативно вирішувати завдання в області національної безпеки, контролю над станом звичайного озброєння. Застосування штучного інтелекту в системі контролю над станом звичайного озброєння дозволяє [7,8]:

- забезпечити об'єктивність і достовірність первинної, аналітичної і прогнозованої інформації стосовно стану звичайного озброєння;

- мати систематичні спостереження за станом звичайного озброєння;

- підвищити оперативність здобуття і достовірність первинних даних за рахунок використання ефективних технологій процесів збору, накопичення і обробки інформації на всіх рівнях державного управління в системі контролю над звичайними озброєннями в Європі;

- забезпечити сумісність технічного, інформаційного і програмного забезпечення в системі контролю над звичайними озброєннями в Європі та управління національною безпекою з використанням штучного інтелекту;

- підвищити рівень і якості інформаційного обслуговування операторів та споживачів інформації стосовно звичайного озброєння на всіх рівнях функціонування системи підтримки прийняття управлінських рішень на основі мережевого доступу до розподілених відомчих і інтегрованих баз даних;

- забезпечити оперативність доведення інформації стосовно контролю над звичайними озброєннями до відповідних органів державного управління;

Враховуючи визначені принципи та нові підходи, що розроблені в роботах [8, 14] пропонується при здійсненні контролю над звичайними озброєннями застосовувати програмно-апаратні засоби і програмні продукти геоінформаційних систем та засоби автоматизованої обробки знімків дистанційного зондування Землі для створення карти розміщення звичайних озброєнь та районів їх виготовлення, створення, випробувань. Процес створення цифрових карт районів контролю над звичайними озброєннями поділяється на декілька послідовних етапів, протягом яких формуються її основні частини:

1. Етап. Підготовчий - формуються вимоги до створюваної карти моніторингу звичайних озброєнь, визначається район спостереження, здійснюється збір і обробка вихідної інформації.

2. Етап. Формування карти динаміки процесів при здійсненні контролю над звичайними озброєннями у визначених районах - здійснюється за допомогою засобів автоматизованої обробки знімків, на основі вихідних знімків, формується спеціальне зображення району контролю.

3. Етап. Формування багатоспектральної мапи динаміки процесів в районах контролю на основі існуючої виделеної спектральної характеристики мапи району спостереження.

4. Етап. Складання якісної порівняльної характеристики мапи динаміки процесів в районах контролю над звичайними озброєннями.

Розглянемо можливості застосування космічних технологій для проведення контролю над звичайними озброєннями з застосуванням штучного інтелекту. Тематична обробка та дешифрування космічних знімків виконується за допомогою програмного забезпечення TROAS – IMAGINE. Для побудови цифрових карт було використано програмне забезпечення ESRI ArcGIS. Базова цифрова картографічна основа створюється на територію району контролю в масштабі 1: 50.000 та містить шари: межі області; межі районів; об'єкти гідрографії (річки, озера, болота); населені пункти (міста, селища, села); дороги (автомобільні, залізничні). Вихідні цифрові карти створені в географічній системі координат UTM – WGS84 і передаються у shp –форматі.

При проведенні досліджень було використано орторектифіковані космічні знімки території України, отримані у Національному центрі управління та випробувань космічних засобів Державного космічного агентства України [8, 14]. Класифікація космічних зображень з метою встановлення розповсюдження певних класів звичайних озброєнь може стати основою для створення системи управління національною безпекою. Для проведення класифікації космічних знімків був використаний програмний продукт ERDAS Imagine, який визнано одним із світових лідерів серед програмних продуктів подібного призначення. ERDAS Imagine широко застосовується для оброблення супутникової інформації у багатьох наукових та виробничих центрах провідних країн Заходу (США, Німеччина, Франція, Італія та ін.).

Обробка матеріалів зйомки включає геодезичну (географічну) прив'язку, ліквідацію або облік геометричних спотворень знімків, перетворення і дешифрування їх. Контурне дешифрування полягає у виділенні серед району спостереження масиву топографічних об'єктів і контурів площ для подальшого опису їх шляхом наземного огляду або способом аеротаксації. Таксаційне дешифрування є найбільш складним і важким. Воно полягає в поділі району спостереження на таксаційні ділянки та визначенні геологічного складу.

Існує велика кількість сучасних пакетів з обробки даних ДЗЗ, які доцільне використовувати в системах штучного інтелекту. Підбір матеріалів космічної зйомки є важливим етапом проведення класифікації для моніторингу району спостереження. Для робіт по тематичному дешифруванню та створенню цифрових карт територій контролю над звичайними озброєннями були використані орторектифіковані космічні знімки з супутника Landsat-7, які були отримані у 2019 році (рис. 1).

Технологічно процес дешифрування з використанням штучного інтелекту можна розділити на два основні етапи: машинна класифікація; візуальне дешифрування. Машинна класифікація дозволяє автоматизувати процес дешифрування. Метою класифікації є одержання тематичної інформації із знімка. У процесі класифікації у комп'ютерних системах статистичні дані одержуються із спектральних характеристик усіх пікселів зображення. При цьому сортування базується на математичних критеріях. Існує два шляхи класифікації: з неконтрольованим навчанням; з контрольованим навчанням. Нами був обраний другий шлях розрахунку з метою його розповсюдження для можливих районів контролю над звичайними озброєннями. Дана класифікація проводиться за допомогою навчання по обраним еталонам із створенням для кожного з них відповідної сигнатури, які в подальшому й використовуються для визначення центрів класів спостереження. Процес формування сигнатур доцільно завершити, якщо простір ознак максимально заповнений спектральними образами, які не перетинаються. Далі встановлювалися кольорові градації сформованими сигнатурами класам і давалася назва. В результаті створюється набір сигнатур, що визначають вибірку навчання. Кожна сигнатура відповідає класу та використовується у відповідності з вирішальним правилом для віднесення пікселів до того чи іншого класу (рис. 2).

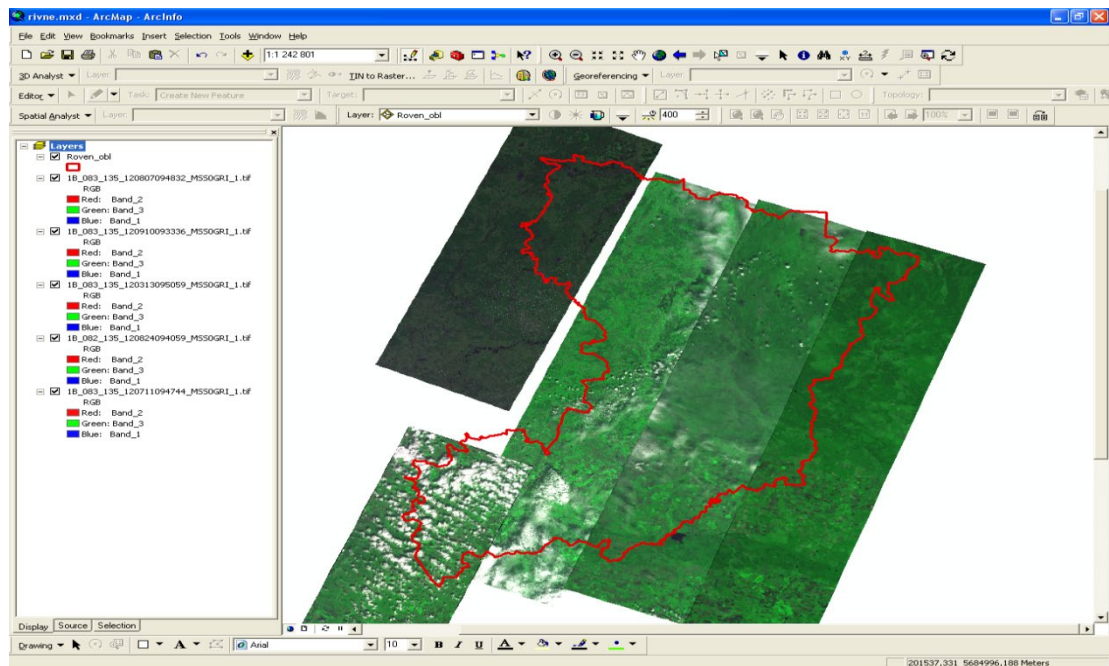


Рисунок 1 – Розташування космічних знімків з супутника Landsat-7 на досліджувану територію, *авторська розробка*

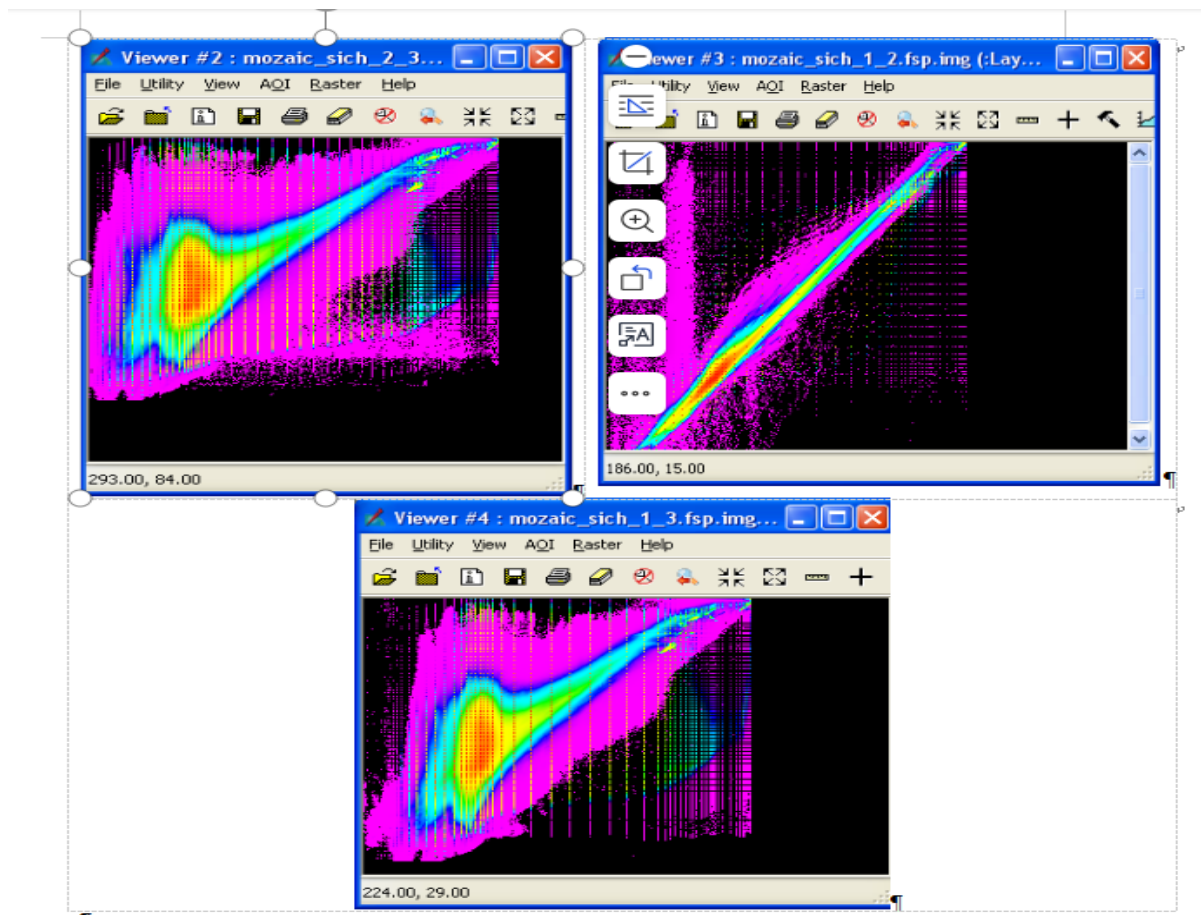


Рисунок 2 – Варіанти результуючих зображень простору ознак, утворених на основі комбінацій різних каналів, *авторська розробка*

Модуль класифікації ERDAS Imagine має багато підходів в залежності від можливостей знімка, типу створених сигнатур, вибору спеціаліста-аналітика. В процесі роботи були обрані сигнатури типу "еліпс" (рис. 3).

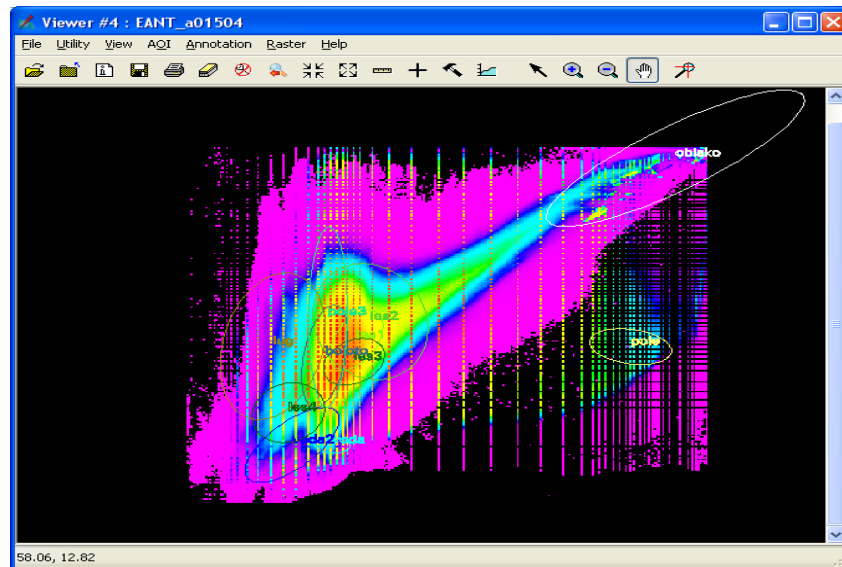


Рисунок 3 – Перегляд об'єктів еталонів на зображенні простору ознак, *авторська розробка*

Для того щоб отримати кольорове зображення було проведено поєднання колонок атрибутів растрів вихідного тематичного та отриманого після генералізації (рис. 4). В результаті чого колір напівтонової шкали зміниться на відповідний колір з еталонного файлу.

Після проведеної генералізації отримане тематичне зображення знову було проаналізоване з метою об'єднання (злиття) класів (функція перекодування тематичного растрового шару). В результаті було отримане відредаговане зображення (рис. 4).

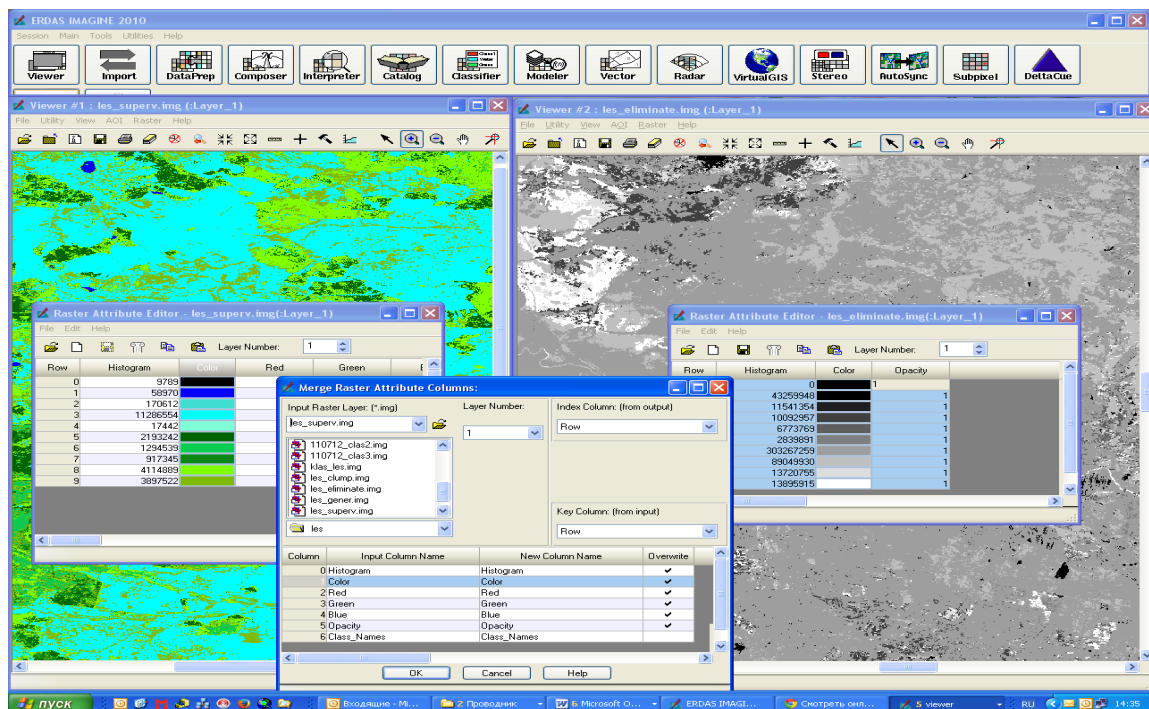


Рисунок 4 – Процес встановлення зв'язку між еталонним і генералізованим зображеннями, *авторська розробка*

Отримане зображення використовується для формування управлінських рішень щодо контролю над звичайними озброєннями.

Висновки. Міжнародне співробітництво у сфері контролю над звичайними озброєннями в Європі є невід'ємною частиною сучасної системи безпеки. Воно забезпечує механізми

ефективного реагування на глобальні виклики, зміцнює оборонні можливості держави та національній безпеці держави. У той же час для забезпечення успішності такого співробітництва важливо застосовувати аерокосмічні технології для здійснення моніторингових завдань, а також штучного інтелекту при формуванні управлінських рішень в системі контролю над звичайними озброєннями в Європі. Для контролю над звичайними озброєннями в Європі сьогодні доцільне використовувати сучасні інформаційні технології (використання матеріалів дистанційного зондування Землі зі супутників та літальних апаратів, а також застосування штучного інтелекту для формування управлінських рішень щодо забезпечення національної безпеки держави). Проведені дослідження свідчать про необхідність здійснення заходів щодо невідкладної організації постійного контролю за станом звичайних озброєнь в Європі та удосконалення системи контролю на основі інноваційних технологій для підвищення її ефективності. Перспективи подальших досліджень полягають у розробці апаратного та програмного забезпечення інформаційно-аналітичної системи контролю над звичайними озброєннями в Європі.

ЛІТЕРАТУРА:

1. Міжнародні відносини та зовнішня політика України: підручник / Ю. В. Пунда та ін. Київ: НУОУ ім. Івана Черняхівського, 2020. 328 с.
2. Мороз В.М. Виклики для системи контролю над звичайними озброєннями: економічний та соціальний аспекти. Національні інтереси України, 1(6), 2025. С. 49-63. <http://perspectives.pp.ua/index.php/niu/article/view/18531/18566>
3. Качинський А.Б. Безпека складних систем: моногр. / за ред. С.О. Довгого. К.: ТОВ "Видавництво "ЮСТОН", 2017. 468 с.
4. Методологія комплексного використання військових і невійськових сил та засобів сектору безпеки і оборони для протидії сучасним загрозам воєнній безпеці України: монографія / В. Ю. Богданович та ін. Київ: НУОУ ім. Івана Черняхівського, 2019. 268 с.
5. Ситник Г., Мороз В. Формування ефективної системи контролю над звичайними озброєннями в Європі: проблематика дослідження. Вісник Київського національного університету імені Тараса Шевченка. Національна безпека, 1(1), 2024 11-18. <https://doi.org/10.17721/3041-1912.2024/1-1/11>
6. Ситник Г.П., Орел М.Г. Глобалізаційні виклики: урядування майбутнього. Монографія / авт.кол. Л.Г.Комаха, І.В.Алексєєнко, В.А.Гошовська та ін.; за заг.ред. Л.Г.Комахи, І.В.Алексєєнко. Київ: ВПЦ "Київський університет", 2022. 976 с.
7. Багатоспектральні методи дистанційного зондування Землі в задачах природокористування / [Лялька В.І., Федоровський О.Д., Попов М.О. та ін] під ред. В.І.Лялька, М.О.Попова. — К.: Наук.думка, 2006. — 357 с.
8. Машков Олег, Присяжний Володимир, Оводенко Тамара. Напрями застосування системного підходу в системі державного управління екологічною безпекою з використанням аерокосмічних технологій. Вісник Київського національного університету імені Тараса Шевченка, ISSN 3041-1912 (Print), ISSN 3041-1920 (Online): Національна безпека 2(2)/2024, с.17-24, УДК 351:311.3:627.7, DOI: <https://doi.org/10.17721/3041-1912.2024/2-3/11>
9. Nils J. Nilsson . The Quest for Artificial Intelligence. – 1. – Cambridge University Press, 2009. – 578 с. - ISBN 978-0521116398 .
10. Stuart J. Russell, Peter Norvig . Artificial Intelligence: A Modern Approach. – 3. – Pearson, 2015. – ISBN 978-9332543515.
11. Концепція створення інтелектуальної інформаційної системи для підтримки прийняття рішень у галузі екологічної безпеки. Бондар О.І., Машков О.А., Присяжний В.І., Оводенко Т.С., Печений В.Л. / Екологічні науки: науково-практичний журнал. К.: ДЕА, -Випуск 3(48), 2023, с.7-16.
12. Системи штучного інтелекту: навчальний посібник. / Н. Б. Шаховська, Р. М. Камінський, О. Б. Вовк. - Львів: Вид-во Львівської політехніки, 2018. - 392 с. - ISBN 966-941-197-6 .
13. Daalder, I. H., & Goldgeier, J. M. (2006) Global NATO and the post-Cold War order. Foreign Affairs, 85(5), 105–113. <https://www.foreignaffairs.com/articles/united-states/2006-09-01/globalnato-and-post-cold-war-order>
14. Машков О.А., Мухіна К.Е., Присяжний В.І. Системний підхід до синтезу управлінських рішень забезпечення національної безпеки держави / Актуальні питання у сучасній науці, № 4(34) 2025, с.330-340. DOI: [https://doi.org/10.52058/2786-6300-2025-4\(34\)](https://doi.org/10.52058/2786-6300-2025-4(34)).

REFERENCES:

1. Mizhnarodni vidnosyny ta zovnishnya polityka Ukrayiny [International Relations and Foreign Policy of Ukraine]: Textbook (2020) / Yu. V. Punda et al. Kyiv: Ivan Chernyakhovsky National Defense University of Ukraine, 2020. 328 p. [in Ukrainian].
2. Moroz V.M. Vyklyky dlya systemy kontrolyu nad zvychnymy ozbroynnyamy: ekonomichnyy ta sotsial'nyy aspekty [Challenges for the conventional arms control system: economic and social aspects]. National Interests of Ukraine, 1(6), 2025. P. 49-63. <http://perspectives.pp.ua/index.php/niu/article/view/18531/18566> . [in Ukrainian].
3. Kachynsky A.B. Bezpeka skladnykh system [Security of complex systems]: monograph / edited by S.O. Dovgy. K.: LLC "Yuston Publishing House", 2017. 468 p.. [in Ukrainian].
4. Metodolohiya kompleksnoho vykorystannya viyskovykh i neviyskovykh syl ta zasobiv sektoru bezpeky i oborony dlya protydyi suchasnym zahrozam voyennyi bezpetsi Ukrayiny [Methodology of the integrated use of military and non-military forces and means of the security and defense sector to counter modern threats to the military security of Ukraine]: monograph (2019) / V. Yu. Bogdanovych et al. Kyiv: Ivan Chernyakhovsky National Defense University of Ukraine, 2019. 268 p. [in Ukrainian].
5. Sytnyk G., Moroz V. Formuvannya efektyvnoyi systemy kontrolyu nad zvychnymy ozbroynnyamy v yevropi: problematyka doslidzhennya [Formation of an effective system of control over conventional arms in Europe]: research issues. Bulletin of the Taras Shevchenko National University of Kyiv. National Security, 1(1), 2024 11-18. <https://doi.org/10.17721/3041-1912.2024/1-1/11> . [in Ukrainian].
6. Sytnyk G.P., Orel M.G. Hlobalizatsiyni vyklyky: uryaduvannya maybutn'oho [Globalization challenges: governance of the future]. Monograph / co-authors L.G. Komakha, I.V. Alekseenko, V.A. Goshovskaya and others; editors L.G. Komakha, I.V. Alekseenko. Kyiv: VOC "Kyiv University", 2022. 976 p.. [in Ukrainian].
7. Bahatospektral'ni metody dystantsiynoho zonduvannya Zemli v zadachakh pryrodokorystuvannya [Multispectral methods of remote sensing of the Earth in environmental management problems] / [Lyalko V.I., Fedorovsky O.D., Popov M.O. and others], ed. V.I. Lyalko, M.O. Popova. — K.: Nauk.dumka, 2006. — 357 p.
8. Mashkov Oleg, Prysyazhny Volodymyr, Ovodenko Tamara. (2024). Napryamy zastosuvannya systemnoho pidkhodu v systemi derzhavnoho upravlinnya ekolohichnoyu bezpekoyu z vykorystanniam aerokosmichnykh tekhnolohiy [Directions for the Application of a System Approach in the System of State Management of Environmental Safety Using Aerospace Technologies]. Bulletin of the Taras Shevchenko National University of Kyiv, ISSN 3041-1912 (Print), ISSN 3041-1920 (Online): National Security 2(2)/2024, pp.17-24, UDC 351:311.3:627.7, DOI: <https://doi.org/10.17721/3041-1912.2024/2-3/11> [in Ukrainian].
9. Nils J. Nilsson . The Quest for Artificial Intelligence. – 1. – Cambridge University Press, 2009. – 578 c. - ISBN 978-0521116398 . [in English].
10. Stuart J. Russell, Peter Norvig . Artificial Intelligence: A Modern Approach. – 3. – Pearson, 2015. – ISBN 978-9332543515. [in English].
11. Kontseptsiya stvorennia intelektual'noyi informatsiynoyi systemy dlya pidtrymky pryynyattya rishen' u haluzi ekolohichnoyi bezpeky. [Concept of creating an intelligent information system to support decision-making in the field of environmental safety]. Bondar O.I., Mashkov O.A., Prysyazhny V.I., Ovodenko T.S., Pecheny V.L. / Ecological Sciences: Scientific and Practical Journal. K.: DEA, - Issue 3(48), 2023, p.7-16.
12. Systemy shtuchnoho intelektu: navchal'nyy posibnyk [Artificial Intelligence Systems]: A Textbook. / N. B. Shakhovska, R. M. Kaminsky, O. B. Vovk. - Lviv: Lviv Polytechnic Publishing House, 2018. - 392 p. - ISBN 966-941-197-6 .
13. Daalder, I. H., & Goldgeier, J. M. (2006) Global NATO and the post-Cold War order. Foreign Affairs, 85(5), 105–113. <https://www.foreignaffairs.com/articles/united-states/2006-09-01/globalnato-and-post-cold-war-order> [in English].
14. Mashkov O.A., Mukhina K.E., Prysyazhny V.I. Systemnyy pidkhid do syntezy upravlins'kykh rishen' zabezpechennya natsional'noyi bezpeky derzhavy [Systemic approach to the synthesis of management decisions to ensure national security of the state] / Current issues in modern science, No. 4(34) 2025, pp. 330-340. DOI: [https://doi.org/10.52058/2786-6300-2025-4\(34\)](https://doi.org/10.52058/2786-6300-2025-4(34)) . [in Ukrainian].

APPLICATION OF AEROSPACE INFORMATION TECHNOLOGIES IN THE SYSTEM OF SUPPORTING MANAGEMENT DECISIONS USING ARTIFICIAL INTELLIGENCE IN THE SYSTEM OF CONTROL OF CONVENTIONAL ARMS IN EUROPE

Abstract. The article examines the features of the application of information aerospace technologies in the system of support for managerial decisions using artificial intelligence in the system of control over conventional arms in Europe. It is determined that the development of innovative information aerospace technologies in the interests of defense is one of the priority tasks of control over conventional arms in Europe. Innovations and new technologies allow to develop a system of control over conventional arms and ensure the national security of the state. The task of innovative activity in the field of control over conventional arms is to identify, study and implement technologies and mechanisms of public administration that will ensure the national interests and national security of Ukraine. When using systems of support for managerial decisions with artificial intelligence in the field of control over conventional arms in Europe, it is possible to effectively determine the current state and problems in the field of control over conventional arms; take into account European experience (American, NATO countries) in the application of mechanisms of public administration in international cooperation in the field of control over conventional arms. For the control of conventional weapons in Europe today, it is advisable to use modern information technologies (the use of remote sensing materials from satellites and aircraft, as well as the use of artificial intelligence to form management decisions to ensure the national security of the state). The conducted studies indicate the need to take measures to urgently organize constant control over the state of conventional weapons in Europe and improve the control system based on innovative technologies to increase its efficiency. International cooperation of Ukraine in the field of control of conventional weapons in Europe contributes to strengthening national security and requires taking into account both the features of the implementation of state management mechanisms in this area and innovative information aerospace technologies in the system of support for making management decisions using artificial intelligence.

Keywords: challenges to regional and global security; information aerospace technologies; international security; national security; system of international relations; conventional arms control systems; artificial intelligence.

УДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ СТВОРЕННЯ КАРТ ЗМІН МІСЦЕВОСТІ ЗА ДОПОМОГОЮ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ARCGIS

У статті розглянуто питання вдосконалення технологій створення карт змін місцевості із застосуванням геоінформаційних систем, зокрема програмного забезпечення ArcGIS, в умовах зростання обсягів геопросторових даних та підвищених вимог до оперативності геопросторової підтримки військ (сил). Актуальність дослідження зумовлена необхідністю своєчасного оновлення топографічної інформації в умовах динамічних змін природного та антропогенного середовища, а також у контексті сучасних бойових дій, що характеризуються високою мінливістю обстановки. Встановлено, що традиційні методи створення карт змін місцевості, які базуються на використанні паперових карт і ручному внесенні змін, не забезпечують необхідного рівня оперативності, точності та інтеграції різномірних джерел геопросторової інформації. Обґрунтовано доцільність переходу до використання геоінформаційних систем як основи автоматизації процесів збору, обробки, аналізу та оновлення просторових даних.

Методичну основу дослідження становлять методи геоінформаційного моделювання, просторового аналізу, обробки растрових і векторних даних, а також аналіз сучасних підходів до виявлення змін місцевості. Доведено ефективність інтеграції багатоджерельних геоданих, зокрема аерофотознімків, космічних зображень, LiDAR-даних, електронних карт і результатів геодезичних вимірювань. Запропоновано удосконалену технологічну схему створення карт змін місцевості, яка передбачає використання електронної чергової карти, інтеграцію різномірних джерел даних, виконання аналізу змін, автоматизовану векторизацію та формування цифрового картографічного продукту. Визначено переваги застосування ArcGIS, зокрема підвищення оперативності обробки даних, зменшення трудомісткості робіт та забезпечення топологічної коректності просторових даних. Практичне значення результатів полягає у можливості їх використання для підвищення ефективності геопросторової підтримки військ (сил), скорочення часу оновлення картографічної інформації та підвищення якості прийняття управлінських рішень.

Ключові слова: геоінформаційна система, геопросторові дані, геопросторова підтримка, ArcGIS, LiDAR, карта змін місцевості, дистанційне зондування Землі, геоприв'язка растрових даних, оновлення топографічних карт.

Вступ та постановка проблеми. У сучасних умовах стрімкого розвитку геоінформаційних технологій особливого значення набуває питання оперативного створення та оновлення топографічних карт та карт змін місцевості [1, 3, 17, 18]. Такі карти використовуються для оцінювання змін природного середовища, моніторингу забудови, транспортної інфраструктури, лісових масивів, гідрографії, а також для потреб геопросторової підтримки військ (сил) [19].

Зростання обсягів геопросторових даних, що надходять із різних джерел, зокрема дистанційного зондування Землі, безпілотних авіаційних систем та геодезичних вимірювань, призводить до необхідності їх оперативної обробки та інтеграції [2]. У цих умовах традиційні підходи до оновлення картографічної інформації втрачають ефективність, оскільки не забезпечують своєчасності прийняття рішень, особливо у сфері військового управління.

Крім того, сучасні бойові дії характеризуються високою динамікою змін обстановки, що вимагає постійного оновлення геопросторових даних. Це обумовлює необхідність переходу від статичних карт до динамічних геоінформаційних моделей місцевості. Традиційна технологія створення карт змін місцевості ґрунтується на використанні паперових топографічних карт, тиражних відбитків та ручного нанесення змін. Такий підхід характеризується значними витратами часу, високою трудомісткістю та ризиком виникнення помилок. Перехід до використання сучасних геоінформаційних систем дає можливість

автоматизувати значну частину операцій, пов'язаних зі збором, аналізом, оновленням та відображенням просторових даних.

ArcGIS є однією з найбільш функціонально розвинених геоінформаційних платформ, що забезпечує підтримку обробки растрових і векторних даних, інтеграцію матеріалів дистанційного зондування Землі, автоматизовану векторизацію, побудову цифрових моделей рельєфу та створення електронних карт різного тематичного навантаження [8].

Важливою особливістю сучасного етапу розвитку геоінформаційних технологій є перехід від використання окремих картографічних продуктів до створення інтегрованих геоінформаційних середовищ, які забезпечують безперервне оновлення даних. У таких умовах карта змін місцевості розглядається не як кінцевий продукт, а як динамічна модель, що постійно уточнюється. Особливої актуальності це набуває у військовій сфері, де достовірність і своєчасність геопросторової інформації безпосередньо впливають на ефективність прийняття рішень. Затримка або неточність даних може призвести до помилок у плануванні операцій та використанні ресурсів.

Незважаючи на значну кількість досліджень у даній сфері, питання формалізації процесу створення карт змін місцевості та кількісної оцінки ефективності використання геоінформаційних систем залишаються недостатньо розробленими та потребують удосконалення.

Аналіз останніх досліджень і публікацій. Питання створення та оновлення топографічних карт та карт змін місцевості досліджувалися у працях українських і зарубіжних науковців [1-5]. Значна увага приділяється використанню дистанційного зондування Землі, супутникових та аерофотознімків, LiDAR-технологій, а також методів автоматичного виявлення змін [6, 7, 11-16]. Сучасні дослідження свідчать, що використання LiDAR-зйомки дозволяє отримувати високоточні цифрові моделі рельєфу та виявляти навіть незначні зміни поверхні місцевості [7]. Дослідники відзначають, що багаточасові цифрові моделі рельєфу, створені за матеріалами LiDAR, забезпечують високу деталізацію змін та дозволяють автоматизувати процес їх виявлення. В останні роки значного поширення набули методи автоматичного виявлення змін на основі алгоритмів глибокого навчання, нейронних мереж та просторово-часового аналізу супутникових зображень. Водночас практична реалізація таких методів потребує використання потужних геоінформаційних платформ, здатних забезпечити інтеграцію різних типів даних та автоматизацію робочих процесів.

Разом з тим, аналіз наукових публікацій показує, що більшість досліджень зосереджена на окремих аспектах процесу створення цифрових карт, таких як обробка даних дистанційного зондування або побудова цифрових моделей рельєфу. Питання комплексної інтеграції різнорідних джерел даних у межах єдиного геоінформаційного середовища розглядаються недостатньо. Також недостатньо уваги приділяється практичним аспектам впровадження таких технологій у діяльність військових підрозділів, зокрема з урахуванням обмежень часу, ресурсів та необхідності забезпечення сумісності геопросторових даних.

Порівняльний аналіз функціональних можливостей різних прикладних програм для роботи з геопросторовими даними показує, що програмне забезпечення ArcGIS найбільш повно відповідає вимогам до створення та оновлення карт змін місцевості, оскільки поєднує можливості редагування векторних карт, роботи з растровими даними, побудови цифрових моделей рельєфу, автоматизованого оформлення картографічних матеріалів та ведення баз геоданих [8-10].

Таким чином, існуючі підходи до створення карт змін місцевості характеризуються фрагментарністю та орієнтацією на окремі технологічні етапи. Недостатньо дослідженим залишається питання побудови цілісної технологічної схеми, яка б забезпечувала ефективну інтеграцію різних джерел геопросторових даних та їх використання в єдиному інформаційному середовищі.

Метою статті є обґрунтування шляхів удосконалення технології створення карт змін місцевості із застосуванням програмного забезпечення ArcGIS та розроблення практичних рекомендацій щодо інтеграції сучасних джерел геоданих, автоматизації процесів обробки та підвищення точності картографічної продукції.

Наукова новизна дослідження полягає у формалізації технологічного процесу створення карт змін місцевості із застосуванням ArcGIS та удосконаленні підходу до інтеграції багатоджерельних геопросторових даних.

Виклад основного матеріалу. Основою удосконаленої технології створення карт змін місцевості є використання електронної чергової карти замість паперових топографічних матеріалів. Усі зміни вносяться безпосередньо до тематичних шарів електронної карти, що дозволяє забезпечити оперативність оновлення та зменшити ймовірність дублювання інформації.

На відміну від паперових карт, електронна чергова карта дозволяє забезпечити багаторазове оновлення інформації без втрати якості та накопичення похибок. Крім того, цифровий формат забезпечує можливість паралельної роботи декількох користувачів, що є важливим у випадку обробки великих обсягів даних. Важливим аспектом є також можливість збереження історії змін, що дозволяє аналізувати динаміку розвитку об'єктів та виконувати ретроспективні дослідження. Використання електронної чергової карти дозволяє реалізувати принцип централізованого зберігання та оновлення геопросторових даних. Це забезпечує узгодженість інформації між різними користувачами та виключає дублювання даних, що є характерним для традиційних підходів. Крім того, цифровий формат карти створює передумови для автоматизації процесів аналізу змін, що значно підвищує ефективність роботи виконавців та знижує ймовірність помилок.

Джерелами інформації про зміни місцевості та розташування об'єктів можуть виступати різноманітні види геопросторових даних, зокрема цифрові або скановані аерофото- та космічні знімки, електронні й паперові картографічні матеріали, що надходять від відповідних установ та організацій, результати геодезичних вимірювань (у тому числі отримані з використанням апаратури, яка забезпечує фіксацію даних на магнітних або оптичних носіях), а також інформація, отримана від розвідувальних підрозділів, спеціалізованих служб, органів місцевого самоврядування та цивільних структур. Таким чином, до процесу оновлення залучається максимально повний обсяг доступних даних різного походження. Внесення змін здійснюється оператором у інтерактивному середовищі редактора карти інструментальної геоінформаційної системи (далі – ГІС) та виконується виключно в межах листів чергової електронної карти, що створена в системі координат WGS-84 та системі цілевказання MGRS [17–18].

Використання великої кількості джерел даних потребує їх узгодження за просторовими, часовими та тематичними характеристиками. Невідповідність координатних систем, різна точність та актуальність даних можуть призводити до виникнення помилок при їх інтеграції. Тому важливим завданням є попередня стандартизація та перевірка якості вхідних даних, що дозволяє забезпечити коректність подальшого аналізу змін місцевості.

Електронні варіанти складального та видавничого оригіналів карти за змістом є тотожними як між собою, так і відповідним тематичним шарам чергової карти, відрізняючись лише особливостями графічного оформлення (зокрема, встановленою кольоровою схемою для окремих об'єктів) та типом носія при виведенні на матеріальну основу. За таких умов процес їх формування може бути оптимізований шляхом копіювання змісту відповідного шару чергової карти до новостворених шарів електронної карти з подальшим виконанням їх стильового оформлення. Подальші етапи технологічного процесу створення карти змін місцевості загалом відповідають підходам, що застосовуються в традиційній технології. Методика внесення змін визначається типом вихідних даних. У випадку використання сканованих або цифрових растрових аерофотознімків, попередньо трансформованих і геоприв'язаних до системи координат векторного шару електронної чергової карти, оновлення здійснюється шляхом автоматизованої або напівавтоматизованої векторизації растру, а також методом цифрування за растровою підкладкою. Процес векторизації виконується для окремих об'єктів або їх фрагментів, виділених на растровому зображенні (наприклад, ділянок відновленої дорожньої мережі). Виявлені зміни вносяться до попередньо сформованого тематичного шару чергової карти, що відповідає векторній моделі території оновлення. Аналогічні підходи застосовуються у випадках, коли джерелом

інформації є скановані паперові картографічні матеріали, на основі яких створено растрові карти для відповідного району робіт.

Якість результатів векторизації безпосередньо визначається характеристиками вихідного зображення, зокрема його роздільною здатністю та рівнем контрастності. Відповідно, використання сучасних засобів редагування карт забезпечує можливість часткової або повної автоматизації процесів збору та нанесення змін за матеріалами аерофотознімання або растровими цифровими картами.

У разі, коли джерелом вихідної інформації є електронна векторна карта, редагування об'єктів (створення, видалення, трансформація геометрії) здійснюється у середовищі геоінформаційних систем із використанням спеціалізованих інструментів редактора. Функціональні можливості редактора дозволяють виконувати як індивідуальні операції редагування, так і обробку об'єктів у груповому режимі, наприклад під час видалення або копіювання наборів елементів, виділених у межах відповідного тематичного шару. Усі зміни, внесені до об'єктів, включаючи їх попередній стан, автоматично фіксуються в системі, що забезпечує можливість відновлення редагованих елементів у разі виникнення помилок або програмно-апаратних збоїв. У процесі створення, модифікації або видалення геометрії об'єктів можуть бути задіяні додаткові режими, спрямовані на підтримку топологічної узгодженості просторових даних, зокрема забезпечення коректності спільних точок, меж і відношень суміжності між об'єктами як в межах одного, так і різних шарів карти. Забезпечення топологічної коректності даних є важливим елементом створення якісної карти змін місцевості. Порушення топології може призвести до помилок у подальшому аналізі, зокрема при визначенні взаємного розташування об'єктів. Тому використання інструментів контролю топології є обов'язковим етапом при редагуванні векторних даних.

Сучасні геоінформаційні програмні засоби забезпечують підтримку не лише геометричної складової просторових даних, але й функціонування реляційних баз даних, у яких зберігаються якісні та кількісні характеристики об'єктів карти у вигляді атрибутивної інформації. У випадках, коли на етапі створення об'єкта відсутня необхідність у введенні атрибутивних даних, програмні засоби редагування дозволяють тимчасово відключити відповідні запити, при цьому обов'язкові параметри автоматично заповнюються значеннями, встановленими за замовчуванням у системі. За потреби геоінформаційні системи надають можливість розширення структури атрибутивних даних шляхом додавання нових характеристик (полів у таблицях атрибутів), а також виконання зв'язку з зовнішніми базами даних. Зазначені можливості є особливо важливими в процесі створення карт змін місцевості, зокрема під час формування підписів об'єктів у випадках використання довідкових джерел або даних, отриманих від різних організацій чи органів місцевого самоврядування. Це, наприклад, актуально при оновленні власних назв населених пунктів. Використання інструментів автоматизованого формування підписів на основі значень атрибутивних таблиць дозволяє суттєво прискорити відповідні процеси, а в окремих випадках - забезпечити їх повну автоматизацію. Крім того, функціональні можливості сучасних ГІС включають засоби генерації вибірок, що створює передумови для автоматизації підготовки формулярів та супровідної документації.

Інтеграція атрибутивної інформації з просторовими даними дозволяє створювати комплексні інформаційні моделі місцевості. Це відкриває можливості для виконання складних аналітичних запитів, зокрема оцінки змін функціонального призначення територій або аналізу інфраструктурних об'єктів. Отже, використання функціональних можливостей сучасного програмного забезпечення геоінформаційних систем для реалізації методики автоматизованого створення карт змін місцевості забезпечує суттєве підвищення ефективності відповідних процесів. Зокрема, це дозволяє:

- трансформувати зміст операцій, пов'язаних із внесенням змін, формуванням підписів та перенесенням інформації між різними варіантами картографічних оригіналів, а також значно скоротити терміни створення оперативного оновлених карт;

- усунути необхідність використання тиражних відбитків топографічних карт у процесі виготовлення одиничних примірників або малих накладів спеціалізованих картографічних продуктів;

- підвищити загальну якість виконання робіт і точність відображення змін місцевості.

Далі доцільно розглянути послідовність виконання робіт зі створення електронної карти району дослідження на основі сканованих картографічних матеріалів відповідно до удосконаленої технологічної схеми (рис. 1).



Рисунок 1 – Удосконалена технологічна схема створення карти змін місцевості із застосуванням інструментальної ГІС

Растрове зображення, завантажене в середовище ArcGIS, саме по собі не може розглядатися як повноцінна растрова карта, оскільки воно не містить просторово-координатної прив'язки. Лише після виконання процедури геоприв'язки таке зображення набуває статусу вимірювального документа та може використовуватися як самостійний інформаційний ресурс або у взаємодії з іншими геопросторовими даними. У середовищі ArcGIS обробка растрових даних здійснюється у внутрішньому форматі RSW. Водночас

растрові дані, представлені в інших форматах (зокрема PCX, BMP, TIFF), можуть бути попередньо перетворені до цього формату для подальшого використання. Існують два основних підходи до завантаження растрових зображень у систему: відкриття їх як окремих документів або інтеграція у вже створений проєкт (векторну, растрову чи комбіновану карту).

Процес геоприв'язки є важливим етапом обробки растрових даних, оскільки визначає точність їх подальшого використання. Вибір методу трансформування залежить від масштабу карти, якості вихідних матеріалів та доступності опорних точок. Помилки на етапі прив'язки можуть накопичуватися та призводити до суттєвих відхилень у визначенні координат об'єктів, що особливо критично при використанні даних у військових цілях.

Важливим аспектом підвищення точності геоприв'язки є також правильний вибір методу трансформування залежно від характеру вихідних даних. Для рівномірно деформованих зображень доцільно використовувати афінні або поліноміальні перетворення, тоді як для складних випадків, пов'язаних із локальними спотвореннями, ефективнішими є методи *spline*-трансформації. Застосування адекватного методу трансформування дозволяє мінімізувати геометричні викривлення та забезпечити відповідність просторового положення об'єктів їх реальному розташуванню.

Окрім цього, необхідно враховувати вплив людського фактора на результати геоприв'язки. Неправильний вибір або неточне встановлення опорних точок може призвести до систематичних помилок, які складно виявити на початкових етапах обробки. У зв'язку з цим доцільним є використання автоматизованих інструментів підбору контрольних точок, а також проведення повторної перевірки результатів із залученням декількох операторів або незалежних джерел даних.

Не менш важливим є забезпечення узгодженості координатних систем та проєкцій при роботі з різними джерелами геопросторової інформації. Використання різних геодезичних датумів або картографічних проєкцій без належної трансформації може призвести до значних просторових зсувів. Тому перед виконанням геоприв'язки необхідно виконувати уніфікацію координатних систем і перевірку параметрів трансформування, що дозволяє забезпечити коректність інтеграції даних у єдиному геоінформаційному середовищі.

Геоприв'язка растрової карти здійснюється в межах документа, що функціонує у визначеній системі координат. Виконання прив'язки растрового зображення можливе за допомогою одного з методів, доступних через інструмент налаштувань (вікно "Властивості" діалогового інтерфейсу "Список растрів") у середовищі ArcGIS. Під час створення великомасштабних планів на основі вихідних картографічних матеріалів доцільним є застосування трансформації за кутовими точками рамки картографічного аркуша. Для дрібномасштабних електронних карт (масштаб дрібніше 1:50 000) з метою підвищення точності відображення растрових даних рекомендується виконувати трансформацію з урахуванням точок деформації (прогину) рамки. У випадках, коли рамка аркуша на растровому зображенні відсутня або збережена частково, трансформація може здійснюватися за опорними точками, що однозначно ідентифікуються на зображенні. Виконання трансформації можливе за наявності достовірних координат щонайменше чотирьох точок, а також за двома точками з використанням режиму масштабування та обертання. Поєднання зазначених підходів дозволяє реалізувати двоетапну процедуру геоприв'язки растрових даних [8, 10].

У випадку формування растрової карти на основі зображення, що складається з окремих фрагментів і не відповідає стандартному поділу на картографічні аркуші (зокрема, при пофрагментному скануванні великого зображення за допомогою вузькоформатного сканера), доцільно застосовувати метод послідовної геоприв'язки окремих растрових фрагментів до вже прив'язаного растрового зображення.

Для формування растрового району з набору окремих растрових зображень необхідно попередньо створити векторну модель району робіт, яка за своїм складом номенклатурних аркушів відповідає структурі растрового покриття, після чого до неї додаються трансформовані растрові дані. Процедура створення векторного району робіт передбачає ініціалізацію карти або плану із заповненням відповідних параметрів у діалогових вікнах,

зокрема типу електронної карти, масштабу, проєкції та системи координат, а також характеристик поділу на аркуші (номенклатури, назв аркушів, координат рамок). Для топографічних карт зі стандартною номенклатурою ці параметри визначаються автоматизовано.

Геоприв'язка растрових зображень, аерофотознімків або космічних знімків у середовищі ArcGIS здійснюється залежно від наявності вихідної інформації про знімок: або за сукупністю опорних точок, або із використанням елементів зовнішнього орієнтування (за умови відомих параметрів знімання, таких як тип знімка та фокусна відстань). За необхідності можливе формування растрового району (фотоплану) шляхом об'єднання окремих попередньо оброблених знімків. Трансформоване растрове зображення автоматично зберігається в системі разом із параметрами виконаного трансформування, що забезпечує його коректне відображення при подальшому додаванні до векторної карти району робіт та автоматичне орієнтування растру [8].

Процес оновлення топографічної карти передбачає внесення змін до окремого тематичного шару електронної карти (у термінології ArcGIS – користувацький шар або карта). Такий шар формується при активній базовій (черговій) електронній карті, причому до нього автоматично імпортується електронний класифікатор базового шару. Зазначений класифікатор у цифровому вигляді містить структуру шарів векторної карти, коди об'єктів і відповідні їм умовні позначення, а також перелік стандартних семантичних характеристик і можливих значень атрибутів. Умовні позначення об'єктів можуть бути реалізовані у двох варіантах: для відображення на екрані та для виведення на друкуючі пристрої або плотери [8, 9].

У середовищі ArcGIS реалізовано електронні класифікатори топографічної інформації для карт і планів масштабів від 1:500 до 1:10 000, а також для карт масштабів від 1:25 000 до 1:1 000 000. У процесі оновлення топографічних карт такі класифікатори використовуються для визначення складу об'єктів та відповідних їм умовних позначень. Під час створення цифрових карт і планів спеціального призначення доцільним є розроблення нових або модифікація існуючих класифікаторів з метою відображення специфічних умовних позначень. У зв'язку з цим у середовищі редактора класифікатора було сформовано електронну базу спеціальних тактичних умовних знаків, що застосовуються у Збройних Силах України [17].

Незважаючи на значні переваги використання ArcGIS, слід враховувати ряд обмежень. До них належать вимоги до обчислювальних ресурсів, необхідність підготовки кваліфікованого персоналу, а також залежність результатів від якості вихідних даних. Крім того, в умовах обмеженого доступу до актуальних даних або їх фрагментарності ефективність запропонованої технології може знижуватися. Це вимагає розроблення підходів до роботи з неповними або застарілими даними.

Висновки. В результаті проведеного дослідження встановлено, що традиційна технологія створення карт змін місцевості, яка базується на використанні паперових топографічних матеріалів і ручного нанесення змін, не відповідає сучасним вимогам щодо оперативності, точності та ефективності обробки геопросторових даних. Її застосування супроводжується значною трудомісткістю, ризиком виникнення помилок та обмеженими можливостями інтеграції різномірних джерел інформації.

Обґрунтовано доцільність переходу до використання геоінформаційних систем, зокрема програмного забезпечення ArcGIS, як базового інструменту створення карт змін місцевості. Встановлено, що застосування електронної чергової карти як основи технологічного процесу дозволяє забезпечити централізоване накопичення, зберігання та оновлення геопросторових даних, а також підвищити узгодженість інформації між різними користувачами. Доведено, що інтеграція різномірних джерел геоданих, таких як аерофотознімки, космічні зображення, матеріали LiDAR-зйомки, електронні карти, геодезичні вимірювання та дані польових спостережень, створює передумови для підвищення повноти та достовірності відображення змін місцевості. Водночас поєднання різних джерел дозволяє компенсувати обмеження кожного з них та забезпечити комплексний аналіз просторової інформації.

Використання автоматизованих і напіваавтоматизованих методів обробки даних у середовищі ArcGIS сприяє суттєвому зменшенню трудомісткості процесів векторизації та нанесення змін, а також підвищенню точності картографічної продукції. При цьому найбільш ефективним є поєднання автоматизованих інструментів із контролем з боку оператора, що забезпечує баланс між швидкістю виконання робіт і якістю результатів.

Узагальнення результатів дослідження дозволило сформулювати удосконалену технологічну схему створення карт змін місцевості, яка включає формування електронної чергової карти, інтеграцію багатоджерельних даних, виконання аналізу змін, їх векторизацію та формування кінцевого картографічного продукту. Запропонована схема відображає взаємозв'язок основних етапів обробки геопросторової інформації та забезпечує можливість їх часткової або повної автоматизації. Практичне значення отриманих результатів полягає у можливості застосування запропонованих підходів для підвищення ефективності оновлення топографічних карт, створення оперативних картографічних матеріалів та вдосконалення системи геопросторової підтримки діяльності військових органів управління. Використання сучасних геоінформаційних технологій дозволяє скоротити час доведення актуальної інформації до підрозділів, підвищити якість геопросторових даних та забезпечити їх відповідність сучасним вимогам.

Перспективи подальших досліджень пов'язані з розвитком методів автоматичного виявлення змін на основі даних дистанційного зондування Землі, впровадженням технологій машинного навчання, а також удосконаленням інтеграції геоінформаційних систем у єдині інформаційно-аналітичні середовища геопросторової підтримки.

ЛІТЕРАТУРА:

1. Лазоренко-Гевель Н., Карпінський Ю., Кінь Д. Особливості створення (оновлення) цифрових топографічних карт для формування основної державної топографічної карти // Сучасні досягнення геодезичної науки та виробництва. 2021. Вип. I (41). С. 113–122. DOI: <https://doi.org/10.33841/1819-1339-1-41-113-122>
2. Коренець О., Підлісецька І., Литвиненко Н., Курач Т. Особливості створення векторної геопросторової бази даних для використання в геоінформаційному порталі Збройних Сил України // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2024. № 4(60). С. 66–71. DOI: <https://doi.org/10.17721/1728-2217.2024.60.66-71>
3. Молочко А., Хірх-Ялан В. Розрахунок коефіцієнтів змін стану місцевості для автоматизації планування робіт по оновленню цифрових топографічних карт // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2017. № 1(36). С. 23–29. DOI: <https://doi.org/10.17721/1728-2217.2017.36.23-29>
4. Belhaj Ali A., Hamza M. H. Updating Traditional 1:50 000 Topographic Maps Using Crowd-Sourced Geodata and Free Sources Satellite Images // Journal of Geographic Information System. 2021. Vol. 13, No. 2. DOI: <https://doi.org/10.4236/jgis.2021.132015>
5. Likhva N. Digital Topographic Mapping in Ukraine: Current State, Challenges, and Development Prospects // European Science. 2025. Vol. 1, No. sge40-01. P. 57–92. DOI: <https://doi.org/10.30890/2709-2313.2025-40-01-014>
6. Wang H., Wu M. Urban change detection of remote sensing images via deep-feature extraction // Scientific Reports. 2025. Vol. 15. Article 21473. DOI: <https://doi.org/10.1038/s41598-025-07252-7>
7. Jung M., Jung J. A scalable method to improve large-scale LiDAR topographic differencing results // Remote Sensing. 2023. Vol. 15, No. 17. P. 4289. DOI: <https://doi.org/10.3390/rs15174289>
8. ArcGIS Pro Documentation. Redlands: Esri Press, 2024. URL: <https://www.esri.com/en-us/arcgis/products/arcgis-pro/resources>
9. ArcGIS Defense Mapping: What's New. 2024. URL: <https://www.esri.com/arcgis-blog/products/defense/defense/whats-new-in-arcgis-defense-mapping-december-2024>
10. Three Key Trends in Imagery and Remote Sensing from Esri UC 2023. 2023. URL: <https://www.esri.com/arcgis-blog/products/arcgis/imagery/three-key-trends-in-imagery-and-remote-sensing-from-esri-uc-2023>
11. Asokan A., Anitha J. Change detection techniques for remote sensing applications: A survey // Earth Science Informatics. 2019. DOI: <https://doi.org/10.1007/s12145-019-00380-5>

12. Bai T., Wang L., Yin D., Sun K., Chen Y. Deep learning for change detection in remote sensing: A review // *Geo-spatial Information Science*. 2023. DOI: <https://doi.org/10.1080/10095020.2022.2085633>
13. Khelifi L., Mignotte M. Deep learning for change detection in remote sensing images // *IEEE Access*. 2020. DOI: <https://doi.org/10.1109/ACCESS.2020.3000973>
14. Wang L., Zhang M., Gao X., Shi W. Advances and challenges in deep learning-based change detection for remote sensing images // *Remote Sensing*. 2024. DOI: <https://doi.org/10.3390/rs16050804>
15. Liu B., Song W., Meng Z., Liu X. Review of land use change detection: A method combining machine learning and bibliometric analysis // *Land*. 2023. DOI: <https://doi.org/10.3390/land12051050>
16. Ali A., Bilal M. A comprehensive review of GIS and remote sensing applications in assessing land use and land cover impacts on groundwater systems // *Environmental Science and Pollution Research*. 2025. DOI: <https://doi.org/10.1007/s11356-025-36787-5>
17. Інструкція зі створення оригіналів спеціальних карт і фотодокументів про місцевість у світовій геодезичній системі WGS-84: затв. наказом командувача Сил підтримки Збройних Сил України від 24.05.2024 № 95а. Київ: КСП ЗСУ, 2024. 110 с.
18. Інструкція зі створення оригіналів топографічних карт у світовій геодезичній системі WGS-84, картографічній проекції Меркатора (UTM), системі цілеуказання MGRS масштабів 1:25 000, 1:50 000, 1:100 000, 1:200 000, 1:500 000, 1:1 000 000: затв. наказом Міністерства оборони України від 18.09.2023 № 563/нм. Київ : КСП ЗСУ, 2023. 213 с.
19. Доктрина геопросторової підтримки Збройних Сил України : затв. наказом начальника Генерального штабу Збройних Сил України від 05.05.2023. Київ : КСП ЗСУ, 2023. 48 с.

REFERENCES:

1. Lazorenko-Hevel, N., Karpinskyi, Yu. and Kin, D. (2021), "Osoblyvosti stvorennia (onovlennia) tsyfrovyykh topohrafichnykh kart dlia formuvannia osnovnoi derzhavnoi topohrafichnoi karty" [Features of creation (updating) of digital topographic maps for the formation of the main state topographic map], *Suchasni dosiahnennia heodezychnoi nauky ta vyrobnytstva*, No. I (41), pp. 113–122. DOI: <https://doi.org/10.33841/1819-1339-1-41-113-122>
2. Korenets, O., Pidlisetska, I., Lytvynenko, N. and Kurach, T. (2024), "Osoblyvosti stvorennia vektornoï heoprostorovoi bazy danykh dlia vykorystannia v heoinformatsiinomu portali Zbroinykh Syl Ukrainy" [Features of creating a vector geospatial database for use in the geoinformation portal of the Armed Forces of Ukraine], *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Viiskovo-spetsialni nauky*, No. 4(60), pp. 66–71. DOI: <https://doi.org/10.17721/1728-2217.2024.60.66-71>
3. Molochko, A. and Khirikh-Yalan, V. (2017), "Rozrakhunok koefitsiientiv zmin stanu mistsevoi dlia avtomatyzatsii planuvannia robit po onovlenniu tsyfrovyykh topohrafichnykh kart" [Calculation of terrain change coefficients for automation of planning works on updating digital topographic maps], *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Viiskovo-spetsialni nauky*, No. 1(36), pp. 23–29. DOI: <https://doi.org/10.17721/1728-2217.2017.36.23-29>
4. Belhaj Ali, A. and Hamza, M.H. (2021), "Updating traditional 1:50,000 topographic maps using crowd-sourced geodata and free satellite imagery", *Journal of Geographic Information System*, Vol. 13, No. 2. DOI: <https://doi.org/10.4236/jgis.2021.132015>
5. Likhva, N. (2025), "Digital topographic mapping in Ukraine: current state, challenges, and development prospects", *European Science*, Vol. 1, No. sge40-01, pp. 57–92. DOI: <https://doi.org/10.30890/2709-2313.2025-40-01-014>
6. Wang, H. and Wu, M. (2025), "Urban change detection of remote sensing images via deep-feature extraction", *Scientific Reports*, Vol. 15, Article 21473. DOI: <https://doi.org/10.1038/s41598-025-07252-7>
7. Jung, M. and Jung, J. (2023), "A scalable method to improve large-scale LiDAR topographic differencing results", *Remote Sensing*, Vol. 15, No. 17, p. 4289. DOI: <https://doi.org/10.3390/rs15174289>
8. Esri (2024), *ArcGIS Pro documentation*, Available at: <https://www.esri.com/en-us/arcgis/products/arcgis-pro/resources>
9. Esri (2024), *ArcGIS Defense Mapping: What's new*, Available at: <https://www.esri.com/arcgis-blog/products/defense/defense/whats-new-in-arcgis-defense-mapping-december-2024>
10. Esri (2023), *Three key trends in imagery and remote sensing from Esri UC 2023*, Available at: <https://www.esri.com/arcgis-blog/products/arcgis/imagery/three-key-trends-in-imagery-and-remote-sensing-from-esri-uc-2023>

11. Asokan, A. and Anitha, J. (2019), "Change detection techniques for remote sensing applications: a survey", *Earth Science Informatics*. DOI: <https://doi.org/10.1007/s12145-019-00380-5>
12. Bai, T., Wang, L., Yin, D., Sun, K. and Chen, Y. (2023), "Deep learning for change detection in remote sensing: a review", *Geo-spatial Information Science*. DOI: <https://doi.org/10.1080/10095020.2022.2085633>
13. Khelifi, L. and Mignotte, M. (2020), "Deep learning for change detection in remote sensing images", *IEEE Access*. DOI: <https://doi.org/10.1109/ACCESS.2020.3000973>
14. Wang, L., Zhang, M., Gao, X. and Shi, W. (2024), "Advances and challenges in deep learning-based change detection for remote sensing images", *Remote Sensing*. DOI: <https://doi.org/10.3390/rs16050804>
15. Liu, B., Song, W., Meng, Z. and Liu, X. (2023), "Review of land use change detection: a method combining machine learning and bibliometric analysis", *Land*. DOI: <https://doi.org/10.3390/land12051050>
16. Ali, A. and Bilal, M. (2025), "A comprehensive review of GIS and remote sensing applications in assessing land use and land cover impacts on groundwater systems", *Environmental Science and Pollution Research*. DOI: <https://doi.org/10.1007/s11356-025-36787-5>
17. Komanduvannia Syl pidtrymky Zbroinykh Syl Ukrainy (2024), *Instruktsiia zi stvorennia oryhinaliv spetsialnykh kart i fotodokumentiv pro mistsevist u svitovii heodezychnii systemi WGS-84* [Instruction on the creation of original special maps and photodocuments of terrain in the WGS-84 geodetic system], Kyiv, 110 p.
18. Ministerstvo oborony Ukrainy (2023), *Instruktsiia zi stvorennia oryhinaliv topografichnykh kart u svitovii heodezychnii systemi WGS-84...* [Instruction on the creation of original topographic maps in the WGS-84 geodetic system...], Kyiv, 213 p.
19. Heneralnyi shtab Zbroinykh Syl Ukrainy (2023), *Doktryna heoprostorovoi pidtrymky Zbroinykh Syl Ukrainy* [Doctrine of geospatial support of the Armed Forces of Ukraine], Kyiv, 48 p.

PhD Korenets O., Lukianchuk A.

IMPROVEMENT OF THE TECHNOLOGY FOR CREATING TERRAIN CHANGE MAPS USING ARCGIS SOFTWARE

The article addresses the issue of improving the technology for creating terrain change maps using geographic information systems, in particular ArcGIS software, under conditions of increasing volumes of geospatial data and growing requirements for the timeliness of geospatial support of military forces. The relevance of the study is обусловлена the need for the prompt updating of topographic information in the context of dynamic changes in the natural and anthropogenic environment, as well as within the framework of modern combat operations characterized by a high degree of situational variability. It has been established that traditional approaches to terrain change mapping, based on the use of paper maps and manual updating, do not meet current requirements in terms of efficiency, accuracy, and the integration of heterogeneous geospatial data sources. The expediency of transitioning to geographic information systems as a foundation for automating data collection, processing, analysis, and updating processes is substantiated.

The methodological basis of the study includes geoinformation modeling, spatial analysis, raster and vector data processing, as well as the analysis of modern approaches to terrain change detection. The effectiveness of integrating multi-source geospatial data, including aerial imagery, satellite images, LiDAR data, digital maps, and geodetic measurements, has been demonstrated. An improved technological framework for terrain change mapping is proposed, which involves the use of a digital base (duty) map, integration of heterogeneous data sources, change analysis, automated vectorization, and the generation of a digital cartographic product. The advantages of using ArcGIS are identified, including increased data processing efficiency, reduced labor intensity, and ensuring the topological consistency of spatial data.

The practical significance of the results lies in their potential application for enhancing the effectiveness of geospatial support for military forces, reducing the time required for updating cartographic information, and improving the quality of decision-making processes.

Keywords: *geographic information system, geospatial data, geospatial support, ArcGIS, LiDAR, terrain change mapping, remote sensing, raster georeferencing, topographic map updating.*

АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА КІБЕРАТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ, ЩО ОБРОБЛЯЮТЬСЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

У статті розглянуто стан забезпечення захищеності критичних інфраструктури а також техносфери в цілому. Як правило виділяють об'єкти чотирьох типів, що відрізняються як ступінь потенційної небезпеки та висунутими вимогами щоб мати змогу захистити їх: об'єкти технічного управління, виробничі об'єкти що є небезпечними, критично значущі об'єкти, стратегічно пріоритетні об'єкти військового призначення, які можуть впливати на стан національної безпеки.

Інформаційні технології дозволяють отримати важливий ефект тонкого регулювання інформаційного впливу залежно від одержувача. Можна виготовити багато варіантів віртуальної реальності, більші того, її (реальність) можна набудовувати на конкретного споживача у момент запиту на одержання.

Показано, що для ефективного функціонування інформаційної системи (ІС) доцільно використовувати у складі системи управління ІР відповідну підсистему забезпечення безпеки з можливістю проведення оцінювання та управління станом захищеності ІС в режимі реального часу та в швидкозмінній природі кібератак.

Сформульовано поняття інформаційна зброя, яка об'єднує в собі електронний і людський аспекти. інформаційних технологій, тому повсякденна робота багатьох автоматизованих систем (АС) і інформаційних систем (ІС) має життєве важливе значення. З іншого боку, головним стратегічним об'єктом впливу інформаційної зброї залишаються люди. В інформаційних системах повинна бути можливість, виявлення та запобігання вторгнень, які реалізуються множиною різнонаправлених за фізичним змістом атак. З метою здійснення такої можливості система захисту інформації (СЗІ) повинна мати у складі систему управління подіями інформаційної безпеки.

Ключові слова: інформаційні ресурси, інформаційна система, кіберзагроза, інформаційна зброя, комбінації кібератак, система захисту інформації.

Вступ та постановка проблеми.

Сучасні об'єкти критичної інфраструктури функціонують як складні технічні системи, що відзначаються багаторівневою структурою, тісною взаємодією елементів та інтеграцією кіберфізичних компонентів. Їх робота відбувається в умовах постійної невизначеності та динамічного зростання загроз, серед яких вагоме місце посідають кіберінциденти, техногенні аварії, природні явища та помилки персоналу. Така сукупність факторів ускладнює процес забезпечення їх надійності та потребує застосування комплексних підходів до захисту, що поєднують організаційні та технічні рішення.

Рівень захищеності зазначених систем визначається їх здатністю протистояти переходу окремих елементів у критичні стани та запобігати розвитку руйнівних сценаріїв під час експлуатації. Водночас досягнення необхідного рівня безпеки ускладнюється низкою чинників невизначеності, зокрема нестабільністю параметрів середовища функціонування, обмеженістю достовірної інформації про внутрішні процеси, а також недосконалістю засобів контролю і математичного опису поведінки систем. Додатковий вплив мають експлуатаційні навантаження та зміна характеристик ключових елементів упродовж життєвого циклу.

У структурі техносфери прийнято виокремлювати декілька категорій об'єктів залежно від рівня потенційної небезпеки та вимог до їх захисту. До них належать об'єкти технічного регулювання, небезпечні виробничі комплекси, критично важливі об'єкти, що підлягають

категоризації в межах системи критичної інфраструктури, а також стратегічні об'єкти військового призначення. Надійність функціонування останніх має особливе значення для підтримання обороноздатності та загального рівня національної безпеки.

Значення критичної інфраструктури для держави визначається тим, що вона забезпечує безперервність ключових процесів у таких сферах, як енергетика, транспорт, зв'язок, медицина та інші життєво важливі галузі. Порушення роботи відповідних систем може мати масштабні наслідки — від економічних втрат до соціальної нестабільності та виникнення загроз безпеці держави і населення [1].

В умовах триваючої збройної агресії проти України особливої актуальності набуває питання стійкості функціонування таких об'єктів. Противник, поряд із застосуванням традиційних засобів ураження, активно використовує інструменти кіберпростору для впливу на системи управління та дестабілізації роботи вразливих елементів інфраструктури. При цьому навіть впровадження сучасних заходів захисту не гарантує повної безпеки, оскільки цифровізація та інтеграція систем у єдине інформаційне середовище створюють нові вразливості.

Таким чином, забезпечення надійного захисту складних технічних систем, що входять до складу критичної інфраструктури, стає одним із ключових завдань сучасного етапу розвитку держави. Це потребує перегляду існуючих підходів до оцінювання ризиків, підвищення рівня адаптивності систем безпеки та впровадження інноваційних методів протидії як фізичним, так і кіберзагрозам [2].

Аналіз досліджень та публікацій.

Аналіз ведення сучасних гібридних війн у світі та проведення кібернетичних операцій, свідчить про розвиток форм, способів та методів, які застосовуються для проведення кібератак на систему управління IP та IC. В ході попередніх досліджень [1] визначено, що для ефективного функціонування IC доцільно використовувати у складі системи управління IP відповідну підсистему забезпечення безпеки з можливістю проведення оцінювання та управління станом захищеності IC в режимі реального часу та в умовах постійних змін в природі кібератак.

До основних особливостей відносяться: різна розмірність мереж, територіально рознесені складові IC, вихід елементів IC за межі контрольованої зони. Зазначені особливості IC роблять їх привабливими з точки зору організації та впровадження швидкої взаємодії між територіально-рознесеними підрозділами державних установ, однак, можуть бути використані зловмисниками для здійснення кібератак з метою вчинення деструктивних дій. Звичайно, функціонування IC в кіберпросторі залежить від множини природних, техногенних та антропогенних чинників, які можуть нашкодити процесу передачі інформації. Але найбільшу шкоду IC може завдати навмисні атаки та вплив на існуючі вразливості системи безпеки, що здійснюються на різних рівнях базової еталонної моделі взаємодії відкритих систем.

Інформаційні системи описуються в працях вітчизняних та закордонних вчених: Субача І.Ю., Бурячка В.Л., Гнатюка С.О., Корченко О.Г., Юдіна О.К., Бучика С.С., Євсєєва С.П., Дудикевича В.Б., Казмирчук С.В., Albers, O. T. Ptaceka, G. Elmasry, P. Camp та інших.

Водночас, основними вимогами, які пред'являються до захищеності IP в IC є: робота в режимі реального часу; врахування загроз характерних інформаційно-телекомунікаційним системам; можливість застосування в системах з високою динамікою зміни топології; децентралізація управління та наявність ієрархічно-розподільної структури; мінімальне завантаження мережі службовою інформацією.

Виходячи з вказаного, одним з найважливіших питань, які необхідно вирішити в процесі експлуатації IC є гарантування інформаційної, програмної та апаратної безпеки, які визначають ступінь захищеності інформаційних ресурсів від вразливостей та кібератак.

На сьогодні спостерігається невідповідність між вказаними можливостями існуючих методів управління станом захищеності IC та вимогами до методів управління станом захищеності IP в IC. Як наслідок вирішення питань безпеки в IC та управління станом захищеності інформаційних систем від вразливостей та кібератак є актуальним і потребує подальших досліджень.

Мета статті є визначення ефективності захищеності інформаційних ресурсів на основі аналізу, вразливостей від зовнішніх та внутрішніх кібератак.

Викладення основного матеріалу.

В умовах функціонування системи кібербезпеки в різних режимах особливої ваги набуває забезпечення захищеності інформаційних ресурсів (ІР) у кіберпросторі. Це, у свою чергу, обумовлює необхідність підвищення ефективності системи управління (СУ) та відповідної підсистеми забезпечення безпеки (ПЗБ), які мають забезпечувати своєчасне виявлення і коректну інтерпретацію впливу кіберзагроз та несанкціонованих втручань. Така оцінка здійснюється на основі аналізу змін сукупності окремих показників, що характеризують рівень захищеності інформаційних ресурсів.

При цьому ключовим аспектом процесу прийняття управлінських рішень у підсистемі кібербезпеки є встановлення об'єктивного ступеня впливу конкретних загроз на загальний стан безпеки інформаційних ресурсів. Саме точність та обґрунтованість такої оцінки визначає ефективність реагування системи на дестабілізуючі фактори.

Одним з важливих факторів розвитку інформаційних технологій є глобальне об'єднання програмних продуктів, технічних засобів та мереж передачі інформації. Таке поєднання надає сучасним технічним засобам нові можливості, зручності у користуванні та керуванні. Проте зворотною стороною таких переваг є додаткові вразливості програмно-керованих технічних засобів. Крім відомих технічних каналів витоку інформації слід враховувати загрози несанкціонованого віддаленого доступу до технічних засобів, наявні в них уразливості та незадекларовані функції, а також можливості впровадження шкідливого програмного забезпечення та програмних закладок. Зазначені вразливості можуть "експлуатуватись" з метою порушення конфіденційності, цілісності, достовірності та доступності інформації, яка обробляється технічними засобами, а також порушення конфіденційності інформації, яка циркулює в місцях їх встановлення.

Сучасне робоче місце в загальному випадку обладнане рядом технічних засобів, які перейшли від "звичайних" технічних засобів до програмно-керованих технічних засобів. Технічні засоби зазначених систем мають у своєму складі модулі або інтерфейси передачі даних, які у певних умов можуть бути використані в якості каналів несанкціонованого керування технічними засобами. Використання програмно-керованих технічних засобів, які мають у своєму складі модулі та інтерфейси передачі даних, потребує вжиття додаткових заходів із захисту інформації, враховуючи сучасні загрози [3].

Порушення захищеності при використанні ІС розподіляються на такі види:

- несанкціонований доступ (НСД) до роботи автоматизованих систем (АС), мереж, баз даних;
- створення руйнівного програмного забезпечення (ПЗ) або технічних засобів, та їх збут або розповсюдження;
- несанкціонований збут або поширення інформації з обмеженим доступом, яка зберігається в АС, мережах або на носіях такої інформації;
- злочини, що здійснені шляхом використання ІС та інформаційної зброї, як засобу досягнення злочинної мети тощо[4].

Поняття інформаційна зброя об'єднує в собі електронний і людський аспекти. З одного боку, суспільство все більше підпадає у залежність від інформаційних технологій, тому повсякденна робота багатьох АС і ІС має життєво важливе значення. З іншого боку, головним стратегічним об'єктом впливу інформаційної зброї залишаються люди. Основними завданнями застосування інформаційної зброї у мережі є:

- порушення цілісності службової та доступної інформації;
- пошкодження систем захисту;
- обмеження порядку доступу до ресурсу законних користувачів, спотворення роботи технічних засобів, комп'ютерних систем.

Види інформаційної зброї у глобальних мережах [5]:

- деструктивні програми типу "комп'ютерні віруси" – програми, що мають здібності до самовідтворення, і, як правило, здатні здійснювати дії, які можуть порушити роботу системи

і/або викликати порушення політики безпеки. Мають можливість впроваджуватися у програми, передаватися лініями зв'язку, мережами передачі даних, виводити з ладу системи керування і т.д.;

- деструктивні програми типу "троянський кінь" – програми, які працюють у звичному режимі, окрім виконання функцій документування, можуть здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми;

- засоби подавлення інформаційного обміну та фальсифікації в ІС, передусім, військового та державного призначення;

- засоби блокування тестових програм;

Ці засоби надають можливості супротивнику завдавати інформаційних ударів. Наприклад, порушити комунікації, паралізувати телефонну мережу, заплутати фінанси, порушити функціонування космічних апаратів.

Універсальність, прихованість, широкий спектр форм програмно-апаратної реалізації, характеризують інформаційну зброю як надзвичайно небезпечну: вона легко маскується під засоби захисту, як безпека інтелектуальної власності. Вона також дозволяє навіть проводити наступальні дії анонімно, без оголошення війни.

З метою запобігання або нейтралізації наслідків застосування інформаційної зброї необхідно вжити наступних заходів [5, 6]:

- збереження матеріально-технічних об'єктів, що є базовою основою ІР;
- забезпечення стабільного функціонування банків і баз даних;
- захист інформації від НСД, перекручування або знищення;
- збереження якості інформації (своєчасності, точності, повноти і необхідної доступності).

Атаки здійснюються з метою порушення конфіденційності, цілісності та працездатності ІР, що зберігається та оброблюється в інформаційних системах (ІС). З цією метою, як свідчить досвід застосування, використовують вразливості ІС, тобто неспроможність системи протистояти певній загрозі або сукупності загроз [5,6,7]. Загальна структура реалізації атак представлена на рис. 1.

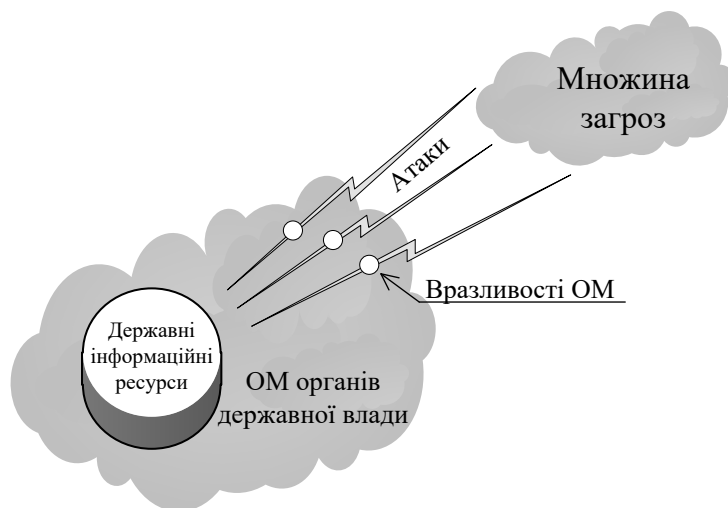


Рисунок 1 – Загальна структура реалізації атак

Для одержання інформації про можливі атаки на інформацію, вимога щодо захисту якої встановлена законодавством, інформаційні наслідки їхнього прояву, а також виявлення найбільш небезпечних кібератак використовують модель поведінки інформаційних систем та ІС при впливі на них кібератак (рис. 2), де КБА – комбінації кібератак, S – підмножина станів ІС, ВФ – виконання функцій ІР, ІНПІС – інтенсивності переходів ІС, МСЗІР – модель системи захисту інформаційних ресурсів [8].

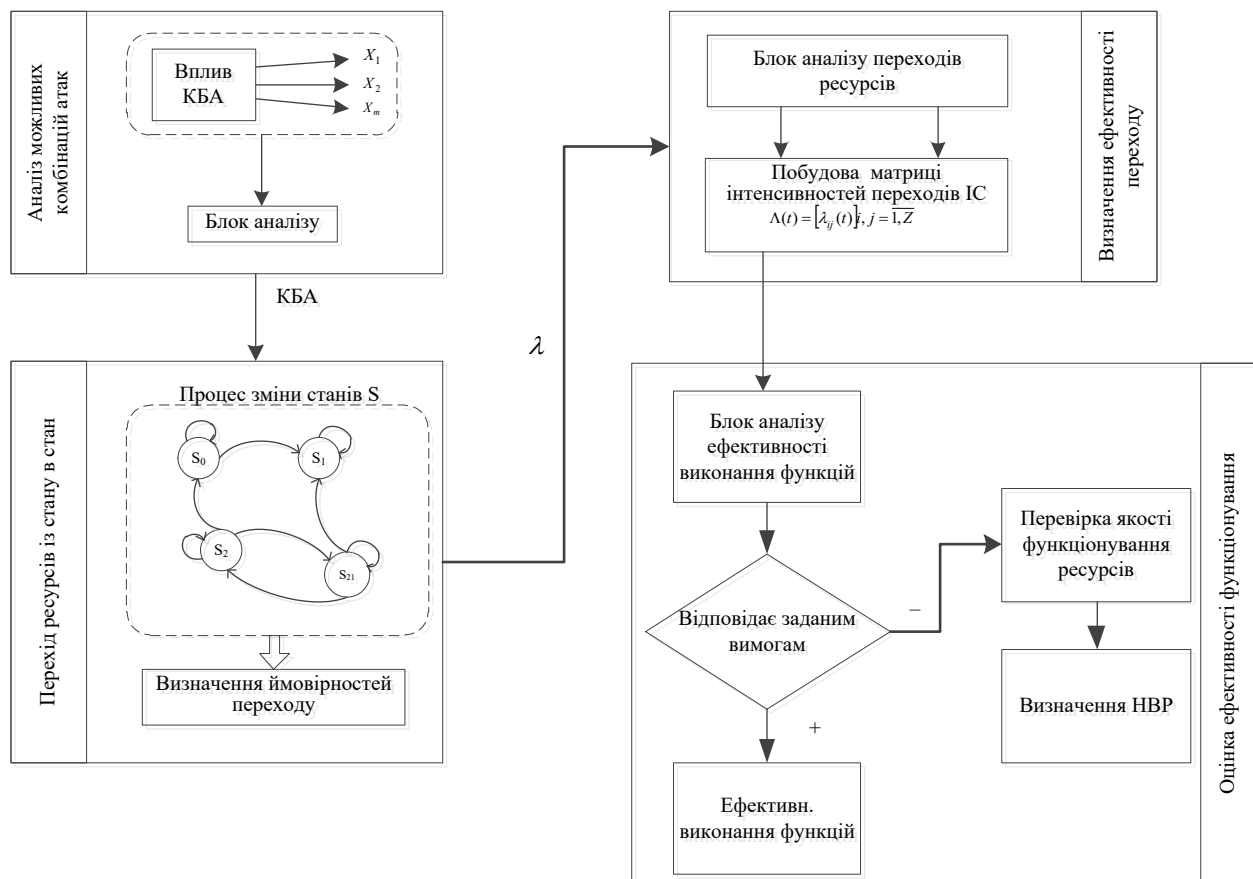


Рисунок 2 – Модель поведінки системи при впливі атак

Більш детально доцільно розглянути сучасні бази даних, що містять описи типових вразливостей і загроз, які взаємодіють між собою на різних рівнях моделі OSI model.

У межах цієї моделі взаємодія між системами фактично реалізується через дві взаємопов'язані схеми – горизонтальну та вертикальну:

- у горизонтальній (розподіленій) моделі розглядається безпосередній обмін даними між однойменними рівнями різних кінцевих вузлів (хостів). Для забезпечення такої взаємодії необхідною умовою є використання однакових протоколів на відповідному рівні в обох системах;

- у вертикальній (ієрархічній) моделі описується взаємодія між сусідніми рівнями в межах однієї системи із застосуванням відповідних інтерфейсів. При цьому кожен рівень надає сервіси вищому рівню та використовує можливості нижчого. Виняток становлять крайні рівні: прикладний рівень орієнтований на взаємодію з користувачем, тоді як фізичний рівень не використовує сервіси інших рівнів.

Перші випадки інформаційної безпеки, що офіційно мають місце в базах даних вразливостей, з'явилися в 1988 році [8, 9]. З тих пір ведеться постійний пошук вразливостей та їх реєстрація як в рамках відкритих проєктів, так і приватними компаніями, науково-дослідними інститутами та дослідниками. Серед лідерів детектування вразливостей слід згадати нижче перелічених розробників відповідних баз даних вразливостей: United State Computer Emergency Readiness Team та база Vulnerability Notes Database (VND); компанія MITRE та її база вразливостей Common Vulnerabilities and Exposures (CVE) [9]; компанія IBM та база вразливостей X-Force [10]; National Institute of Standards and Technology та база National Vulnerabilities Database (NVD) [11].

Розглянемо деякі з перелічених баз вразливостей:

- CVE – довідково-пошукова система посилань вразливостей. Головною складовою системи є CVE ідентифікатори – унікальні ідентифікатори, які присвоюються кожній відомій вразливості в сфері інформаційної безпеки. Система включає в себе понад 98000 записів про

окремі вразливості [10]. Основна різниця в тому, що вона є найбільшою, повною та систематизованою. До основних складових структури записів вразливостей відносяться:

1) статус – в цьому полі може знаходитись або значення Entry (Запис переврений), або значення Candidate (вразливість, яка ще не перевірялась);

2) фаза – це поле включає значення етапу удосконалення вразливості, а також дату присвоєння зазначеного етапу. Може приймати наступні значення: Proposed – фаза пропозиції вразливості; Interim – проміжна фаза вразливості; Modified – фаза модифікації вразливості; Assigned – фаза встановлення вразливості;

3) опис – поле включає в себе опис вразливості;

4) посилання – тут знаходяться посилання на інші джерела із зазначенням точної адреси інтернет-ресурсу опису вразливості та ідентифікатора джерела;

5) голоси – це імена членів голосування, які прийняли рішення щодо внесення вразливості в базу;

6) коментарі – вноситься данні про автора коментаря та самий текстовий зміст.

Додаткова в елементах записів вразливостей може знаходитись тип вразливості, ім'я та ідентифікатор. Ім'я вразливості має формат "CVE-YYYYNNNN", де YYYY – це рік виявлення вразливості, а NNNN – її порядковий номер.

До недоліків бази CVE входить – відсутність певного механізму опису відношення вразливостей до конкретних продуктів, а також присвоєння вразливостям метрик і визначення ступеня небезпеки [12].

Національна база даних вразливостей США (NVD) – сховище даних вразливостей, засноване на стандартах протоколу автоматизації змісту безпеки. База NVD об'єднала в собі опис вразливостей, назви програмного забезпечення з цими вразливостями і оцінки небезпеки вразливостей. За станом на 2017 рік база даних вразливостей NVD біля 70000 записів вразливостей [13].

Структура запису вразливості в базі NVD є розширеною формою подання записи в базі CVE, за рахунок наявності наступних полів: конфігурація вразливих продуктів з урахуванням залежностей; список вразливих продуктів; показники, що характеризують вразливість в форматі "Загальної системи оцінки вразливостей"; тип доступу для реалізації вразливості. Встановлено, що 82,77% вразливостей належать додаткам, 12,28% – операційним системам і 3,59% – апаратному забезпеченню.

Важливою особливістю бази NVD від є застосування Common Platform Enumeration, як одного з кращих словників продуктів серед існуючих аналогів завдяки значного числа записів та уніфікованого формату імен програмно-апаратного забезпечення [11]. Однак у даного формату представлення записів є недоліки:

– неоднозначність різних полів формату;

– використання не всіх існуючих записів даного словника базою NVD.

База вразливостей OSVDB організована для групи фахівців в області безпеки. Мета проекту полягає в тому, щоб забезпечити точну, дана база містить деталізовану, інформацію про вразливість систем забезпечення безпеки. В ній знаходиться понад 110 000 вразливостей [13].

Як правило, реалізація внутрішньосегментної (внутрішньої) атаки є значно простішою порівняно з міжсегментною (зовнішньою). Водночас зовнішні атаки становлять більшу загрозу, ніж внутрішні. Це пояснюється тим, що під час їх здійснення об'єкт впливу та зловмисник можуть перебувати на значній відстані один від одного, що ускладнює застосування ефективних заходів захисту та протидії.

Під порушенням безпеки розуміється несанкціонований доступ до інформаційної системи, який виникає внаслідок дій, що суперечать встановленій політиці безпеки або обходять засоби захисту інформації. Атаку доцільно трактувати як спробу реалізації певної загрози. У свою чергу, загроза — це будь-які умови чи події, здатні призвести до порушення нормального функціонування інформаційних, програмних або апаратних компонентів системи, а також спричинити збитки чи інші негативні наслідки [13, 14].

Розглянемо нині існуючі типи атак на ІС обробки ІР (таблиця 1), та їх параметри [43, 44].

Таблиця 1 – Класифікація атак

Ознака атаки	Тип атаки	Характеристики атаки
За характером впливу	пасивні	Атаки, які безпосередньо не впливають на роботу системи, але можуть нашкодити її політиці безпеки. Складно виявити. Після атаки не залишається не має слідів. Приклад: здійснення прослуховування зв'язку в мережі.
	активні	Атаки, що безпосередньо шкодять роботі системи (зміна конфігурації ІС, порушення працездатності тощо) і порушують прийняту в ній політику безпеки. Як правило всі типи віддалених атак є активними. Необхідно обов'язково виявляти, так як після здійснення атаки в системі відбуваються значні зміни.
За метою впливу	порушення конфіденційності	Перехоплення інформації. Приклад: прослуховування каналу в мережі.
	порушення цілісності	Спотворена інформація. Прикл.: застосування помилкового об'єкта в ІС.
	порушення доступності	Не відбувається НСД (цілісність не порушена), проте доступ до легальних користувачів неможливий. Приклад: відмова в обслуговуванні зареєстрованих користувачів.
За умовою початку здійснення впливу	атака на запит від об'єкта, що атакується	У разі запиту атакуючий очікує передачі від потенційної мети атаки запиту певного типу, який і буде умовою початку здійснення впливу. Ініціатором здійснення початку атаки є об'єкт, що атакується. Приклад: DNS- і ARP-запити в стеці TCP / IP.
	атака по настанню події, що очікується на об'єкті	Якщо подія має місце, атакуючий робить постійне спостереження за станом операційної системи віддаленого об'єкта атаки і при виникненні певних обставин в цій системі починаються неполадки. Ініціатором здійснення початку атаки є об'єкт, на який здійснюється атака. Приклад: переривання сеансу роботи користувача з сервером в мережових операційних системах без видачі команди LOGOUT.
	безумовна атака	У разі безумовної атаки початок її здійснюється по відношенню до мети атаки, тобто атака зрозпочинається негайно і незалежно від стану системи об'єкта атаки. Ініціатором здійснення початку атаки є атакуючий.
За наявністю зворотного зв'язку з об'єктом, який атакується	зі зворотним зв'язком	Атака із зворотним зв'язком – атака, за час якої атакуючий отримує відповіді від об'єкта на частину своїх дій. Це необхідно для продовження атаки і/або здійснювати її більш ефективно, реагуючи на зміни, що відбуваються в системі.
	без зворотного зв'язку (односпрямова на атака)	Атака без зворотного зв'язку – атака, яка відбувається без реакції на поведінку системи, що атакується. Приклад: відмова в обслуговуванні.
За кількістю атакуючих	розподілена	Атака, вироблена двома чи більше атакуючими на одну інформаційну систему (ІС), об'єднаними певним задумом та часом початку здійснення.
	нерозподілена	Нерозподілена атака проводиться одним атакуючим.

Ця послідовність параметрів з'єднання включає такі характеристики: тривалість з'єднання, тип протоколу, послуга мережі, обсяг даних у повідомленні (байти), стан з'єднання, кількість термінових пакетів, спроби встановлення з'єднання тощо.

Як правило атаки спрямовуються на інформаційні ресурси (ІР) у вигляді повідомлень – текстових даних, аудіо- або відеоматеріалів. Структура такого повідомлення містить передзаголовок, заголовок, контрольну суму, текст повідомлення та його завершення. Ці елементи аналізуються системою виявлення атак для ідентифікації потенційних загроз.

Зазначені типи атак здатні впливати на різні аспекти функціонування інформаційної системи (ІС), зокрема на управління ресурсами системи, розмежування доступу користувачів до даних чи функцій, характеристики енергоспоживання, обмін інформаційними пакетами, доступ до кодування та управління даними загалом.

Висновок/ Проведений аналіз атак та вразливостей на ІР, що обробляються в ІС показав різноманітність варіантів будови баз вразливостей. Кожен з варіантів має свої переваги та недоліки, але найбільш важливий напрямом-орієнтованість сучасних баз вразливостей для застосування в експертних системах. Сучасні інформаційні системи, які обробляють ІР, мають велику кількість зовнішніх і внутрішніх вразливостей, а реалізація їх відбувається за завдяки використанню множини різнонаправлених атак. Поширення вразливостей окремого вузла ІС може викликати появу додаткових загроз безпеці ІР, що в ній обробляються. Таким чином для визначення множини параметрів при оцінюванні захищеності ІР в цілому та виявлення нових вразливостей, доцільно забезпечити функціонування системи управління інформаційної безпеки з урахуванням вищезазначених вимог, параметрів даних та характеристичних особливостей сучасних системи управління ІР.

Важливими складовими є дотримання принципів управління життєвим циклом інформаційних систем, стандартизація та посилена увага до кібербезпеки. Подальший успіх залежить від успішної інтеграції систем, покращення співдії між різними елементами, а також нарощування кадрового потенціалу, що дозволить забезпечити суттєве збільшення рівня ефективності та безпеки функціонування систем.

ЛІТЕРАТУРА:

1. Сальник С.В., Сторчак А.С., Герасімов К.К. Аналіз функціонування систем управління державними інформаційними ресурсами. Щоквартальний науково-технічний журнал Наука і техніка Повітряних Сил Збройних Сил України. 2019. Вип. 2(35). С.47-54.
2. Субач І.Ю., Фесьоха В.В., Голуб О.О., Криховецький В.В. Нечітке визначення "типовості" статистичної поведінки у інформаційно-телекомунікаційних мережах. Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил : зб. матеріалів ХІ наук.-практ. конф., 8-9 лист. 2018 р. Київ : ВІТІ ім. Героїв Крут, 2018. С. 213.
3. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України" від 17 вересня 2021 року № 473/2021 URL: <https://zakon.rada.gov.ua/laws/show/473/2021#Text> (дата звернення: 23.06.2023).
4. Лепіх Я.І., Гордієнко Ю.О., Дзядевич С.В., Дружинін А.О., Євтух А.А., Ленков С.В., Мельник В.Г., Проценко В.О., Романов В.О. Мікроелектронні датчики нового покоління для інтелектуальних систем. монографія. Одеса: "Астропринт", 2011. 92 с.
5. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних Реєстрація, зберігання і обробка даних. 2015. Вип. 17(2). С. 39-46.
6. Горбенко В.І., Картавих В.Ю., Субач І.Ю. Модель моніторингу домену управління інформаційної мережі військового призначення Системи обробки інформації. 2013. Вип. 4(111). С. 118-122.
7. Tewari N., Bhardwaj A. Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks // International Journal of Scientific & Engineering Research. 2013. Vol. 4, № 5. P. 348 – 353.
8. Xiao P., He J., Chen Y., Fu Y. A new trusted roaming protocol in wireless mesh networks // International Journal of Sensor Networks. 2013. Vol. 14, Issue 2. P. 109 – 119. doi: 10.1504/IJSNET.2013.056610 89
9. Офіційний сайт Common Vulnerabilities and Exposures. Режим доступу: <http://cve.mitre.org>
10. Офіційний сайт National Vulnerabilities Database. Режим доступу: <http://nvd.nist.gov>

11. Офіційний сайт United States Computer Emergency Readiness Team. Режим доступу: <http://www.us-cert.gov>
12. Zhang Y., Lee W., Huang Y. Intrusion detection techniques for mobile wireless networks. *Wireless Networks Journal (ACM WINET)*. 2003. № 9(5). P. 545–556.
13. Janakiraman R., Waldvogel M., Zhang Qi. A peer-to-peer approach to network intrusion detection and prevention. *Enabling Technologies: Infrastructure for Collaborative Enterprises*. 2003. P. 226–231, DOI:10.1109/ENABL. 2003.1231412
14. Alshboul Y., Streff K., Analyzing Information Security Model for Small-Medium Sized Businesses, Twenty-first Americas Conference on Information Systems, Puerto Rico, 2015.
15. Safa N.S., Solms R.V., Furnell S. Information security policy compliance model in organizations. *Computers & Security*. 2016. Vol. 56. P. 70-82. DOI:10.1016/j.cose.2015.10.006

REFERENCES:

1. Salnyk S.V., Storchak A.S., Herasimov K.K. (2019) Analiz funktsionuvannia system upravlinnia derzhavnymy informatsiynymy resursamy [Analysis of the functioning of state information resource management systems]. *Shchokvartalnyi naukovo-tekhnichnyi zhurnal Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy*. Vyp. 2(35). S.47-54. (in Ukrainian)
2. Subach I.Yu, Fesokha V.V., Holub O.O, Krykhovetskyi V.V. (2018) Nechitke vyznachennia "typovosti" statystychnoi povedinky u informatsiino-telekomunikatsiinykh merezhakh [Unclear definition of the "typicality" of statistical behavior in information and telecommunications networks.]. *Priorytetni napriamky rozvytku telekomunikatsiinykh system ta merezh spetsialnoho pryznachennia. Zastosuvannia pidrozdiliv, kompleksiv, zasobiv zviazku ta avtomatyzatsii v operatsii Obiednanykh syl : zb. materialiv XI nauk.-prakt. konf., 8-9 lyst. 2018 r. Kyiv : VITI im. Heroiv Krut*, 2018. 213. (in Ukrainian)
3. Ukaz Prezydenta Ukrainy (2021) "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehichnyi oboronnyi biuletyn Ukrainy" № 473/2021 Available at: <https://zakon.rada.gov.ua/laws/show/473/2021#Text> . (accessed 23 January 2023). (in Ukrainian)
4. Lepikh Ya.I., Hordiienko Yu.O, Dziadevych S.V., Druzhynin A.O., Yevtukh A.A., Lienkov S.V., Melnyk V.H., Protsenko V.O., Romanov V.O. (2011). *Mikroelektronni datchyky novoho pokolinnia dlia intelektualnykh system*. [New generation microelectronic sensors for intelligent systems.] Odesa: "Astroprint". (in Ukrainian)
5. Korpan Ya.V. (2015) Klasyfikatsiia zahroz informatsiinii bezpetsi v kompiuternykh systemakh pry viddalenii obrobtisi danykh Reiestratsiia, zberihannia i obrobka danykh [Classification of threats to information security in computer systems during remote data processing. Data registration, storage and processing.]. 2015. Vyp. 17(2). S. 39-46.
6. Horbenko V.I., Kartavykh V.Yu., Subach I.Yu.(2013) Model monitorynhu domenu upravlinnia informatsiinoi merezhi viiskovoho pryznachennia [Military information network control domain monitoring model] *Systemy obrobky informatsii*. Vyp. 4(111). 118-122.
7. Tewari N., Bhardwaj A. (2013) Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks *International Journal of Scientific & Engineering Research*. Vol. 4, 5. 348-353. (in English)
8. Xiao P., He J., Chen Y., Fu Y. A(2013) A new trusted roaming protocol in wireless mesh networks *.International Journal of Sensor Networks*,14, Issue 2. P. 109 -119. (in English) [https:// doi.org/10.1504/IJSNET.2013.056610](https://doi.org/10.1504/IJSNET.2013.056610) 89
9. Ofitsiinyi sait Common Vulnerabilities and Exposures. Rezhym dostupu: <http://cve.mitre.org>(in English)
10. Ofitsiinyi sait National Vulnerabilities Database. Rezhym dostupu: <http://nvd.nist.gov>(in English)
11. Ofitsiinyi sait United States Computer Emergency Readiness Team. Rezhym dostupu: <http://www.us-cert.gov>(in English)
12. Zhang Y., Lee W., Huang Y. (2003) Intrusion detection techniques for mobile wireless networks. *Wireless Networks Journal (ACM WINET)*. 2003. № 9(5). P. 545–556. (in English)
13. Janakiraman R., Waldvogel M., Zhang Qi. (2003) A peer-to-peer approach to network intrusion detection and prevention. *Enabling Technologies: Infrastructure for Collaborative Enterprises*. . P. 226–231, DOI:10.1109/ENABL. 2003.1231412 (in English)
14. Alshboul Y., Streff K.(2015), Analyzing Information Security Model for Small-Medium Sized Businesses, Twenty-first Americas Conference on Information Systems, Puerto Rico (in English)
15. Safa N.S., Solms R.V., Furnell S.(2016) Information security policy compliance model in organizations. *Computers & Security*. 2016. Vol. 56. P. 70-82. DOI:10.1016/j.cose.2015.10.006 (in English)

**ANALYSIS OF VULNERABILITIES AND CYBERATTACKS ON INFORMATION
RESOURCES PROCESSED WITHIN INFORMATION SYSTEMS**

The article examines the state of security across critical infrastructure and the technosphere as a whole. Typically, four types of facilities are distinguished based on their degree of potential dangers and specific protection requirements: technical control facilities, hazardous industrial facilities, critically significant facilities, and strategically priority military facilities able to affect national security.

Information technologies provide a crucial effect by allowing the precise regulation of informational influence based on the recipient. Multiple variations of virtual reality can be generated; moreover, this environment can be dynamically adapted to the needs of a specific user at the very moment they submit a request.

It is demonstrated that for the effective operation of an information system (IS), an appropriate security assurance subsystem should be integrated into the information resource (IR) management system. This subsystem must be capable of assessing and managing the IS security condition in real time, accounting for the rapidly evolving nature of cyberattacks.

The paper formulates the concept of information weaponry, which combines the electronic and human aspects of information technologies. Consequently, the continuous daily operation of various automated systems (AS) and information systems (IS) is of critical importance. Conversely, humans remain the primary strategic target of information weapons. Information systems must possess the capability to detect and prevent intrusions which are realized by a multitude of attacks of different types in terms of their physical nature. To facilitate this, the information security system (ISS) must incorporate a security information and event management (SIEM) system.

Keywords: information resources, information system, cyber threat, information weapons, cyberattack combinations, information security system.

док. техн. наук, проф. **Богданович В.Ю.** (ЦНДІ ЗСУ)
к.в.н, ст.д. **Цибізов А.Л.** (ЦНДІ ЗСУ)
к.юр.н, доц. **Гуляк О.В.** (АО "Українська оборонна промисловість")

DOI: <https://doi.org/10.17721/2519-481X/2025/89-06>

СПРОЩЕНА МЕТОДИКА ОБҐРУНТУВАННЯ РЕКОМЕНДАЦІЙ ЩОДО КОРИГУВАННЯ ПОЛІТИКИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ ЗА РЕЗУЛЬТАТАМИ СТРАТЕГІЧНОГО АНАЛІЗУ ГЕОПОЛІТИЧНОЇ ТА ВІЙСЬКОВОЇ МОГУТНОСТІ НЕДРУЖНІХ ДЕРЖАВ

Стаття присвячена вивченню спрощеної методики обґрунтування рекомендацій щодо коригування політики національної безпеки за результатами стратегічного аналізу факторів геополітичної та військової могутності недружніх держав, яка містить дві основні складові, що дають змогу обґрунтовувати рекомендації щодо внесення змін у Стратегію національної безпеки та у Стратегію розвитку оборонно-промислового комплексу України. Мета статті-розроблення спрощеної методики обґрунтування рекомендацій щодо коригування політики національної безпеки держави за результатами стратегічного аналізу геополітичної та військової могутності недружніх держав. Використано аналіз літературних джерел методики обґрунтування рекомендацій щодо коригування політики національної безпеки за результатами стратегічного аналізу факторів геополітичної та військової могутності недружніх держав. Використано теоретичні методи наукових досліджень, а саме: аналіз, синтез, порівняння, узагальнення, систематизацію. Результати досліджень полягають у методиці з оцінювання геополітичної і військової могутності вибраної держави на основі факторів, які визначаються за допомогою інформаційно-моніторингової системи. При цьому геополітична складова методики орієнтується на коригуванні політики національної безпеки таким чином, щоб знизити рівень геополітичної могутності недружньої держави, а військова складова – на підвищенні військової могутності власної держави, у тому числі й шляхом розвитку оборонно-промислового комплексу.

Обґрунтовані у такий спосіб пропозиції щодо впровадження зазначених заходів фіксуються і передаються у Центр прийняття рішень для подальшої обробки.

В перспективі можлива адаптація військової могутності України до визначеного у правовому просторі рівня військової могутності вибраної недружньої держави.

Ключові слова: безпекове середовище, воєнна безпека, військова могутність держави, геополітична могутність держави, загрози воєнного характеру, національна безпека, стратегічний аналіз, "чорні лебеді".

Вступ та постановка проблеми. Воєнно-політичне керівництво держави зацікавлене у розробленні експертно-аналітичного інструментарію стратегічного оцінювання (прогнозування) політики недружніх держав, здатних протидіяти, у тому числі із залученням збройних засобів, реалізації національних інтересів України. Завчасне і ефективне виявлення намірів недружніх держав, превентивне реагування на загрози національній безпеці, своєчасне розроблення ефективного озброєння, військової та спеціальної техніки національним оборонно-промисловим комплексом (ОПК) дасть змогу підвищити рівень забезпечення національної безпеки у її визначальних сферах, рівень захисту об'єктів критичної інфраструктури, покращити стан всеосяжної оборони, зміцнити національний дух і в цілому військову могутність держави.

Статтю присвячено проблемі раннього виявлення намірів і підготовки недружніх держав до протидії реалізації національних інтересів Україною у визначеній перспективі за результатами стратегічного аналізу геополітичної і військової могутності цих держав.

Сучасна система міжнародної безпеки перебуває у стані глибокої турбулентності, що зумовлено наростанням геополітичної конкуренції, трансформацією регіональних балансів сил,

появою нових центрів впливу та ускладненням конфліктогенних процесів. Сучасне безпекове середовище характеризується високою непередбачуваністю та демонструє нестійкість світового порядку (Муженко та ін., 2024).

Поява нових гарячих точок на глобальній мапі, неочікувані технологічні прориви, масштабні політичні зміни в окремих країнах, а також широке застосування безпілотних і роботизованих систем озброєння формують безпекове середовище, у якому висока непередбачуваність майбутнього стає новою нормою.

У таких умовах першочерговими завданнями військово-політичного керівництва держави стають захист суверенітету, територіальної цілісності й недоторканності, що потребує формування оновленої, науково обґрунтованої стратегії національної та воєнної безпеки (Стратегія національної безпеки..., 2020). Її розроблення можливе лише за умови впровадження сучасних технологій стратегічного аналізу, здатних враховувати як детерміновані геополітичні чинники, так і широкий спектр динамічних конфліктогенних процесів і явищ.

Аналіз останніх наукових досліджень і публікацій. У науковій літературі проблематиці оцінювання рівня впливу негативних тенденцій та загроз безпекового середовища на національну безпеку держави приділено значну увагу. Зокрема, автори свідчать, що таке оцінювання суттєво залежить від якісного аналізу інформації і своєчасних прогнозів.

Так, у дослідженні (Kotoulas, & Pusztai, 2022), в якому автори акцентують увагу на геополітичних мотивах і ревізіоністських імперативах росії, що визначають її зовнішньополітичну поведінку на міжнародній арені, висвітлюються методологічні підходи до аналізу причин, характеру та наслідків воєнних конфліктів, що вже мали місце в історії. Зокрема, значущим для досліджень у сфері воєнної безпеки є акцент на системному підході до оцінювання зовнішніх загроз та стратегічних викликів, включно з сучасними кіберзагрозами, тероризмом і поширенням зброї масового ураження. Книга слугує методологічною основою для розроблення комплексних стратегій управління ризиками у сфері національної та регіональної безпеки, але не дає змоги здійснювати стратегічний аналіз геополітичних факторів і процесів.

У дослідженні (Taleb, 2010) розглянуто феномен малоімовірних, але високоефектних подій ("чорних лебедів"), які радикально змінюють перебіг соціальних, економічних і політичних процесів та не піддаються традиційному прогнозуванню. Для тематики статті джерело є методологічно значущим, оскільки обґрунтовує обмеженість лінійних і детерміністських підходів до аналізу складних систем безпеки. Запропонована автором логіка мислення в умовах радикальної невизначеності безпосередньо підсилює необхідність використання адаптивних, ієрархічних і сценарних методів стратегічного аналізу. У контексті дослідження книга формує теоретичне підґрунтя для включення "чорних лебедів" до методики оцінювання військової могутності вибраної держави.

У монографії (Богданович та ін., 2021) запропоновано методологічний інструментарій забезпечення воєнної безпеки України в умовах сучасних, зокрема асиметричних, загроз. У ній розроблено методику оцінювання зовнішнього безпекового середовища та запропоновано практичний підхід для його аналізу в умовах сучасних збройних конфліктів. Матеріал може бути частково використаний для оцінювання військової могутності держави.

Однак, у відкритих джерелах, з якими вдалося ознайомитися авторам, відсутні методики стратегічного аналізу геополітичної і військової складової факторів і їхніх показників, ініційованих іншими авторами.

Метою статті є: розроблення спрощеної методики обґрунтування рекомендацій щодо коригування політики національної безпеки держави за результатами стратегічного аналізу геополітичної та військової могутності недружніх держав.

Виклад основного матеріалу. Суть спрощеної методики полягає в експертно-аналітичному оцінюванні змін геополітичної і воєнної могутності вибраної держави на основі геополітичних та військово-політичних факторів та їхніх основних показників за допомогою інформаційно-моніторингової системи (Богданович, & Висідалко, 2015), виявленні найбільш впливових показників геополітичної та військової могутності, за якими здійснюється пошук заходів із прискореного зниження ("замороження") рівня геополітичної могутності недружньої держави (етапи з індексом г) або підвищення рівня військової могутності власної держави,

наприклад, пропозиції ОПК щодо впровадження новітніх зразків озброєння та військової техніки (етапи з індексом в), рис. 1.

Обґрунтовані у такий спосіб рекомендації щодо впровадження пропонованих заходів фіксують і передають у Центр ухвалення рішень для подальшого оброблення.

Спрощена методика охоплює дві інформаційно насичені складові: геополітичну і військову. За рішенням вищого військово-політичного керівництва спрощена методика може використовуватися оперативними черговими військово-стратегічних структур у повсякденній діяльності, а в разі виявлення змін, що перевищують установлені пороги, здійснюється оцінювання геополітичної та військової могутності з використанням Комплексної методики обґрунтування рекомендацій щодо коригування політики національної безпеки за результатами стратегічного аналізу геополітичної та військової могутності недружніх держав (далі комплексна методика).

Звісно, що оцінювання за цією методикою має здійснюватися окремим сертифікованим підрозділом, призначеним для такої діяльності.

На етапі № 1 в, г вхідними даними для спрощеної методики є множина недружніх держав $\{G_{ndm}\}$, $m=1, M$, де M – загальна кількість недружніх держав.

Формування множин факторів геополітичної і військової могутності та їхніх показників здійснюється періодично, а самі ієрархії оцінювання геополітичної та військової могутності кожної m -ї недружньої держави містяться у відповідній базі даних.

За допомогою інформаційно-моніторингової системи (Богданович, & Висідалко, 2015), здійснюється оцінювання поточних рівнів геополітичної та військової могутності m -ї недружньої держави або змін цих рівнів.

Спрощену схему методики обґрунтування рекомендацій щодо коригування політики національної безпеки розглянемо на прикладі стратегічного аналізу військової могутності недружніх держав.

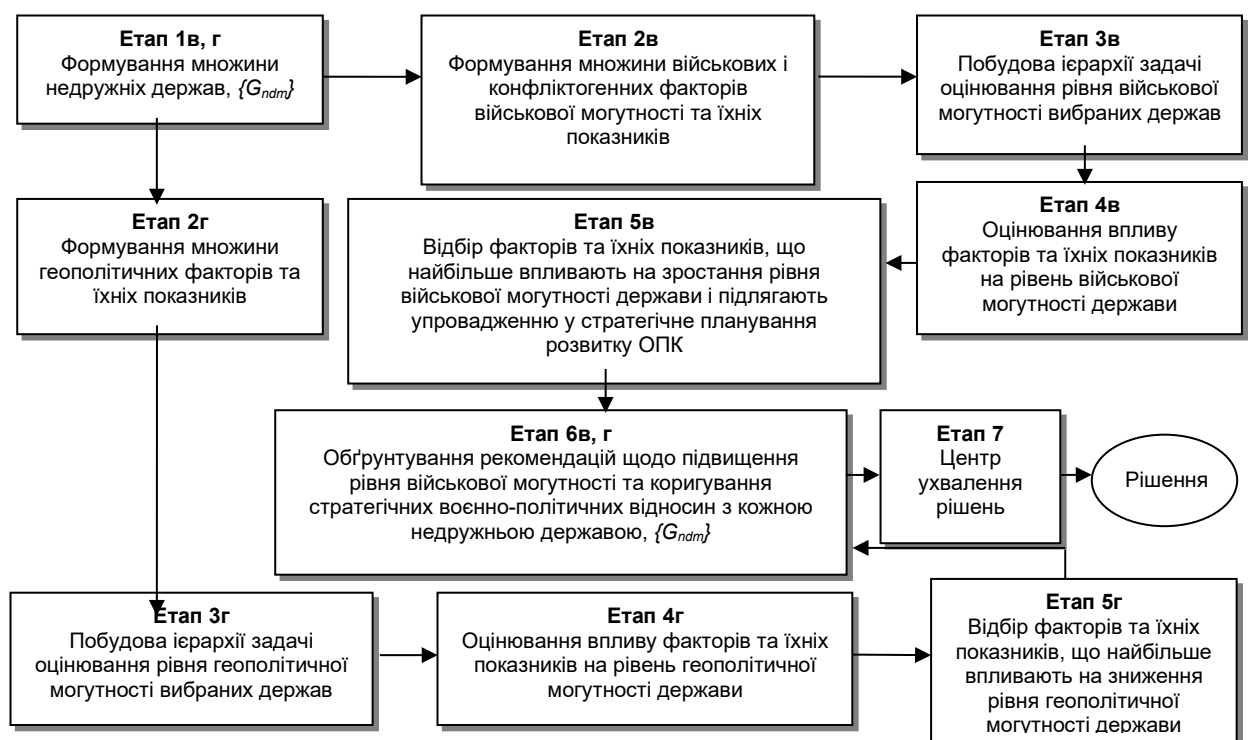


Рисунок 1 – Спрощена схема методики обґрунтування рекомендацій щодо коригування політики національної безпеки за результатами стратегічного аналізу геополітичної і військової могутності недружніх держав

На етапі № 2 в експерти формують множини військових факторів та їхніх показників, які у сукупності формують військову могутність держави. Зрозуміло, що для кожної держави ця множина факторів і показників буде своя, тому у більшості випадків можна знайти специфічні, притаманні саме цій державі фактори (Богданович, Свида, & Скулиш, 2012).

Для подальших викладок вибираємо гіпотетичну недружню державу G_{ndm} , воєнний потенціал якої подібний до воєнного потенціалу України.

На етапі № 3 в будується ієрархія задачі оцінювання рівня військової могутності вибраної недружньої держави (рис. 2).



Рисунок 2 – Спрощена ієрархія задачі оцінювання рівня військової могутності m -ї недружньої держави, G_{ndm}

На етапі № 4 в здійснюється експертно-аналітичне оцінювання впливу факторів та їхніх показників на рівень військової могутності держави, за якими здійснюється оцінювання поточного рівня військової могутності m -ї держави в системі координат "рівень військової могутності – час".

На етапі № 5 в експерти-аналітики та фахівці, яких залучають до стратегічного аналізу, вивчають результати етапу № 4 в, обґрунтовують рекомендації військового характеру щодо коригування Стратегії національної безпеки, Стратегії воєнної безпеки та інших документів з конкретною досліджуваною державою. При цьому кожна рекомендація має проходити "рецензування" за процедурою етапу № 4 в для визначення очікуваного зростання рівня військової могутності цієї держави.

Це дасть змогу нормативно визначити завдання з реалізації результатів стратегічного аналізу щодо коригування оборонно-промислової політики, витрати на реалізацію превентивних заходів у різних сферах національної безпеки, а також юридичну відповідальність посадових осіб, яких призначають для вирішення завдань воєнної безпеки держави.

На етапах № 6–№ 7 (у Центрі ухвалення рішень) ухвалюють стратегічні рішення щодо впровадження результатів проведеного стратегічного аналізу військових факторів недружніх держав, чий воєнний потенціал подібний до воєнного потенціалу України. Розробляють та ухвалюють Державні програми розвитку збройних формувань, освітні програми вищих військово-навчальних закладів, вносять зміни до інших документів стратегічного рівня (Про Стратегію воєнної..., 2021). Рішення, які ухвалюють на цьому етапі, мають закритий характер.

Оцінювання рівня геополітичної могутності вибраних держав здійснюється аналогічно на етапах 2г–5г за затвердженими факторами та їхніми показниками з прийнятою періодичністю.

Рекомендації щодо коригування в бік зростання військової могутності власної держави стосуються насамперед Стратегії воєнної безпеки та стратегічного планування розвитку ОПК (Про Стратегію розвитку..., 2021).

Більш детально оцінювання рівня геополітичної та військової могутності недружніх держав наведено в монографії (Богданович, Свида, & Скулиш, 2012).

Висновки. Спрощена методика обґрунтування рекомендацій щодо коригування політики національної безпеки за результатами стратегічного аналізу факторів геополітичної і військової могутності недружніх по відношенню до України держав містить дві складові, які з достатньою для практики точністю на стратегічному рівні дають змогу обґрунтовувати рекомендації щодо внесення змін у Стратегію воєнної безпеки та у Стратегію розвитку оборонно-промислового

комплексу України. При цьому геополітична складова методики орієнтується на корегування політики національної безпеки таким чином, щоб знизити рівень геополітичної могутності недружньої держави, а військова складова спрямована на підвищення військової могутності власної держави, у тому числі і шляхом розвитку ОПК.

Більш детально процеси обґрунтування рекомендацій щодо корегування політики національної безпеки за результатами стратегічного аналізу факторів геополітичної та військової могутності недружніх держав та їх практичної реалізації буде розглянуто у Комплексній методиці обґрунтування рекомендацій щодо коригування політики національної та оборонно-промислової політики за результатами стратегічного аналізу геополітичної і військової могутності недружніх держав.

Такий підхід дає змогу визначати ступінь юридичної відповідальності військово-політичного керівництва держави за ухвалені рішення щодо реалізації стратегічних рекомендацій за результатами стратегічного аналізу геополітичної і військової могутності недружніх держав.

ЛІТЕРАТУРА:

1. Богданович, В. Ю., & Висідалко, А. Л. (2015). Шляхи удосконалення методичних основ та інструментальних засобів підтримки процесів прийняття рішень в системі забезпечення національної безпеки. Сучасні інформаційні технології у сфері безпеки та оборони. НУОУ.
2. Богданович, В. Ю., Свида, І. Ю., & Скулиш, Є. Д. (2012). Теоретико-методологічні основи забезпечення національної безпеки України: моногр. У 7 т. Т. 4: Воєнна безпека держави і шляхи її забезпечення. (За заг. ред. Є. Д. Скулиша). Наук.-вид. відділ НА СБ України.
3. Методологія деескалації загроз зниження впливу негативних тенденцій геополітичної та воєнно-політичної обстановки на забезпечення воєнної безпеки України. (2024). (В. М. Муженко, В. Ю. Богданович, А. Л. Цибізов, О. В. Передрій). НАСВ.
4. Методологія комплексного використання військових і невійськових сил та засобів сектору безпеки і оборони для протидії сучасним загрозам воєнній безпеці України. (2021). (2-ге вид., розш. та доп.). (В. Ю. Богданович, І. С. Романченко, І. Ю. Свида, А. М. Сиротенко, О. В. Дублян). НУОУ.
5. Президент України. (2020). Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України" (392/2020). <http://www.president.gov.ua/documents/3922020-35037>
6. Президент України. (2021). Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України" (121/2021). <http://www.president.gov.ua/documents/1212021-37661>
7. Президент України. (2021). Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегію розвитку оборонно-промислового комплексу України" (372/2021). <http://www.president.gov.ua/documents/3722021-38143>.
8. Kotoulas, I. E., & Pusztai, W. (2022). Geopolitics of the War in Ukraine [Геополітика війни в Україні]: Report No 4. Foreign Affairs Institute (FAINST). Athens. <https://euagenda.eu/upload/publications/geopolitics-of-the-war-in-ukraine-final.pdf>
9. Nassim Nicholas Taleb. (2010). The Black Swan: The Impact of the Highly Improbable. Penguin Books.

REFERENCES:

1. Bogdanovych, V. Yu., & Vysidalko, A. L. (2015). Shlyahy udoskonalennya metodichnykh osnov instrumentalnykh zasobiv pidtrymky protsesiv prynyatya rishen v systemi zabezpechennya natsionalnoyi bezpeky. Suchasni informachiyni tekhnologiyi u sferi bezpeky i oborony. NUOU.
2. Bogdanovych, V. Yu., Svyda, I. Yu., & Skulysh, Ye. D. (2012). Teoretyko-metodologichni osnovy zabezpechennya natsionalnoyi bezpeky Ukrainy. U 7 t. T. 4: Voenna bezpeka derzhavy i shlyahy yiyi zabezpechennya. (Za zag. red. Ye. D. Skulysha). Nauk.-vyd. viddil NA SB Ukrainy.
3. Kotoulas, I. E., & Pusztai, W. (2022). Geopolitics of the War in Ukraine [Геополітика війни в Україні]: Report No 4. Foreign Affairs Institute (FAINST). Athens. <https://euagenda.eu/upload/publications/geopolitics-of-the-war-in-ukraine-final.pdf>

4. Metodologiya deeskalatsiyi zagroz znyzhennya vplyivu negatyvnykh tendentsiy geopolitychnoyi ta voenno-politychnoyi obstanovky na zabezpechennya voyennoyi bezpeky Ukrainy. (2024). (V. M. Muzhenko, V. Yu. Bogdanovych, A. L. Tsybizov, O. V. Peredriyi). NASV.
5. Metodologiya kompleksnogo vykorystannya viyskovykh i neviyskovykh syl ta zasobiv sectoru bezpeky i oborony dlya protydyi suchasnym zagrozam voyenniy bezpetsi Ukrainy. (2021). (Vyd. 2-ge). (V. Yu. Bogdanovych, I. Yu. Svyda, I. S. Romanchenko, A. M. Syrotenko, O. V. Dublyan). NUOU.
6. Nassim Nicholas Taleb. (2010). The Black Swan: The Impact of the Highly Improbable. Penguin Books.
7. Prezydent Ukrainy. (2020). Pro rishennja Rady natsionalnoyi bezpeky i oborony Ukrainy vid 14.09.2020 "Pro Strategiyu natsionalnoyi bezpeky Ukrainy" (392/2020). <http://www.president.gov.ua/documents/3922020-35037>
8. Prezydent Ukrainy. (2021). Pro rishennja Rady natsionalnoyi bezpeky i oborony Ukrainy vid 25.03.2021 "Pro Strategiyu voyennoyi bezpeky Ukrainy" (121/2021). <http://www.president.gov.ua/documents/1212021-37661>
9. Prezydent Ukrainy. (2021). Pro rishennja Rady natsionalnoyi bezpeky i oborony Ukrainy vid 20.08.2021 "Pro Strategiyu rozvytku oboronno-promyslovogo kompleksu Ukrainy" (372/2021) <http://www.president.gov.ua/documents/3722021-38143>.

**DSc (Engin.), Prof Bohdanovych.V, PhD (Military),
Sen. Res.Tsybizov A., Assoc. Prof Hulak O.**

SIMPLIFIED METHODOLOGY FOR SUBSTANTIATING RECOMMENDATIONS ON ADJUSTING THE STATE'S NATIONAL SECURITY POLICY BASED ON THE RESULTS OF STRATEGIC ANALYSIS OF THE GEOPOLITICAL AND MILITARY POWER OF UNFRIENDLY STATES

The relevance of the article lies in the presentation of a simplified methodology for substantiating recommendations on adjusting national security policy based on the results of strategic analysis of the factors of geopolitical and military power of unfriendly states. This methodology comprises two main components that enable the justification of recommendations for introducing changes to the National Security Strategy and the Strategy for the Development of Ukraine's Defense-Industrial Complex. Used during the research content-analysis of scientific sources, comparison, classification, systematization.

Results. The core of the methodology involves assessing the geopolitical and military power of the selected state based on factors determined through an information-monitoring system. The geopolitical component of the methodology focuses on adjusting national security policy in a manner that reduces the level of geopolitical power of the hostile state, while the military component aims to enhance the military power of one's own state, including through the development of the defense-industrial complex.

Proposals justified in this manner regarding the implementation of the aforementioned measures are documented and transmitted to the Decision-Making Center for further processing.

In the long term, it is possible to adapt Ukraine's military power to the level of military power of the selected hostile state as defined within the legal framework.

This approach also makes it possible to determine the degree of legal responsibility of the state's military-political leadership for decisions taken in implementing strategic recommendations derived from the strategic analysis of the geopolitical and military power of unfriendly states.

Keywords: security environment, military security, military power of the state, factors, geopolitical power of the state, military threats, national security, strategic analysis, "black swans".

ОБСЕ ЯК ІНСТИТУЦІЙНИЙ МЕХАНІЗМ ФОРМУВАННЯ ДОВІРИ, ВІЙСЬКОВОЇ ТРАНСПАРЕНТНОСТІ, КОНТРОЛЮ НАД ОЗБРОЄННЯМИ ТА ЗАПОБІГАННЯ КОНФЛІКТАМ У ЄВРОПІ

Стаття присвячена аналізу ОБСЕ як комплексний інституційний механізм поєднання режимів військової прозорості, заходів зі зміцнення довіри та безпеки, інструментів раннього попередження й врегулювання конфліктів.

У сучасному європейському безпековому середовищі, що характеризується геополітичною фрагментацією та ерозією традиційних режимів контролю над озброєннями, довіра між державами більше не може розглядатися як результат політичних декларацій чи спільності цінностей. Вона формується через інституційні механізми передбачуваності, у яких військова транспарентність відіграє ключову роль

Дослідження базується на поєднанні інституціонального підходу та методології безпекових студій. Проведено якісний порівняльний аналіз ключових документів ОБСЕ (Віденський документ 2011, Кодекс поведінки щодо воєнно-політичних аспектів безпеки 1994 року), діяльності Центру запобігання конфліктам, польових місій та інституту Верховного комісара у справах національних меншин. Здійснено декомпозицію інструментів за нормативним, верифікаційним, аналітичним і медіаційним вимірами з акцентом на їх взаємодію. Метою дослідження є визначення взаємозв'язку між режимами військової транспарентності та інструментами врегулювання конфліктів у межах Організації з безпеки і співробітництва в Європі, а також обґрунтування напрямів їх інституційної оптимізації в умовах тривалої кризи європейської архітектури безпеки.

Результати дослідження показують, що ефективність ОБСЕ визначається не окремими інструментами, а їхньою взаємодією, яка забезпечує процедурну передбачуваність і знижує ризик ескалації. Виявлено ключові обмеження: консенсусна модель ухвалення рішень, формалізація режимів транспарентності, фрагментація військової діяльності нижче порогових значень та слабка інтеграція верифікаційних даних з механізмами раннього попередження й медіації. Запропоновано авторську модель оптимізації, що передбачає модернізацію порогових критеріїв, посилення аналітичної автономії Центру запобігання конфліктам, впровадження цифрових інструментів верифікації та тісніше поєднання моніторингу з медіаційними практиками.

Ключові слова: ОБСЕ, військова транспарентність, формування довіри, контроль над озброєннями, Віденський документ 2011, запобігання конфліктам, раннє попередження, медіація, європейська безпека, верифікація.

Вступ та постановка проблеми. Європейський безпековий простір увійшов у фазу, коли довіра між державами перестала виконувати роль майже непомітної передумови стабільності і знову стала предметом відкритого політичного суперництва. Упродовж тривалого часу здавалося, що інституційні механізми передбачуваності, сформовані після завершення холодної війни, достатньо міцні, аби стримувати неконтрольовану ескалацію навіть за наявності глибоких політичних розбіжностей. Останнє десятиліття змусило переглянути цю оцінку. Коли режими повідомлення, інспекцій, спостереження, обміну військовою інформацією та кризових консультацій перестають сприйматися як спільна цінність або хоча б як необхідна процедурна умова співіснування, вони швидко втрачають політичний зміст. Формально інструменти залишаються, але їхня стабілізаційна функція поступово розмивається.

У цьому сенсі проблема діяльності Організації з безпеки і співробітництва в Європі (ОБСЕ) полягає не лише у неповному використанні її інструментів. Більш складним є питання їхньої легітимності. В умовах відновлення силового суперництва сама логіка взаємодії держав починає піддавати сумніву доцільність процедур, які були розроблені для середовища відносної передбачуваності (Віденський документ, 2011; Code of Conduct on Politico-Military Aspects of Security, 1994). Організація визначає військову транспарентність, обмін

інформацією, інспекції, спостереження і консультації як ключові елементи зниження ризику інцидентів та помилкових оцінок намірів. Однак ефективність цих інструментів прямо залежить від готовності держав не лише формально дотримуватися процедур, але й не обходити їхній зміст.

Існує й інша проблема, менш очевидна, але методологічно важлива. У наукових дослідженнях механізми формування довіри та інструменти врегулювання конфліктів часто аналізуються окремо. В одних роботах увага зосереджується на військовій прозорості, режимах повідомлення та верифікації. В інших дослідженнях центр тяжіння переноситься на дипломатичні формати, посередництво, польові місії або кризове управління. Такий поділ певною мірою виправданий аналітичною зручністю, проте він погано відображає реальну інституційну практику ОБСЄ.

У межах цієї організації довіра рідко виникає лише як результат переговорного процесу. Так само і транспарентність не зводиться до технічного обміну інформацією. Повідомлення про військову діяльність, спостереження за навчаннями, верифікаційні візити, механізми раннього попередження, діалогові формати та моніторинг конфліктів утворюють взаємопов'язану систему. Вона працює нерівномірно і не завжди ефективно, однак саме їхня взаємодія створює мінімальний рівень передбачуваності. (OSCE Handbook on Confidence- and Security-Building Measures, 2014; High Commissioner on National Minorities: Mandate and Activities, 2023; European Security and Cooperation, Yearbook, 2021). У цьому сенсі ОБСЄ доцільно розглядати не лише як дипломатичний майданчик, а швидше як інституційну екосистему процедурної передбачуваності.

Додаткову актуальність проблемі надає інституційна специфіка самої організації. ОБСЄ фактично залишається однією з небагатьох загальноєвропейських платформ, де військово-політичний, конфліктно-посередницький і нормативний виміри безпеки формально поєднані. Віденський документ 2011 року, Кодекс поведінки щодо воєнно-політичних аспектів безпеки, діяльність Форуму зі співробітництва в галузі безпеки (Organization for Security and Co-operation in Europe, 2022a), робота Центру запобігання конфліктам (Organization for Security and Co-operation in Europe, 2023a), інститут Верховного комісара у справах національних меншин (Organization for Security and Co-operation in Europe, 2023b), а також досвід Спеціальної моніторингової місії в Україні демонструють, що функціонування організації не зводиться до одного виміру ефективності.

Оцінювати ОБСЄ виключно через здатність швидко припиняти війни означало б спрощувати її історичну роль. Як зазначається в аналітичних доповідях, сила цієї інституції традиційно полягала в збереженні каналів комунікації, створенні процедурної довіри та обмеженні ризику ескалації локальних криз (OSCE Network of Think Tanks and Academic Institutions, 2022; OSCE Yearbook 2021, 2022; Conflict Prevention Centre, 2023).

Аналіз основних наукових досліджень і публікацій. Методологічна конструкція дослідження спрямована на ідентифікацію механізмів, через які військова транспарентність трансформується у передбачуваність поведінки держав і, опосередковано, у довіру як функціональну характеристику безпекового середовища в межах Організації з безпеки і співробітництва в Європі. Вихідною аналітичною установкою є розмежування нормативно декларованої транспарентності та її операційної спроможності впливати на динаміку конфліктів.

Концептуально дослідження спирається на поєднання інституціоналізму та підходів безпекових студій, де інститути розглядаються не як статичні правила, а як середовище взаємодії акторів із асиметричними інтересами. Це дозволяє фіксувати не лише формальні параметри режимів транспарентності, а й ступінь їх фактичної імплементації. У цьому контексті ключові документи, зокрема Віденський документ 2011 та Кодекс поведінки щодо воєнно-політичних аспектів безпеки, інтерпретуються як інституційні матриці, що задають рамки допустимої військової поведінки, але не гарантують їх дотримання.

Аналітичний дизайн вибудований як багаторівнева модель. На нормативному рівні здійснюється декомпозиція інструментів ОБСЄ за функціональними параметрами: обмін інформацією, верифікація, раннє попередження, медіація. На операційному рівні аналізується, як ці інструменти взаємодіють у практиці, формуючи або, навпаки, підбиваючи ефект передбачуваності.

Емпірична частина базується на якісному порівняльному аналізі, орієнтованому на зіставлення задекларованих механізмів і фактичних практик їх застосування. Порівняння здійснюється між різними типами інструментів ОБСЄ, що виконують суміжні функції, але мають різну ступінь обов'язковості та політичної підтримки. Це дає змогу виявити внутрішні дисбаланси системи, зокрема розрив між обсягом доступної інформації та її використанням у процесах раннього реагування.

Методологічні обмеження мають подвійний характер. З одного боку, доступ до первинних даних про виконання заходів транспарентності є фрагментованим і часто політизованим. З іншого, консенсусна процедура ухвалення рішень у межах ОБСЄ ускладнює формалізацію критеріїв ефективності, зміщуючи аналіз у площину якісних оцінок. Це обмежує можливість кількісної верифікації, але водночас дозволяє точніше фіксувати інституційні розриви.

Обрана методологія орієнтована не на опис інструментів як таких, а на виявлення їх функціональної спроможності в умовах зростаючої стратегічної невизначеності. Такий підхід відкриває можливість оцінювати ОБСЄ як динамічну систему, чутливу до змін політичного контексту, а не як фіксований набір процедур.

Аналіз останніх досліджень і публікацій. У сучасній науковій літературі можна виокремити кілька відносно автономних підходів до осмислення ролі ОБСЄ у структурі європейської безпеки. Перший пов'язаний із традицією досліджень контролю над озброєннями та заходів зміцнення довіри і безпеки. У цьому корпусі робіт військова транспарентність розглядається як базовий механізм формування передбачуваності, тоді як Віденський документ постає інструментом зниження ризику помилкової інтерпретації військової активності.

Особливо показовими є дослідження Л. Кулеса та В. Зелнера. У їхніх роботах підкреслюється, що навіть у ситуації різкого падіння взаємної довіри режими повідомлення, верифікації та інспекцій можуть виконувати функцію своєрідної "мінімальної стабілізації". Інакше кажучи, вони не усувають політичного конфлікту, але знижують імовірність того, що конфронтація перейде в режим неконтрольованого ризику. (Kulesa, 2020; Zellner, 2017). Це твердження виглядає переконливим, хоча його застосовність значною мірою залежить від політичної волі держав підтримувати відповідні процедури.

Другий напрям досліджень концентрується на конфліктному вимірі діяльності ОБСЄ: ранньому попередженні, посередництві, польових операціях, моніторингу та кризовому менеджменті. У цьому контексті важливими є праці Гертеля та колег (Härtel et al., 2021), Пундзіуте-Галлуа (Pundziūtė-Gallois, 2023), а також спільне дослідження Гулієва і Гавріха (Guliyev & Gawrich, 2021). Ці автори показують, що ОБСЄ функціонує не лише як форум для міждержавного діалогу. У низці випадків вона виконує прикладні функції: від фасилітації переговорів до польового спостереження та підтримки процедурної довіри в конфліктних середовищах (Wolff, 2018; Pundziūtė-Gallois, 2023).

Цікавим є і більш стриманий висновок, який простежується у частині цієї літератури: організація часто виявляється відносно ефективною саме там, де не декларує амбіцій швидкого досягнення "великого миру". Її практична роль нерідко полягає у підтриманні контактів, фіксації фактів, документуванні подій та стримуванні подальшої деградації безпекового середовища. Подібна оцінка, втім, не є беззаперечною, оскільки вона значною мірою залежить від того, які критерії ефективності використовуються.

Серед вітчизняних досліджень дотичних проблем контролю над озброєннями та формування безпекової передбачуваності в Європі заслуговують увагу публікації 2026 року. Зокрема, в дослідженні "Теоретичні засади контролю над звичайними озброєннями в Європі в умовах трансформації безпекового середовища" вітчизняних вчених В. Гурковського, Є. Романенка та Н. Павлія (Gurkovskyi et al., 2026) обґрунтовано, що в сучасних умовах геополітичної фрагментації класичні режими транспарентності (зокрема Віденський документ) потребують не лише технічного оновлення порогових критеріїв, але й глибшого інституційного переосмислення, аби запобігти фрагментації військової активності та ілюзії контролю. Доповнює цей аналіз дослідження Н. Клименко "Глобальна та регіональна безпека: контроль над звичайними озброєннями, гуманітарна, соціальна та економічна складові" (Klymenko & Taran, 2026), де авторка акцентує, що ефективність механізмів ОБСЄ залежить

не лише від військово-технічної верифікації, а й від врахування гуманітарних, соціальних та економічних наслідків обмеження озброєнь, що створює додаткові стимули для політичної волі держав-учасниць. Обидві роботи підтверджують ключовий висновок статті: військова транспарентність і врегулювання конфліктів у межах ОБСЄ не можуть розглядатися ізольовано, а вимагають комплексної інтеграції нормативного, верифікаційного та медіаційного вимірів, що особливо актуально для української безпекової політики в умовах триваючої кризи європейської архітектури безпеки.

Третій напрям досліджень пов'язаний із ширшим теоретичним осмисленням транспарентності як правового і політичного принципу. У роботах М. Соссаї (Sossai, 2013) транспарентність розглядається не лише як технічна процедура обміну інформацією, а як одна з опорних категорій режимів роззброєння і нерозповсюдження. Такий підхід дозволяє вийти за межі вузько інструментального розуміння військової прозорості. У сфері безпеки транспарентність фактично формує середовище, у якому наміри держав стають принаймні частково зрозумілими, а отже менш загрозливими для інших акторів.

Близькі за логікою висновки містяться і в дослідженнях А. Ісакова та С. Вольфа (Wolff, 2018). Вони демонструють, що механізми попередження конфліктів та робота з напруженням усередині суспільств також спираються на інституційно організовану довіру. Йдеться про раннє виявлення ризиків, посередництво, правові рекомендації, а також про локальне нарощування спроможностей, яке інколи залишається менш помітним у політичних оцінках діяльності організації.

Попри значний масив досліджень, у літературі зберігається кілька помітних прогалин. По-перше, бракує робіт, які системно поєднували б воєнно-технічні інструменти транспарентності з політико-дипломатичними механізмами врегулювання конфліктів у межах єдиної аналітичної моделі. По-друге, криза контролю над озброєннями та криза довіри нерідко аналізуються як окремі процеси, хоча на практиці вони швидше є різними проявами однієї глибшої трансформації європейського безпекового порядку. Нарешті, у частині робіт ОБСЄ описується переважно через призму її слабкості. Така оцінка не обов'язково помилкова, але вона інколи ігнорує інший аспект – зміну режиму корисності організації: від амбіцій великої політичної угоди до підтримання каналів кризової комунікації, спостереження і верифікації.

У наукових працях простежується відсутність єдності у трактуванні природи довіри та механізмів її формування.

Метою статті є: визначення взаємозв'язку між режимами військової транспарентності та інструментами врегулювання конфліктів у межах Організації з безпеки і співробітництва в Європі, а також обґрунтування напрямів їх інституційної оптимізації в умовах тривалої кризи європейської архітектури безпеки.

Виклад основного матеріалу. Проблема довіри у сфері безпеки зазвичай трактується як психологічна або політична категорія. Однак у випадку ОБСЄ таке розуміння є недостатнім. У межах цієї інституції довіра функціонує передусім як процедурно організований механізм управління безпековими ризиками. Вона виникає не через збіг ціннісних орієнтацій або взаємну політичну симпатію держав, а через наявність стабільних каналів обміну інформацією, системи перевірки військової діяльності, регулярних консультацій та інституційних форматів деескалації.

Таким чином, у логіці ОБСЄ йдеться не про повну політичну довіру, а про її процедурний мінімум. Саме цей мінімум дозволяє підтримувати певну керованість безпекового середовища навіть у ситуації високої взаємної підозри між державами. Інституційна архітектура ОБСЄ орієнтована не на усунення конфлікту інтересів, а на зниження ризику його неконтрольованої ескалації.

Таке розуміння безпосередньо впливає з концепції заходів зміцнення довіри та безпеки. У документах ОБСЄ вони визначаються як інструменти, спрямовані на підвищення передбачуваності військової діяльності, зменшення ймовірності інцидентів і формування практики превентивної взаємодії. У цьому контексті довіра не передує інституціям, а частково продукується ними. Чим більш систематичними є повідомлення про військову активність, спостереження за навчаннями, інспекції та оцінювальні візити, тим вищою стає здатність держав інтерпретувати поведінку одна одної як прогнозовану.

Звідси випливає ключове положення: зниження транспарентності неминує веде до ерозії довіри. У свою чергу, дефіцит довіри стимулює подальше приховування намірів і маніпулювання інформацією. Такий взаємопосилювальний процес формує структурне середовище стратегічної невизначеності, у якому навіть обмежені військові дії можуть інтерпретуватися як потенційна загроза.

Нормативним виміром цієї логіки виступає Кодекс поведінки щодо воєнно-політичних аспектів безпеки (Organization for Security and Cooperation in Europe, 1994). Документ поєднує міждержавний і внутрішньодержавний рівні безпеки, наголошуючи на принципі її неподільності та на необхідності демократичного контролю над силовими структурами. Важливість цього положення виходить за межі правового регулювання. Прозорість оборонного планування, підзвітність військових інститутів та цивільний контроль зменшують ризик непрогнозованого застосування сили як у внутрішньополітичному, так і у міжнародному вимірі. У результаті довіра набуває подвійної природи: вона формується як між державами, так і всередині їхніх інституційних систем.

Найконкретнішим інструментом формування передбачуваності в ОБСЄ є Віденський документ 2011 (Organization for Security and Co-operation in Europe, 2011). Він встановлює процедури обміну військовою інформацією, механізми спостереження за навчаннями та інспекційні формати. Однак розвиток безпекового середовища останніх років продемонстрував обмеження цього режиму. Дослідники відзначають, що слабкість інструментів транспарентності проявляється тоді, коли держави використовують формальні параметри документа для обходу його сутнісної логіки (Engvall, 2021; Kulesa, 2020). Йдеться про ситуації, коли масштабні військові активності фрагментуються або проводяться нижче встановлених порогів повідомлення.

У таких умовах виникає парадокс неповної прозорості. Формально інституційний режим продовжує діяти, проте його здатність забезпечувати реальну передбачуваність зменшується. Найбільший ризик полягає в тому, що створюється ілюзія контролю над ситуацією тоді, коли сам механізм контролю вже послаблений. Військова транспарентність, таким чином, виступає матеріальною основою довіри, але не її гарантією.

Коли держави мають доступ до регулярної інформації, інспекцій і процедур верифікації, вони рідше виходять із найгірших сценаріїв поведінки іншої сторони. Якщо ж ці механізми слабшають, стратегічне планування починає базуватися на припущенні про потенційно найнебезпечніші наміри опонента. Саме тому навіть обмежені інструменти транспарентності здатні відігравати стримувальну роль.

Таблиця 1 – Інституційні інструменти ОБСЄ та їхня функція у формуванні довіри

Інструмент	Основна функція	Внесок у формування довіри	Ключове обмеження
Віденський документ 2011	Повідомлення про військову діяльність, інспекції, спостереження за навчаннями	Підвищення передбачуваності військової активності	Використання порогів та винятків для обходу процедур
Кодекс поведінки щодо воєнно-політичних аспектів безпеки	Нормативні принципи використання сили, демократичний цивільний контроль	Формування довіри до процедур застосування військової сили	Політична, а не юридично примусова природа
Центр запобігання конфліктам ОБСЄ	Раннє попередження, аналітика ризиків, підтримка кризового менеджменту	Інституційна координація реагування на безпекові ризики	Обмежена автономія від політичних рішень держав

Інструмент	Основна функція	Внесок у формування довіри	Ключове обмеження
Спеціальна моніторингова місія ОБСЄ в Україні	Польовий моніторинг, звітність, фасилітація локального діалогу	Формування спільного фактичного інформаційного поля	Обмеження доступу та політизація оцінок
Верховний комісар ОБСЄ у справах національних меншин	Превентивна дипломатія та рекомендації щодо міжетнічних відносин	Зниження конфліктного потенціалу на ранній стадії	Залежність ефективності від готовності сторін співпрацювати

Представлена схема показує, що довіра в інституційній логіці ОБСЄ формується на кількох взаємопов'язаних рівнях: нормативному, інформаційно-верифікаційному, аналітичному та посередницькому. Центральне місце в цій структурі посідає Центр запобігання конфліктам ОБСЄ. На відміну від більш помітних політичних форматів, саме цей підрозділ забезпечує щоденне функціонування системи раннього попередження, підтримку польових місій та аналітичну оцінку безпекових ризиків.

У цьому контексті стає очевидним, що військова транспарентність не може розглядатися ізольовано від механізмів врегулювання конфліктів. Інформація, отримана через режими верифікації, має бути інтегрована в систему раннього попередження та політичних консультацій. Якщо цей зв'язок слабшає, навіть достовірні дані не перетворюються на політичну дію.

Саме тому в сучасних аналітичних оцінках дедалі частіше порушується питання про розширення аналітичної автономії Центру запобігання конфліктам. Йдеться не лише про технічні вдосконалення, а про здатність інституції переводити сигнали ризику в політичний порядок денний до того, як вони переростуть у кризу.

Посередницька діяльність ОБСЄ має специфічний характер. Організація рідко досягає швидких дипломатичних проривів. Її ефективність проявляється у підтриманні комунікаційних каналів, створенні процедурних рамок діалогу та поступовому зниженні напруженості. Порівняльна перевага ОБСЄ полягає у поєднанні інклюзивності, інституційної легітимності та накопиченого досвіду фасилітації переговорів.

Водночас консенсусна модель прийняття рішень створює структурне обмеження. Політична воля держав-учасниць є одночасно джерелом легітимності організації і фактором її вразливості. ОБСЄ здатна забезпечувати процедури взаємодії, але не має інструментів примусу до їх виконання.

У таких умовах більш коректним критерієм оцінки ефективності організації є не здатність швидко завершувати конфлікти, а спроможність підтримувати інфраструктуру керованої конфліктності – систему моніторингу, раннього попередження та комунікації, що знижує ризик неконтрольованої ескалації.

Таблиця 2 – Авторська модель оптимізації інституційних механізмів ОБСЄ

Проблемний фактор	Поточний наслідок	Оптимізаційний підхід	Очікуваний ефект
Застарілі параметри режиму транспарентності	Обхід процедур повідомлення	Оновлення порогів військової активності	Зменшення "сірих зон" у військовій прозорості
Слабкий зв'язок між інформацією та аналізом	Запізніла політична реакція	Посилення аналітичної автономії Центру запобігання конфліктам	Швидше винесення ризиків у політичний порядок денний

Проблемний фактор	Поточний наслідок	Оптимізаційний підхід	Очікуваний ефект
Обмежені інструменти перевірки	Сумніви щодо достовірності даних	Використання цифрових і гібридних механізмів верифікації	Підвищення надійності інформації
Розрив між моніторингом і медіацією	Переговори без спільної фактичної бази	Інтеграція звітності, аналізу та фасилітації	Посилення деескалаційного потенціалу
Низька швидкість реагування на кризу	Зволікання під час ескалації	Інституціоналізація швидких консультацій	Зниження ризику ненавмисного загострення

Проведений аналіз дозволяє сформулювати узагальнену логіку взаємодії довіри, транспарентності та врегулювання конфліктів.

Послідовність деескалаційної взаємодії: військова інформація → верифікація → передбачуваність → зниження ризику хибної інтерпретації → збереження каналів діалогу → медіація → стримування ескалації → часткове відновлення довіри.

Зворотна динаміка має протилежний ефект: блокування прозорості → дефіцит перевірюваних фактів → домінування найгірших сценаріїв → зростання недовіри → ослаблення переговорних форматів → ескалаційні рішення.

Отже, довіра та транспарентність перебувають у відносинах взаємного відтворення. Прозорість не гарантує довіри, проте без неї довіра майже не має інституційних механізмів відновлення.

У сучасному безпековому середовищі ОБСЄ залишається унікальною інституційною платформою, яка поєднує політичний діалог, режим військової прозорості, польовий моніторинг і превентивну дипломатію. Саме ця багаторівнева структура дозволяє розглядати організацію як один із ключових елементів процедурної безпеки в Європі.

Висновки. Проведене дослідження дозволяє розглядати проблематику формування довіри та врегулювання конфліктів у межах ОБСЄ як єдиний аналітичний комплекс. Поєднання нормативних документів, механізмів військової прозорості, аналітичних структур (Organization for Security and Co-operation in Europe, 2023a) та посередницьких форматів (Pundziūtė-Gallois, 2023; Wolff, 2018) створює багаторівневу архітектуру процедурної передбачуваності.

Проведене дослідження дозволяє розглядати проблематику формування довіри та врегулювання конфліктів у межах ОБСЄ як єдиний аналітичний комплекс. Поєднання цих двох дослідницьких ліній оптимізації механізмів довіри та підвищення військової транспарентності у сфері контролю над озброєннями виявилось не лише методологічно виправданим, а й концептуально необхідним. Аналіз засвідчив, що в інституційній логіці ОБСЄ вони не існують як автономні напрямки. Режими транспарентності виконують роль структурної передумови політичного діалогу, тоді як врегулювання конфліктів неможливо відокремити від процедур перевірки, моніторингу, звітності та систем раннього попередження.

Отримані результати свідчать про те, що специфіка ОБСЄ полягає у багаторівневій архітектурі її інструментів. Нормативні документи, механізми військової прозорості, аналітичні структури та посередницькі формати функціонують як взаємопов'язана система. У межах цієї системи Віденський документ 2011, Кодекс поведінки щодо воєнно-політичних аспектів безпеки, діяльність Форум зі співробітництва в галузі безпеки ОБСЄ, Центр запобігання конфліктам ОБСЄ, польові місії та інститут Верховний комісар ОБСЄ у справах національних меншин виконують різні, але взаємодоповнювальні функції. Їхня взаємодія створює середовище інституційної передбачуваності, у якому нормативні принципи, технічні процедури перевірки, аналітична оцінка ризиків і дипломатична медіація підсилюють одна одну. Саме така комбінація пояснює унікальне місце ОБСЄ серед інших європейських безпекових інституцій.

Разом із тим аналіз показує, що ефективність цієї архітектури істотно обмежується низкою структурних факторів. Консensusний характер ухвалення рішень зумовлює залежність організації від політичної волі держав-учасниць. У ситуації її послаблення інституційні

механізми зберігають формальну дію, проте поступово втрачають практичну результативність (OSCE Network of Think Tanks and Academic Institutions, 2022; OSCE Yearbook 2021, 2022).. Додаткові обмеження виникають через практику формального дотримання правил із одночасним обходом їхнього змісту, обмежені мандати польових місій та недостатню інтегрованість між системами верифікації, аналітики ризиків і медіаційними процесами. У результаті інституційна реакція організації нерідко відстає від динаміки розвитку кризових ситуацій, а режими військової прозорості частково втрачають свій деескалаційний потенціал.

Дослідження дає підстави визначити кілька пріоритетних напрямів інституційної оптимізації ОБСЄ. За переконанням автора статті, першочерговим завданням є оновлення параметрів режиму військової транспарентності, передусім через модернізацію положень Віденський документ 2011 та перегляд його порогових критеріїв. Другий напрям пов'язаний із посиленням аналітичної спроможності Центр запобігання конфліктам ОБСЄ, що передбачає розширення можливостей для незалежної оцінки безпекових ризиків і більш раннього винесення проблемних питань на політичний порядок денний. Не менш важливим є технологічне оновлення процедур перевірки й звітності, включно з використанням сучасних інструментів цифрової верифікації та удосконалених методів обробки інформації. Нарешті, підвищення ефективності організації потребує тіснішого поєднання механізмів військової прозорості з посередницькими та медіаційними форматами, що дозволить використовувати верифікаційні дані як фактичну основу переговорних процесів.

Загальний висновок дослідження полягає в тому, що довіра в сучасному безпековому середовищі не формується через декларативні політичні заяви. Вона виникає як результат функціонування інституційних процедур передбачуваності: систем обміну інформацією, перевірки, консультацій і раннього попередження. У цьому контексті ОБСЄ, попри очевидні інституційні обмеження, продовжує відігравати важливу роль у підтриманні мінімальної керованості європейського безпекового середовища. Як зазначали авторами, її значення полягає не у здатності швидко усувати конфлікти, а у збереженні інфраструктури діалогу, прозорості та ризик-редукції.

Подальші дослідження можуть розвиватися в кількох напрямках. Перспективним є поглиблений аналіз модернізації режимів військової транспарентності з урахуванням нових технологічних факторів, зокрема використання безпілотних систем, цифрових інструментів верифікації та змін у характері військової мобільності. Не менш важливим виглядає порівняльне дослідження ефективності різних моделей посередництва ОБСЄ у затяжних конфліктах пострадянського простору. Окремої уваги потребує питання можливого поєднання політично зобов'язуючих режимів ОБСЄ з більш жорсткими механізмами комплаєнсу без втрати інклюзивного характеру організації, що залишається одним із її ключових інституційних ресурсів.

ОБСЄ зберігає унікальне місце в європейській безпековій архітектурі як платформа процедурної передбачуваності, проте потребує термінової інституційної адаптації до умов геополітичної фрагментації. Збереження її ролі залежить від оновлення режимів військової транспарентності, посилення аналітичної та медіаційної складових і відновлення політичної волі держав-учасниць. Результати мають практичне значення для української політики у сфері європейської безпеки та контролю над озброєннями.

ЛІТЕРАТУРА:

1. Гертель, А., Пісаренко, А., та Умланд, А. (2021). The OSCE's Special Monitoring Mission to Ukraine: The SMM's Work in the Donbas and Its Ukrainian Critique in 2014–2019. *Security and Human Rights*, 31(1-4), 121–154.
2. Гулієв, Ф., та Гавріх, А. (2021). OSCE mediation strategies in Eastern Ukraine and Nagorno-Karabakh: a comparative analysis. *European Security*, 30(4), 569–588.
3. Гурковський, В. І., Романенко, Є. О., та Павлій, Н. І. (2026). Теоретичні засади контролю над звичайними озброєннями в Європі в умовах трансформації безпекового середовища. *Національні інтереси України*, 2(19), 132–151. [https://doi.org/10.52058/3041-1793-2026-2\(19\)-132-151](https://doi.org/10.52058/3041-1793-2026-2(19)-132-151)

4. Клименко, Н., та Таран, Є. (2026). Глобальна та регіональна безпека: контроль над звичайними озброєннями, гуманітарна, соціальна та економічна складові. Національні інтереси України, 2(19), 263–275. [https://doi.org/10.52058/3041-1793-2026-2\(19\)-263-275](https://doi.org/10.52058/3041-1793-2026-2(19)-263-275)
5. Організація з безпеки і співробітництва в Європі. (1994). Code of Conduct on Politico-Military Aspects of Security. Будапешт. <https://www.osce.org/fsc/41355>
6. Організація з безпеки і співробітництва в Європі. (2011). Віденський документ 2011 про заходи зі зміцнення довіри та безпеки. Відень. <https://www.osce.org/fsc/41355>
7. Організація з безпеки і співробітництва в Європі. (2014). OSCE Handbook on Confidence- and Security-Building Measures. Відень.
8. Організація з безпеки і співробітництва в Європі. (2022). Forum for Security Co-operation: Overview and Functions. Відень.
9. Організація з безпеки і співробітництва в Європі. (2023a). Conflict Prevention Centre. OSCE Secretariat. Відень.
10. Організація з безпеки і співробітництва в Європі. (2023b). High Commissioner on National Minorities: Mandate and Activities. Гаага.
11. Пундзюте-Галлуа, Е. (2023). The OSCE and the Minsk Process for Ukraine. How Diplomatic Innovation Transforms International Organisations. European Review of International Studies, 10(2), 136–165. <https://doi.org/10.1163/21967415-10020006>
12. Coccaï, M. (2013). Transparency as a Cornerstone of Disarmament and Non-proliferation Regimes. In A. Bianchi & A. Peters (Eds.), Transparency in International Law (pp. 392–416). Cambridge University Press.
13. Вольф, С. (2018). Conflict Management in the OSCE Area. Routledge.
14. Engvall, J. (2021). Transparency and Risk Reduction in European Security. Stockholm International Peace Research Institute.
15. Kulesa, L. (2020). The Future of Conventional Arms Control in Europe. Polish Institute of International Affairs.
16. OSCE Network of Think Tanks and Academic Institutions. (2022). Revitalizing European Security Architecture. Відень.
17. OSCE Yearbook 2021: European Security and Cooperation. (2022). Nomos. <https://doi.org/10.5771/9783748911456>
18. Zellner, W. (2017). OSCE Confidence- and Security-Building Measures: Evolution and Challenges. Institute for Peace Research and Security Policy at the University of Hamburg.

REFERENCES:

1. Engvall, J. (2021). Transparency and risk reduction in European security. Stockholm International Peace Research Institute.
2. Guliyev, F., & Gawrich, A. (2021). OSCE mediation strategies in Eastern Ukraine and Nagorno-Karabakh: A comparative analysis. European Security, 30(4), 569–588. <https://doi.org/10.1080/09662839.2021.1900121>
3. Gurkovskyi, V. I., Romanenko, Ye. O., & Pavlii, N. I. (2026). Teoretychni zasady kontroliu nad zvychnymy ozbroienniamy v Yevropi v umovakh transformatsii bezpekovoho seredovyscha [Theoretical foundations of conventional arms control in Europe in the conditions of security environment transformation]. Natsional'ni interesy Ukrainy, 2(19), 132–151. [https://doi.org/10.52058/3041-1793-2026-2\(19\)-132-151](https://doi.org/10.52058/3041-1793-2026-2(19)-132-151)
4. Härtel, A., Pisarenko, A., & Umland, A. (2021). The OSCE's Special Monitoring Mission to Ukraine: The SMM's work in the Donbas and its Ukrainian critique in 2014–2019. Security and Human Rights, 31(1-4), 121–154. <https://doi.org/10.1163/18750230-03101004>
5. Klymenko, N., & Taran, Ye. (2026). Global and regional security: Control over conventional armaments, humanitarian, social and economic components. Natsional'ni interesy Ukrainy, 2(19), 263–275. [https://doi.org/10.52058/3041-1793-2026-2\(19\)-263-275](https://doi.org/10.52058/3041-1793-2026-2(19)-263-275)
6. Kulesa, L. (2020). The future of conventional arms control in Europe. Polish Institute of International Affairs.
7. Organization for Security and Co-operation in Europe. (1994). Code of Conduct on Politico-Military Aspects of Security. <https://www.osce.org/fsc/41355>

8. Organization for Security and Co-operation in Europe. (2011). Vienna Document 2011 on confidence- and security-building measures. <https://www.osce.org/fsc/41355>
9. Organization for Security and Co-operation in Europe. (2014). OSCE handbook on confidence- and security-building measures. Vienna.
10. Organization for Security and Co-operation in Europe. (2022a). Forum for Security Co-operation: Overview and functions. Vienna.
11. Organization for Security and Co-operation in Europe. (2022b). Revitalizing European security architecture. OSCE Network of Think Tanks and Academic Institutions. Vienna.
12. Organization for Security and Co-operation in Europe. (2023a). Conflict Prevention Centre. OSCE Secretariat. Vienna.
13. Organization for Security and Co-operation in Europe. (2023b). High Commissioner on National Minorities: Mandate and activities. The Hague.
14. OSCE Yearbook 2021: European security and cooperation. (2022). Nomos. <https://doi.org/10.5771/9783748911456>
15. Pundziūtė-Gallois, E. (2023). The OSCE and the Minsk Process for Ukraine. How diplomatic innovation transforms international organisations. *European Review of International Studies*, 10(2), 136–165. <https://doi.org/10.1163/21967415-10020006>
16. Sossai, M. (2013). Transparency as a cornerstone of disarmament and non-proliferation regimes. In A. Bianchi & A. Peters (Eds.), *Transparency in international law* (pp. 392–416). Cambridge University Press.
17. Wolff, S. (2018). *Conflict management in the OSCE area*. Routledge.
18. Zellner, W. (2017). *OSCE confidence- and security-building measures: Evolution and challenges*. Institute for Peace Research and Security Policy at the University of Hamburg.

DSc. of Public Administration. Prof. Gurkovskiy V.

OSCE AS AN INSTITUTIONAL MECHANISM FOR CONFIDENCE-BUILDING, MILITARY TRANSPARENCY, ARMS CONTROL AND CONFLICT PREVENTION IN EUROPE

***Introduction.** In the contemporary European security environment marked by geopolitical fragmentation and the erosion of traditional arms control regimes, trust between States can no longer be viewed as a derivative of political declarations or shared values. It emerges through institutional mechanisms of predictability, in which military transparency plays a central role. The article examines the OSCE as a comprehensive institutional mechanism that integrates military transparency regimes, confidence- and security-building measures, early warning instruments, and conflict resolution tools.*

***Methods.** The study combines the institutional approach with security studies methodology. It employs qualitative comparative analysis of key OSCE documents (Vienna Document 2011, Code of Conduct on Politico-Military Aspects of Security 1994), as well as the activities of the Conflict Prevention Centre, field operations, and the High Commissioner on National Minorities. The instruments are decomposed according to normative, verification, analytical, and mediation dimensions, with emphasis on their interaction.*

***Results.** The effectiveness of the OSCE is shown to stem not from isolated tools but from their interaction, which ensures procedural predictability and reduces the risk of escalation. Key limitations identified include the consensus-based decision-making model, formalization of transparency regimes, fragmentation of military activities below notification thresholds, and insufficient integration between verification data, early warning, and mediation. An original optimization model is proposed, encompassing modernization of notification thresholds, strengthening the analytical autonomy of the Conflict Prevention Centre, introduction of digital verification tools, and closer linkage between monitoring and mediation practices.*

***Conclusions.** The OSCE retains a unique position in the European security architecture as a platform of procedural predictability, yet requires urgent institutional adaptation to conditions of geopolitical fragmentation. Its continued relevance depends on updating military transparency regimes, enhancing analytical and mediation components, and restoring the political will of participating States. The findings are of practical relevance for Ukrainian policy in the fields of European security and arms control.*

***Keywords:** OSCE, military transparency, trust-building, arms control, Vienna Document 2011, conflict prevention, early warning, mediation, European security, verification.*

ДІАЛЕКТИЧНА ВЗАЄМОЗУМОВЛЕНІСТЬ ФЕНОМЕНІВ "БЕЗПЕКА" ТА "НЕБЕЗПЕКА" У КОНТЕКСТІ ВЗАЄМОДІЇ СИСТЕМ РІЗНОЇ ПРИРОДИ

Анотація. З'ясовано, що феномени "безпека" та "небезпека" у контексті взаємодії систем різної природи визначають характер соціальної взаємодії, впливають на всі аспекти суспільного життя та створюють передумови для розвитку механізмів безпеки. Акцентовується увага на тому, що традиційні підходи не враховують діалектичну природу та системний характер впливу фізичних, біологічних і соціальних явищ, які позначають термінами "безпека" та "небезпека", що ускладнює розробку ефективних стратегій забезпечення безпеки систем. Доведено, що діалектичне осмислення безпеки та небезпеки в соціальних системах, дозволяє розглядати їх не лише як об'єктивні фактори, а й як соціальні конструкти, які мають суб'єктивну природу та зумовлюють соціальні взаємодії та що суб'єктивне сприйняття небезпек може не відповідати їхньому реальному змісту, передусім тому, що вказані конструкти відіграють ключову роль у формуванні суспільного уявлення про безпеку та небезпеку, що може призвести до неадекватних управлінських рішень. Обґрунтовано, що важливим є врахування можливого різкого зростання соціальної ентропії, яка призводить до суспільної дестабілізації, та що безпека соціальної системи залежить від особливостей соціальної взаємодії, здатності адаптуватися до нових умов, а баланс між безпекою та небезпекою є визначальним фактором її стійкості, що має враховуватися при розробці відповідних управлінських стратегій. Розкрито роль категорій "сутність" та "явище", особливості використання термінів "поняття" і "концепт" при дослідженні вказаних явищ, а також розуміння спрямованості та системності явищ, які породжують ці феномени. З'ясовано, що застосування діалектичного підходу до розкриття змісту феноменів "безпека" та "небезпека" зумовлює необхідність розуміти під категорією "сутність" внутрішню, глибинну, відносно приховану, стійку сторону досліджуваного об'єкта (процесу), наслідки функціонування якого, інтерпретуються як безпека чи небезпека, а під явищем – категорію, яка відображає зовнішні, більш змінні та очевидні його характеристики. Тому в межах вказаного підходу при розкритті змісту явищ, які інтерпретують як безпеку чи небезпеку, необхідно використовувати термін "концепт". Аналіз змісту діалектичних законів розвитку та парних категорій (необхідність та випадковість; можливість та дійсність), дозволив дійти низки висновків методологічного характеру, зокрема, що зміна фізичних, біологічних та соціальних явищ, які позначають вказаними концептами, відбувається по безальтернативній лінії розвитку, який здійснюється шляхом його роздвоєння на протилежні взаємозумовлені сторони, які відображаються у явищах, серед яких одні здійснюють безпечний, а інші небезпечний вплив на розвиток предмета та що суперечність змісту "небезпека" і "безпека" відображає єдність протилежних сторін тенденцій розвитку предмета й є внутрішнім джерелом його зміни. Доведено, що концепти "небезпека" і "безпека" є дихотомічними, підпорядкованими концепту "розвиток", а їх зміст детермінований середовищем розвитку предмета та що при переході межі можливих кількісних накопичень всередині даної якості предмета відбувається стрибок, наслідком якого є можлива трансформація "безпеки" у "небезпеку" і, навпаки. Акцентовується увага на необхідності виявлення причинно-наслідкового зв'язку явищ, які позначають вказаними концептами тобто чіткого усвідомлення, які саме явища здійснюють або можуть здійснювати, позитивний чи негативний вплив на об'єкт (процес), а відтак є причиною небезпеки чи безпеки. Тому перспективи досліджень вбачаються у розробці засад удосконалення механізмів реагування на різке зростання соціальної ентропії та подальшого розкриття діалектичної сутності явищ, які позначають вказаними концептами, з використанням основних положень теорії хаосу та синергетики.

Ключові слова: безпека, небезпека, соціальний конструкт, система, соціальна взаємодія, соціальний феномен, концепт, явище, сутність, діалектичний підхід, діалектичні закони.

Вступ та постановка проблеми. Проблема забезпечення безпеки систем різної природи традиційно перебуває у колі наукового дискурсу, а частина науковців вважає, що "безпеку" та "небезпеку" при її вирішенні необхідно розглядати як специфічні феномени. Розкриття їх змісту потребує передусім філософського осмислення цих феноменів як ключових категорій, що допомагають досліджувати розвиток фізичних, біологічних і соціальних систем та, відповідно, факторів, які є причинами небезпеки (безпеки). При цьому основна складність полягає у відсутності єдиного підходу, який би дозволив поєднати емпіричні дані про фізичні (природні катаклізми, техногенні аварії тощо), біологічні (інфекції, генетичні зміни тощо) та соціальні фактори (конфлікти, кризи тощо) у контексті генерування ними небезпек для буття систем різної природи з подальшим теоретичним осмисленням їхнього змісту.

Традиційні ж підходи, які використовують при розкритті змісту феноменів "безпека" та "небезпека" та вирішенні проблем забезпечення безпеки систем різної природи в основному базуються на ідеях запобігання небезпекам та створення механізмів щодо їхньої нейтралізації. При цьому при розкритті змісту цих феноменів, як правило, обмежуються інтерпретацією їх визначень у нормативних документах, які є статичними, не враховують діалектичної природи феноменів, їхню взаємозумовленість, єдність і протилежність та багатогранність проявів у реальному світі явищ. Це призводить до ігнорування закономірностей розвитку фізичних, біологічних та соціальних явищ, які позначають термінами "небезпека" та "безпека", породжує суттєві труднощі в пошуках адекватних рішень щодо реагування на них, робить їх фрагментарними, особливо в соціальних системах, де суб'єктивність сприйняття та латентність соціальних явищ, ускладнюють їх прогнозування та контроль і, як наслідок - низької ефективності стратегій реагування на небезпеки. Окрім того, вирішення проблеми забезпечення безпеки систем різної природи ускладнюється досить обмеженою здатністю людини впливати на природні та створені нею штучні фізичні та біологічні системи, які не тільки сприяють вирішенню вказаної проблеми, а й розширюють коло існуючих та ймовірних небезпек для вказаних систем. Глобальні ж зміни у природних системах, технологічний прогрес та соціальна ентропія породжують додаткові труднощі вирішення проблеми.

Водночас, діалектичний підхід є потужним методологічним засобом, який дозволяє глибше зрозуміти безпековий вимір закономірностей розвитку систем різної природи та значною мірою усунути вказані труднощі. Його використання у науково-практичній площині дозволяє поєднати емпіричний рівень аналізу явищ, які породжують безпеки та небезпеки для систем із теоретичним осмисленням їхньої сутності, дозволяє виявити причини та закономірності їх виникнення. Тому актуальним завданням є розкриття сутності та можливостей вказаного підходу при з'ясуванні змісту та діалектичної взаємозумовленості явищ, які позначають термінами "безпека" та "небезпека" у контексті взаємодії систем різної природи (фізичних, біологічних і соціальних) як динамічного процесу, що розширює методологічну базу їх дослідження та розробки безпекових заходів в умовах зростаючої невизначеності та криз характерних для сучасного світу.

Аналіз останніх досліджень і публікацій. Феномени "безпека" та "небезпека" є досить складними та багатоаспектними для однозначного визначення їх змісту фундаментальними категоріями. Водночас, з'ясування їх змісту дозволяє розкрити наслідки та особливості функціонування, розвитку та взаємодії систем різної природи, а для соціальних систем - характер, спрямованість та динаміку соціальних процесів, структурну стабільність суспільства, умови життєдіяльності людини, розвиток цих систем в цілому. Водночас, у сучасному науковому дискурсі терміни "безпека" та "небезпека" використовуються досить часто у різних ракурсах. Так, у роботі [1] вони розглядають як певний стан системи, що визначає її стійкість до небезпек, а у [2] - у контексті деякого процесу у межах якого суспільство реалізує різноманітні заходи щодо реагування на небезпеки людини, суспільству та державі. В деяких роботах, наприклад в [3;4], вказані терміни розглядаються як певний "соціальний конструкт", який формується внаслідок соціальних взаємодій та трансформацій.

Досить часто використовують похідні поняття утворені з використанням термінів "безпека" та "небезпека", наприклад "політична безпека", "воєнна безпека", "економічна безпека" та різні методи виявлення та аналізу небезпек для реагування у відповідній сфері

життєдіяльності суспільства та держави [5-7], а також досліджується взаємозумовленість явищ, які породжують небезпеки та безпеки в сучасному світі [8;9]. Значним також є коло досліджень різних аспектів забезпечення безпеки людини, суспільства та соціальних інститутів, наприклад: забезпечення екологічної безпеки сучасних держав [10]; стану національної безпеки України в контексті гуманітарних, природно-ресурсних, екологічних та техніко-технологічних проблем [11]; політико-правових заходів щодо підвищення стійкості критичної інфраструктури України [12]; шляхів реагування на епідеміологічні загрози [13]; екологічної та біологічної безпеки України [14]. В роботах, які сьогодні є класичними, "безпека" та "небезпека" розглядаються як соціальні феномени та певний "соціальний конструкт", який формується внаслідок сучасних соціальних взаємодій та наслідків глобалізації для людини і суспільства [3;4;15]. Тому в соціальних системах їх все частіше використовують для визначення характеру та інтенсивності соціальних процесів, структурної стабільності та умов розвитку цих систем. Так, у роботі [16] розкривається специфіка соціальних уявлень сучасної молоді про безпеку та небезпеку на різних соціальних рівнях, в [17] розглядається соціокультурна складова безпеки у добу постмодерну, а в роботі [18] наведено системний аналіз соціальних і культурних вимірів ризиків в сучасному суспільстві.

Аналіз наведених праць дозволяє стверджувати про їх значну наукову цінність для розуміння змісту феноменів "безпека" та "небезпека" при вирішенні проблем пов'язаних із забезпеченням безпеки систем різної природи національного, регіонального та глобального масштабів. Водночас, вони: належною мірою не відображають динамічної природи безпеки та небезпеки у контексті взаємодії фізичних, біологічних і соціальних систем; недостатньо розкривають діалектичну взаємозумовленість явищ різної природи, які позначають термінами "безпека" та "небезпека", що не дозволяє виявити справжні причини та закономірності їх розвитку; як правило, використовують нормативні поняття безпеки та небезпеки, які, не відображають їхньої динамічної природи та амбівалентності. Внаслідок цього виникає проблема адаптації цих термінів до наукового аналізу, щоб забезпечити цілісне розуміння сутності та діалектичної взаємозумовленості феноменів "безпека" та "небезпека", а відтак і суттєві труднощі при вирішенні практичних питань щодо безпекових аспектів життєдіяльності людини, суспільства та держави. Важливою передумовою подолання цих труднощів є подальше розкриття діалектичної взаємозумовленості змісту феноменів "безпека" та "небезпека" у контексті взаємодії систем різної природи (фізичних, біологічних та соціальних), що й зумовлює актуальність нашого дослідження.

Мета дослідження полягає у розкритті діалектичної взаємозумовленості феноменів "безпека" та "небезпека" у контексті взаємодії систем різної природи. Головна увага приділена фізичній, біологічній та соціальній складовій безпеці людини та основам діалектичного підходу при розкритті змісту вказаних феноменів.

Виклад основного матеріалу. Фізична складова безпеки людини. Проблема належного реагування на небезпеки людині, які породжувались фізичними явищами у середовищі її існування, виникла разом з її появою на планеті. Йдеться про землетруси, повені, урагани, тайфуни, лісові пожежі, зміни клімату тощо. При цьому можливість людини знизити до прийняттого рівня негативний вплив цих небезпек і сьогодні досить обмежена, оскільки вони відображають ті чи інші якості та властивості фізичних планетарних систем, зумовлених законами природи. Тому людина вимушена пристосовуватися до впливу на її безпеку вказаних явищ використовуючи отримані знання про них та створюючи відповідні штучні фізичні системи. Їх функціонування у заданих параметрах дозволяє людині успішно вирішувати питання пов'язані з її безпекою. Тому такі штучні фізичні системи, як будинки, енергетична, транспортна, промислова інфраструктура та інші мають для неї значну цінність. Проте, створення та функціонування цих систем часто супроводжується значним руйнуванням природних фізичних і біологічних систем, що породжує додаткові небезпеки безпеці людини. Особливо, коли виникають аварії на промислових підприємствах та енергетичних об'єктах, транспортні та екологічні катастрофи техногенного характеру, які призводять, зокрема до значних жертв серед населення, викидів шкідливих речовин, забруднення води, ґрунтів, повітря тощо. Їх соціальні наслідки також можуть бути досить значними, наприклад,

призвести до необхідності вимушеного переселення людей з екологічно небезпечних територій, соціальної нестабільності через зниження довіри до органів державної влади, соціальних конфліктів через нерівний доступ до ресурсів і медичної допомоги, соціального хаосу, панічних настроїв, погіршення криміногенної ситуації. Тому фізична складова небезпеки людини зумовлена не тільки можливим негативним впливом фізичних явищ природного характеру, а й функціонуванням та аваріями (катастрофами) створених нею штучних фізичних систем.

Біологічна складова безпеки людини. Людина, попри найвищий ступінь біологічного розвитку, залишається досить вразливою при взаємодії з іншими формами життя, особливо тими, які перебувають на найнижчому рівні розвитку: бактеріями, вірусами та токсинами, які викликають ті чи інші захворювання. Вони в цілому поділяються на: хвороби від тварин; природно-осередкові інфекції, які вражають тварин і людей; хвороби людини. Ці хвороби зумовлені наслідками функціонування біологічних систем природного походження. Проте вже сьогодні люди активно маніпулюють геномом і протеомом, а це може призвести до небезпеки появи зокрема, абіотичних організмоподібних синтетичних молекулярних систем, стелс-патогенів, які значно розширюють коло небезпек біологічного характеру для людини. Очевидно, що сучасні біотехнології відкривають нові горизонти для медицини та сільського господарства, але вони також створюють і небачені раніше небезпеки. Так, генетично модифіковані організми допомагають у боротьбі з голодом, проте існує значний і до кінця не вивчений ризик непередбачуваних мутацій або екологічного дисбалансу. Створення штучних вірусів або бактерій також може використовуватися як зброя проти людства, а аматорські експерименти із генетичними модифікаціями можуть призвести до неконтрольованих наслідків. Тому для забезпечення належного рівня біобезпеки потрібен жорсткий державний контроль за науковими розробками, вдосконалення механізмів раннього виявлення біологічних небезпек та відповідні міжнародні угоди у цій сфері.

Своєрідним локомотивом розвитку фізичних та біологічних небезпек для людини є зміна клімату, яка є незворотною. Зміна клімату та значні техногенні аварії і катастрофи мають довготривалі наслідки для здоров'я, здійснюють потужний вплив на економічні, політичні та соціальні процеси, на соціальну стабільність, що значно розширює коло небезпек для людини. З метою зниження негативного впливу фізичних і біологічних явищ на безпеку людини, фізичними та біологічними системами можна керувати. Потік енергії чи речовини за певних умов може привести ці системи до бажаного людині стану. Проте реальна здатність людини здійснювати глобальний вплив на природні фізичні та біологічні системи залишається обмеженою.

Соціальна складова безпеки людини. Соціальні явища, які зумовлюють соціальну складову безпеки людини є наслідком їх діяльності та організацій (соціальних інститутів). Вони мають динамічний характер, свої просторові та часові характеристики й проявляються у процесі соціальної взаємодії елементів соціальних систем. Вказаними елементами можуть бути дії, ідеї, думки, почуття, інтереси, потреби, властивості окремих індивідів, соціальні групи, соціальні інститути (організації), соціальні процеси у випадку, коли вони відіграють значну роль у життєдіяльності суспільства, тобто фактично є матеріальними та духовними продуктами людської діяльності. Принципово важливим є те, що будь-яке соціальне явище є результатом взаємодії людей, яка здійснюється в соціальному просторі безпосередньо в контактній групі або опосередковано, через їх причетність до спільнот та через соціальні інститути та, як правило, має латентний характер, тобто вони виражають не тільки очевидні характеристики функціонування соціальних систем, а й більш глибокі процеси, зв'язок яких з соціальним явищем безпосередньо не спостерігається [19].

Науково-прикладний інтерес представляють ті соціальні явища, які характеризують стійкі, повторювані й типові зв'язки та відносини соціальної дійсності. Якщо їх повторюваність, масовість, типовість, суспільна значущість встановлені, то такі явища можна розглядати як соціальний факт [19]. Кількісне вивчення сукупності соціальних явищ, інтенсивності прояву їхніх якісних ознак сприяє усвідомленню ймовірного характеру природи соціальних зв'язків і відносин, що дозволяє зафіксувати закономірності,

особливості та тенденції розвитку явищ в соціальних системах. Таким чином, розкриття сутності соціальних явищ, які позначають термінами "небезпека" або "безпека", має здійснюватися крізь призму дій (взаємодій) людей, здійснюваних безпосередньо або через соціальні інститути, їх потреб, інтересів, які утворюють множину соціальних фактів, які мають матеріальну і духовну визначеність. Тому сутність цих явищ визначається особливостями, динамікою, характером, спрямованістю тощо соціальних взаємодій. Це означає, що вказані соціальні явища формують єдиний динамічний процес виникнення та еволюції соціальних систем, який відбувається згідно законів діалектики [20]. Водночас аналіз соціальних явищ, які позначають термінами "безпека" та "небезпека" у контексті соціальної взаємодії дозволяє дійти висновку, що вони є взаємопов'язаними ключовими категоріями вказаної взаємодії, що впливають на всі аспекти соціального життя. Тому "безпека" та "небезпека" є водночас соціальними феноменами.

Так безпека, як соціальний феномен, охоплює такі її прояви в соціальних взаємодіях як, наприклад: особисту безпеку (захист життя, здоров'я, прав і свобод людини); соціальну безпеку (наявність соціальних гарантій, захист від соціальної ізоляції); політичну безпеку (стійкість політичної системи та встановлених процедур отримання і передачі влади); економічну безпеку (можливість реалізовувати економічні права, мати стабільні доходи). Водночас, небезпека, як соціальний феномен, охоплює такі її прояви в соціальних взаємодіях як, наприклад: конфлікти (міжетнічні, міждержавні тощо); зростання злочинності (зокрема, підвищення рівня насильства та правопорушень); політичну нестабільність (революції, державні перевороти тощо); економічні кризи (безробіття, інфляція тощо). Вказані соціальні феномени здійснюють вплив, зокрема на суспільні та правові норми, політичні та економічні стратегії, культурні цінності тощо, а відтак і на якісно-кількісні характеристики соціальної взаємодії. Тому вони значною мірою визначають характер відносин між людьми, економічну та політичну стабільність. Так, належний рівень безпеки соціальної системи впливає на рівень довіри в суспільстві, що сприяє соціальній мобільності, тобто можливості кожного досягти успіху незалежно від походження чи соціального статусу, а високий рівень небезпеки призводить до соціальної ізоляції, дискримінації, ксенофобії та агресії, створення соціальних бар'єрів, що ускладнюють інтеграцію меншин або вразливих груп.

Таким чином, у кінцевому підсумку, соціальні явища, які позначають концептами "безпека" та "небезпека" є взаємопов'язаними соціальними категоріями та соціальними феноменами. Вони визначають якісно-кількісні характеристики соціальної взаємодії, у тому числі розвиток соціальних інститутів. Тому вони здійснюють вирішальний вплив зокрема, на формування в соціальних системах правових норм, систем управління, рівня довіри між людьми. Це означає, що важливим є пошук та дотримання певного балансу між двома взаємопов'язаними протилежностями, які перебувають у єдності та боротьбі: безпекою та небезпекою. Якщо розглядати цей баланс у контексті соціальної взаємодії, то важливими є зокрема, наступні заходи: розвиток культури безпеки в усіх елементах соціальної системи; розбудова ефективних інститутів безпеки; збереження балансу між свободою та державним контролем; постійне підвищення рівня довіри через відкритий діалог та демократичні процедури і процеси.

Варто акцентувати увагу на тому, що при розробці та реалізації цих та інших заходів, не менш важливим є й врахування змісту та взаємозв'язку соціальних конструктів, яким належить визначальна роль у соціальній взаємодії, а також можливих причин і наслідків різкого зростання соціальної ентропії в умовах криз. Соціальні конструкти віддзеркалюють в елементах соціальної системи поточні уявлення, наприклад про: сенс життя, національні цінності та інтереси, демократичні принципи, ринкову економіку. Вони виникають в силу того, що люди згодні діяти так, ніби ці явища існують, або згодні дотримуватись певних правил поведінки, оскільки, як зазначають П. Бергер та Т. Лукман, індивіди мають знання у вигляді суб'єктивних уявлень і вважають їх реальними, вони не переймаються питаннями, що для них "реально", оскільки вважають "свою реальність" "знаннями", тому люди в різних суспільствах вважають самі по собі зрозумілі їм абсолютно різні "реальності" [3]. Через це осмислення індивідами одних і тих же соціальних явищ, а відтак і змін в соціальних системах,

може бути досить різним. Воно залежить від ідеології, культури, світоглядно-ціннісних орієнтацій тощо. При цьому сутність соціального буття, як зазначав М. Вебер, полягає у наявності в ньому певного сенсу, який також є соціальним конструктом [21]. Соціальні конструкти завжди штучні, проте їх сприйняття масами дозволяє перебудовувати реальність реагуючи на небезпеки (реальні або уявні) своїй безпеці. Оскільки знання людей про оточуючий їх соціальний світ є результатом їх домовленостей, то, в кінцевому підсумку, будь-які соціальні конструкти є для них частиною об'єктивної реальності. Викладене вище повною мірою стосується й соціальних конструктів, які утворюють методологічну основу вирішення проблеми пошуку та дотримання прийняттого балансу між безпекою та небезпекою у контексті соціальної взаємодії.

Не викликає сумніву й важливість виявлення та врахування можливих причин та наслідків різкого зростання соціальної ентропії в умовах криз при розробці та реалізації заходів для забезпечення прийняттого балансу між безпекою та небезпекою у контексті соціальної взаємодії. Як відомо, у фізиці ентропія є мірою хаосу та невпорядкованості. В соціології та теорії управління термін "соціальна ентропія" використовують для характеристики ступеня дезорганізації соціальних систем у процесі поступового накопичення нестабільності та невизначеності в організаційно-функціональних структурах, що призводить до кризових явищ. Будь-які кризові явища в соціальних системах, які зумовлені перманентними якісно-кількісними змінами в них, є об'єктивною реальністю. Ці зміни супроводжуються зростанням соціальної ентропії, що проявляється, коли кризові явища в системі набули ознак системної кризи. Тому суспільство, як дисипативна система, має адекватно реагувати на небезпеку різкого зростання соціальної ентропії.

Визначальними ознаками та характеристиками соціальної ентропії є, зокрема: зниження довіри до держави та суспільних інститутів; фрагментація суспільства; ескалація конфліктів; нестабільність політичних систем; деградація моральних та правових норм. Якщо соціальна ентропія, не контролюється, вона може призвести до тяжких наслідків: політичного хаосу та розпаду держави; розколу суспільства за релігійними, етнічними чи ідеологічними лініями і, як наслідок до громадянської війни; економічного краху; деградації громадянських прав, оскільки у таких умовах, як правило, виникають анархія та диктатури. Тому чим вища соціальна ентропія, тим менш передбачуваним стає розвиток суспільства, а державні інститути можуть втрачати здатність ефективно виконувати свої функції. Різке зростання соціальної ентропії є індикатором зростання нестабільності суспільства, посилює рівень небезпек, пов'язаних з політичними та соціально-економічними кризами. Для її зменшення необхідне адекватне реагування з боку політиків та органів державного управління на фактори, які призводять до її різкого зростання, зокрема, на такі як: політична нестабільність та криза легітимності; економічні дисбаланси та зростання нерівності; маніпуляція суспільною свідомістю; поляризація суспільства; криза ідентичності; масові міграційні процеси; зміна стилю життя та пріоритетів.

В кінцевому підсумку, якщо розглядати еволюцію соціальних систем у контексті соціальних взаємодій, то можна дійти однозначного висновку, що джерелом походження соціальної складової "безпеки" та "небезпеки" є людина та створені нею соціальні інститути. При цьому конфлікти (кризи), які виникають у процесі вказаних взаємодій, є каталізатором змін. Вони можуть призвести як до бажаних, так і не бажаних змін в соціальній системі. Це означає, що термін "конфлікт" взаємопов'язаний з термінами "безпека" та "небезпека". Дійсно, будь-який конфлікт, який виникає у процесі соціальних взаємодій, породжує небезпеки для соціальної системи. Проте, з іншого боку, він зумовлює необхідність реагування на небезпеки, тобто створення відповідних механізмів забезпечення безпеки системи. Конфліктологія як наука досліджує природу конфліктів, їх типологію та методи управління ними [22]. Джерелам конфліктів можуть бути, зокрема: політичні чинники, наприклад, суперечності між органами державної влади та суспільством стосовно пріоритетів розвитку; економічні - зумовлені, наприклад, значною нерівністю у розподілі ресурсів; культурні - основою яких можуть бути розбіжності в світоглядно-ціннісних орієнтаціях. Тому з позицій конфліктології безпеку соціальної системи та її елементів можна розглядати як

процес балансування між їх інтересами (цілями), що вступають у суперечності породжуючи ті чи інші небезпеки для них. Це стосується як деструктивних конфліктів, які створюючи кризові ситуації в системі, так і конструктивних, які можуть сприяти її розвитку, наприклад, шляхом зміни застарілих норм.

Таким чином, сукупність небезпек для безпеки людини фізичного, біологічного та соціального характеру зумовлена багатьма факторами. При цьому безпека та небезпека є феноменами соціальної взаємодії, оскільки впливають на поведінку людей, суспільні відносини, політичні процеси та економічну стабільність. У безпечному середовищі люди більш відкриті до співпраці, довіри та комунікації, тоді як в умовах небезпеки схильні до ізоляції, агресії або підвищеної обережності. Взаємозв'язок цих феноменів із соціальною взаємодією проявляється у різних сферах життя. Тому безпека людини передусім залежить від сприятливих для неї умов середовища існування мінливості яких потребує постійного вжиття відповідних заходів, у тому числі пов'язаних з виявленням, оцінюванням, прогнозуванням, мінімізацією негативних для безпеки людини наслідків фізичних, біологічних та соціальних явищ.

Основи діалектичного підходу при розкритті змісту феноменів "безпека" та "небезпека". Практична реалізація можливостей діалектичного підходу при розкритті змісту цих феноменів зумовлює необхідність розкриття ролі категорій "сутність" та "явище", особливості використання термінів "поняття" і "концепт" та розуміння спрямованості та системності явищ, які породжують вказані феномени

Поняття "сутність" належить до філософських категорій та виражає головне, основне, визначальне в предметі, таке що зумовлене глибинними, необхідними, внутрішніми зв'язками й тенденціями розвитку і пізнається на рівні теоретичного мислення [19]. Як відомо, всі предмети (об'єкти, процеси тощо) постійно змінюються у просторі і часі відповідно до загальних законів розвитку матеріального світу. Тому сутність предмету також змінюється та розвивається відповідно до згаданих законів. Це дозволяє під сутністю розуміти невід'ємну якість предмету, без якої його неможливо осмислити. Сутність предмета виражається в його визначенні. Поняття "явище" також належить до філософських категорій. Його використовують "для позначення зовнішніх властивостей та виявів предметів, що пізнаються на чуттєвому рівні" [19]. Категорії "сутність" та "явище" взаємопов'язані, тому, як і сутність, явище може змінюватися, розвиватися. Проте єдність цих категорій не означає їхньої totoжності, оскільки сутність предметів завжди пов'язана з внутрішнім змістом явищ, а він прихований від безпосереднього сприйняття. Тому у діалектичному матеріалізмі сутність і явище розглядають у діалектичній єдності, як етапи пізнання предметів матеріального світу у процесі якого те чи інше явище відображає певну сторону (якості, властивості) сутності предмету.

В теорії систем реально існуючі системи поділяють на фізичні, біологічні та соціальні, а різні аспекти їх функціонування відображають різноманітні явища, які дозволяють виявити якості та властивості систем зумовлені певними законами (закономірностями) [23]. Так, різні аспекти функціонування фізичних систем відображають фізичні явища, які зумовлені фізичними законами, а різні аспекти функціонування біологічних - біологічні явища. Останні зумовлені як фізичними, так і біологічними законами, що описують статистично вірогідні закономірності, які відбуваються з тілами живої природи. Серед них зокрема, закон незворотності еволюційних процесів, закон стрибкоподібного характеру еволюції, а також біогеохімічні закони, які вивів В. Вернадський [24], зокрема, що еволюція видів повинна йти в напрямку, що збільшує прояв біогенної міграції атомів в біосфері, а відтак в ній право на життя отримують тільки види, необхідні самій біосфері для виконання певних функцій і посилення тим самим біогенної міграції хімічних елементів.

Різні аспекти функціонування соціальних систем відображають соціальні явища, які зумовлені соціальними законами, що описують закономірності, що проявляються у процесі взаємодії соціальних систем та їх елементів. Водночас, при дослідженні цих систем необхідно також врахувати фізичні та біологічні закони, що ускладнює вирішення проблеми забезпечення безпеки цих систем [2]. Проте окремої уваги заслуговують передусім соціальні

явища, тобто ті, які відображають функціонування соціальних систем. В соціології під ними розуміють "усе те в соціальній дійсності, що виявляє себе, розкриває зовнішні, безпосередньо дані форми свого існування; елементи соціальної реальності, яким притаманна вся повнота соціальних властивостей та ознак, універсальні об'єктивні характеристики соціального світу, соціальних об'єктів" [25, стр. 334-335].

Таким чином, в межах діалектичного підходу досліджуючи феномени "безпека" та "небезпека", під сутністю необхідно розуміти внутрішню, глибинну, відносно приховану та стійку сторону об'єкта (процесу), наявні або можливі наслідки функціонування якого (дія), інтерпретуються як безпека чи небезпека стосовно цього або іншого об'єкта (процесу). Тому вказана сутність пізнається тільки на рівні абстрактного мислення й співмірна з такими категоріями як "загальне", "закон". Водночас, під явищем необхідно розуміти категорію, яка відображає зовнішні, більш змінні та очевидні характеристики об'єкта (процесу), тому воно чуттєво сприймається, на відміну від його сутності. Це означає, що пізнати (розкрити) сутність феноменів "безпека" та "небезпека" можна тільки через явища, які відображають різні аспекти функціонування тих чи інших систем.

Щодо особливості використання термінів "поняття" і "концепт", то у нормативній літературі терміни "безпека" та "небезпека" використовуються як поняття, оскільки будь-яке поняття, як правило, передбачає мінімізацію суб'єктивності та варіативності [19]. Це важливо при прийнятті, наприклад, управлінських рішень [19]. Тому зміст поняття є статичним і нормативним, що не дозволяє у науковому сенсі відобразити повною мірою у його змісті істотні властивості, зв'язки, відношення, суперечності, тенденції розвитку об'єктів (процесів) реального світу, наслідком яких є те чи інше явище. Тому при наукових дослідженнях явищ, які інтерпретують як "небезпеку" чи "безпеку", доцільним є вживання терміну "концепт". Як правило, вказані явища відображають різні аспекти функціонування систем, а термін "концепт" має амбівалентну структуру, бо поєднує в собі ціннісну, образну і поняттєву сторони сутності об'єктів, що дозволяє системно розкрити природу явищ, які є причинами безпеки чи небезпеки, тобто дозволяє відобразити у його змісті істотні властивості, зв'язки, відношення, суперечності, тенденції розвитку системи, а відтак передбачає фіксацію ознак і властивостей елементів пізнання системи, особливості її функціонування, які відображають ті чи інші явища.

І, насамкінець, принципово важливим для практичної реалізації можливостей діалектичного підходу є також розуміння спрямованості та системності явищ, які позначають феноменами "безпека" та "небезпека". Як відомо уявлення древньогрецьких філософів, які розглядали світ як такий, що перебуває у вічному становленні, а саме становлення вважали результатом вселенської роздвоєності світу на протилежні сторони (сухе — вологе, добро — зло тощо), єдність та взаємоперехід яких і є джерелом розвитку світу стали ядром діалектики, теоретичні основи якої було викладено в творах Г.Гегеля [20;26]. Зміст діалектики визначається фундаментальними категоріями: зв'язок, взаємодія, рух, розвиток. При цьому вихідним є твердження, що єдність і цілісність матеріального світу полягає у вічних та універсальних взаємозв'язках, а відтак базисною основою діалектики є принцип зв'язку [19]. Категорія "взаємодія", яка відображає процеси взаємовпливу взаємопов'язаних об'єктів, що спричиняє їх взаємну зміну (рух), також має об'єктивний та універсальний характер. Діалектико-матеріалістична концепція розвитку акцентує увагу на властивостях розвитку як процесу: спрямованість змін, їх незворотність, спадковість, виникнення нового, що принципово відрізняє розвиток від руху. Тому розвиток також є базовим принципом діалектики.

Таким чином, Г.Гегель [20;26] сформулював три закони діалектики: єдності та боротьби протилежностей; взаємного переходу кількісних та якісних змін; заперечення заперечення.

Закон єдності та боротьби протилежностей вказує на внутрішнє джерело саморозвитку світу, відповідаючи на питання, чому розвиваються предмети (об'єкти, явища, процеси) реального світу. Протилежність, суперечність, тотожність, відмінність є його категоріями. Вихідною умовою закону є положення про те, що всі предмети є внутрішньо суперечливими і саме ця суперечність являє собою джерело зміни об'єктів, будь-якого руху та розвитку.

Водночас суперечність розглядається не тільки як відношення протилежних сторін, а й як процес їх розгортання в предметі, ступенями якого є тотожність, відмінність, протилежність, конфлікт. Категорія тотожності означає початковий ступінь розвитку суперечності, Поступово вона переходить в стан відмінності, а потім і стан суттєвої відмінності – протилежностей, коли предмет стає відмінним від того, яким він був на стадії тотожності. На останній стадії розвитку суперечності протилежні сторони переходять в стан конфлікту, результатом якого є розв'язання суперечності через зникнення даного предмета та створення предмета нової якості.

Закон взаємного переходу кількісних та якісних змін описує механізм зміни предметів використовуючи категорії: якість, властивість, кількість, міра, стрибок. У даному випадку під якістю розуміється об'єктивна, цілісна, відносно стійка сукупність ознак, які визначають суть та специфіку предмета. Категорія якості знаменує собою відносний спокій, стійкість предмета, тому його якість змінюється дискретно, стрибкоподібно. Категорія кількість відображає параметри предмета, які можна виразити числом та проявляє себе як абсолютний неперервний рух, змінність. Таким чином, специфікою якості є постійність, стійкість, а кількості – абсолютний неперервний рух, змінність. Вказана специфіка є вихідною умовою дії закону взаємного переходу кількісних та якісних змін. Його суть зводиться до того, що кількісні накопичення всередині даної якості, перевищивши міру, з необхідністю викликають якісні зміни, які, в свою чергу, приводять до нових кількісних показників всередині вже нової якості. Після появи нового предмета, його якість надає певний простір для кількісних накопичень, але до певної межі при переході якої відбувається зміна якості предмета.

Закон-заперечення заперечення вказує на напрям розвитку предметів реального світу. Суть закону зводиться до того, що розвиток відбувається через поєднання циклічності та поступальності. Його категоріями є: метафізичне заперечення, діалектичне заперечення, заперечення заперечення, тріада, справедливість, спадковість, спрямованість.

У процесі переходу від старого до нового зі "старим" можна вчинити двояко: знищити його, перервавши перспективу розвитку предмета (метафізичне заперечення); "зняти" старе в новій якості з утриманням в новому позитивного та цінного зі старого (діалектичне заперечення), тому зберігається зв'язок між новим та старим, спадковість, подальша перспектива розвитку предмета. Діалектичне заперечення домінує у розвитку предметів, але вказаний процес не зупиняється на ньому. Для завершення дії закону необхідно щоб процес пройшов стадію заперечення заперечення. Воно означає: утримання та синтез позитивного з вихідного пункту та його діалектичного заперечення, коли долається їх односторонність і створюється вища цілісність; повернення начебто до старого, але на новій, більш якісній основі. Заперечення заперечення є новим вихідним пунктом для подальшого розвитку об'єкта.

Крім законів, теорія діалектики включає в себе низку важливих категорій. Вони є об'єктивними за змістом, суб'єктивними за формою і бувають парними та непарними. Основні закони діалектики формулюються тільки через непарні категорії: суперечність, кількість, якість, заперечення тощо. До парних категорій діалектики належать: загальне та одиничне, причина та наслідок, необхідність та випадковість, сутність та явище, зміст та форма, дійсність та можливість. Категорії сутність та явище ми розглядали вище. Разом з тим для розкритті діалектичної сутності явищ, які позначають концептами "безпека" та "небезпека" доцільно окреслити зміст таких парних категорій як: причина та наслідок; необхідність та випадковість; можливість та дійсність.

Під причиною розуміється явище, дія якого з необхідністю приводить до виникнення іншого явища, яке називається наслідком. Причина завжди передує наслідку. Вона викликає його, але й наслідок чинить зворотний вплив на причину, оскільки стає причиною іншого наслідку. Матеріальний світ "пронизаний" причинно-наслідковими ланцюгами. Вони складають зміст твердження, що в світі абсолютно все має свою причину (принцип детермінізму). У межах нашого дослідження це означає, що внаслідок взаємодії фізичних, біологічних та соціальних систем можуть виникати явища, які ми позначаємо концептами "безпека" та "небезпека", тобто ці явища є причинами безпеки чи небезпеки для реальних об'єктів (процесів).

Важливим для розкритті сутності явищ, які позначають концептами "безпека" та "небезпека", крізь призму безальтернативній лінії розвитку, є також врахування таких парних категорій як: необхідність та випадковість та можливість та дійсність. Під необхідністю розуміється розвиток явищ, який випливає із внутрішнього стійкого зв'язку об'єктів і має бути неминучим, а випадковість визначає проблематичність та необов'язковість виникнення об'єктів, її неможливо точно передбачити. Випадковість є формою вияву необхідності та її доповненням і може лише прискорювати або сповільнювати необхідний процес. Під можливістю розуміється об'єктивно існуюча тенденція виникнення об'єкта, яка зумовлена певною закономірністю, а під дійсністю реалізована можливість. При цьому кожна дійсність знову породжує "віяло можливостей", з яких реалізується (стає новою дійсністю) лише одна реальна, яка виявляє закономірну, суттєву тенденцію розвитку даного об'єкта.

Аналіз окресленого змісту діалектичних законів розвитку предметів реального світу, а також парних категорій (необхідність та випадковість; можливість та дійсність), дозволяє дійти наступних висновків методологічного характеру принципово важливих у науково-практичному сенсі при розкритті сутності та діалектичної взаємозумовленості явищ, які позначають концептами "безпека" та "небезпека".

1. Зміна фізичних, біологічних та соціальних явищ, які позначають концептами "безпека" та "небезпека", відбувається по безальтернативній лінії розвитку, а їх визначальними рисами є системність, впорядкованість, закономірність та необхідність, тобто ці зміни є процесом, що здійснюється за законами логіки та необхідності. Тому у змінах вказаних явищ не може бути панування випадковостей, які визначають необов'язковість виникнення змін, які неможливо передбачити. Ті чи інші випадковості можуть лише прискорювати або сповільнювати необхідний закономірний процес змін.

2. Розвиток предметів реального світу здійснюється шляхом його роздвоєння на дві протилежні, але взаємозумовлені сторони, які у загальному випадку, знаходять своє відображення у фізичних, біологічних та соціальних явищах. Ці явища здійснюють позитивний або негативний вплив на розвиток. Одні явища породжують небезпеки (перепони, шкоду тощо) для розвитку предмета (його структури, взаємодії із середовищем тощо), тобто їх вплив є негативним. Інші явища сприяють створенню належних умов (енергетичних, ресурсних тощо) для розвитку предмета, тобто їх вплив є позитивним (безпечним).

3. Суперечність між фізичними, біологічними та соціальними явищами, для позначення яких використовують концепти "небезпека" і "безпека", відображає єдність протилежних сторін тенденцій розвитку предмета і постійну боротьбу між ними. Вона є внутрішнім джерелом зміни та розвитку предмета. Це означає, що взаємовідносини між вказаними явищами є джерелом внутрішнього імпульсу змін, які зумовлюють розвиток предмета, тобто перетворення його в інший.

4. Концепти "небезпека" і "безпека", які використовують для позначення фізичних, біологічних та соціальних явищ, які здійснюють вплив на розвиток предмета, є дихотомічними та підпорядкованими концепту "розвиток". Тому об'єктивний зміст цих концептів детермінований середовищем та обставинами, в яких відбувається розвиток предмета. Ці явища взаємодіють у процесі кількісних та якісних змін явищ, що об'єктивно зумовлює системний характер якісно-кількісних характеристик як "небезпеки", так і "безпеки" й дозволяє, зокрема, здійснювати їх класифікацію та оцінювання за інтенсивністю, масштабами тощо.

5. Фізичні, біологічні та соціальні явища, які позначають концептами "безпека" та "небезпека", вирізняються певною якістю, яка є об'єктивною, цілісною, відносно стійкою сукупністю ознак. Ці ознаки визначають суть та специфіку явища та проявляється через властивості, які є способом виявлення певної сторони явища по відношенню до інших, з якими воно вступає у взаємодію. Кількісні накопичення всередині даної якості до перевищення міри (межі), за якою з необхідністю виникають якісні зміни явищ, породжують безперервний процес зміни інтенсивності впливу цих явищ на якісно-кількісні характеристики як безпеки, так і небезпеки. При переході межі, до якої можуть бути можливими кількісні накопичення в явищах, відбувається стрибок, тобто зміна якості цих явищ. Його логічним наслідком є

можлива трансформація ("перетікання") "безпеки" у "небезпеку" і, навпаки. У даному випадку проявляється дія закону заперечення заперечення. Тобто у процесі трансформації відбувається утримання та синтез позитивного з вихідного пункту розвитку явищ, які позначають концептами "безпека" та "небезпека", та його діалектичне заперечення, коли долається їх односторонність і створюється вища цілісність на новій, більш якійсній основі.

6. В науково-практичному сенсі при виявленні та оцінюванні явищ, які позначають концептами "безпека" та "небезпека", принципово важливим є розкриття причинно-наслідкового зв'язку явищ. Тобто необхідно чітко усвідомлювати, які саме явища здійснюються, або можуть здійснюватися, позитивний чи негативний вплив на об'єкт (процес), а відтак є причиною небезпеки чи безпеки. У цьому ж контексті важливими є й відповіді на питання: які явища є неминучими, а які випадковими, а також, які з потенційних можливостей розвитку є реальними, тобто такими, що уособлюють закономірну та суттєву тенденцію розвитку явища.

Наведені висновки, які ґрунтуються на філософській концепції розвитку, дозволяють значною мірою розкрити діалектичну сутність явищ, які позначають концептами "безпека" та "небезпека". Проте сьогодні при визначенні траєкторій безпечного розвитку предметів (об'єктів, процесів) необхідно використовувати й наукові положення інших теорій (концепцій), які досліджують системи. Йдеться зокрема, про теорію хаосу, яка досліджує системи, динаміка яких залежить від початкових умов, що робить довгострокове прогнозування їх розвитку складним та синергетику, в межах якої досліджують процеси самоорганізації в системах різної природи у контексті сумісної дії елементів середовища у нерівноважному стані [27]. Тому подальше розкриття діалектичної сутності явищ, які позначають концептами "безпека" та "небезпека", потребує додаткових досліджень.

Таким чином, розкриття сутності та можливостей діалектичного підходу до розкриття змісту та взаємозумовленості явищ, які позначають концептами "безпека" та "небезпека", дозволяє осмислити безпековий вимір закономірностей розвитку та функціонування систем різної природи, а його практичне використання - поєднувати емпіричний рівень аналізу цих явищ із теоретичним осмисленням їхньої сутності. У даному випадку, наприклад, закон єдності та боротьби протилежностей проявляється у тому, що явище, яке позначають категорією "безпека" не може існувати без явища, яке позначають категорією "небезпеки", яке власне й породжує потребу у вдосконаленні відповідних механізмів захисту системи. Закон переходу кількісних змін у якісні проявляється передусім у тому, що "накопичення" "небезпек" в системі на певному етапі призводить до кризової ситуації, що потребує суттєвих змін в системі, а в певних випадках і її трансформації для переведення на більш безпечну траєкторію розвитку. Взаємозумовленість "небезпеки" та "безпеки", як двох протилежностей, проявляється відповідно до закону заперечення заперечення, оскільки попередня система еволюціонує через подолання (заперечення) тих чи інших "небезпек" та створення нової структури системи, яка дозволяє забезпечувати їй прийнятний баланс між явищами, які інтерпретуються як "безпеки" та "небезпеки".

Висновки. 1. У контексті аналізу взаємодії систем різної природи встановлено, що безпека та небезпека є взаємопов'язаними феноменами, які в соціальних системах визначають характер соціальної взаємодії. Вони не існують окремо один від одного, оскільки небезпека створює передумови для розвитку механізмів безпеки, а накопичення небезпек у системі може призводити до криз, які стимулюють її трансформацію. При цьому використання підходів, які не враховують діалектичну природу, динамічний характер, системний характер впливу фізичних, біологічних і соціальних явищ, які позначають термінами "безпека" та "небезпека", ускладнює розробку ефективних стратегій забезпечення безпеки цих систем.

2. Діалектичне осмислення безпеки та небезпеки в соціальних системах, дозволяє розглядати їх не лише як об'єктивні фактори, а й як соціальні конструкти, які мають суб'єктивну природу та зумовлюють соціальні взаємодії, а природні катаклізми, техногенні катастрофи, епідемії та соціальні кризи розширюють коло небезпек для систем різної природи, що вимагає розробки адаптивних підходів для реагування на ці небезпеки. При цьому суб'єктивне сприйняття небезпек може не відповідати їхньому реальному змісту, передусім тому, що соціальні конструкти відіграють ключову роль у формуванні суспільного уявлення

про безпеку та небезпеку, що може призвести до неадекватних управлінських рішень. Важливим у даному випадку є й врахування можливого різкого зростання соціальної ентропії, яка призводить до суспільної дестабілізації.

3. Безпека соціальної системи залежить від особливостей соціальної взаємодії та її здатності адаптуватися до нових умов, а баланс між безпекою та небезпекою є визначальним фактором стійкості систем. Це має враховуватися при розробці управлінських стратегій пріоритетами яких мають бути зокрема, розвиток культури безпеки, створення ефективних інститутів безпеки, збереження балансу між свободою та державним контролем, формування механізмів запобігання кризовим явищам, підвищення рівня довіри у суспільстві, як важливого чинника соціальної стабільності.

4. Розкрито сутність та можливості використання діалектичного підходу при розкритті змісту феноменів "безпека" та "небезпека" шляхом розкриття ролі категорій "сутність" та "явище", особливості використання термінів "поняття" і "концепт" та розуміння спрямованості та системності явищ, які породжують вказані феномени. Застосування діалектичного підходу до розкриття змісту феноменів "безпека" та "небезпека" зумовлює необхідність розуміти під категорією "сутність" внутрішню, глибинну, відносно приховану, стійку сторону того чи іншого досліджуваного об'єкта (процесу), наслідки функціонування якого, інтерпретуються як безпека чи небезпека, а під явищем – категорію, яка взаємопов'язана з категорією "сутність" та відображає зовнішні, більш змінні та очевидні його характеристики. Тому в межах вказаного підходу при розкритті змісту явищ, які відображають специфіку та варіативну оціночну характеристику розвитку систем (об'єктів, процесів) та які інтерпретують як безпеку чи небезпеку, необхідно використовувати термін "концепт".

5. Аналіз змісту діалектичних законів розвитку предметів реального світу та парних категорій (необхідність та випадковість; можливість та дійсність), дозволяв дійти низки висновків методологічного характеру. Так, зміна фізичних, біологічних та соціальних явищ, які позначають концептами "безпека" та "небезпека", відбувається по безальтернативній лінії розвитку, який здійснюється шляхом його роздвоєння на протилежні взаємозумовлені сторони, тобто ці концепти є дихотомічними, підпорядкованими концепту "розвиток", зміст якого детермінований середовищем розвитку предмета. При цьому явища, які позначають вказаними концептами, вирізняються певною якістю, яка є об'єктивною, цілісною, відносно стійкою сукупністю ознак, які визначають специфіку явища (системність, впорядкованість, закономірність та необхідність), тобто ці зміни є процесом, що здійснюється за законами логіки та необхідності, а ті чи інші випадковості можуть лише прискорювати або сповільнювати необхідний закономірний процес змін. При переході ж межі можливих кількісних накопичень всередині даної якості можлива трансформація ("перетікання") "безпеки" у "небезпеку" і, навпаки.

6. З'ясовано, що в науково-практичному сенсі при виявленні та оцінюванні явищ, які позначають концептами "безпека" та "небезпека", принципово важливим є розкриття причинно-наслідкового зв'язку явищ. Тобто необхідно чітко усвідомлювати, які саме явища здійснюють, або можуть здійснювати, позитивний чи негативний вплив на об'єкт (процес), а відтак є причиною небезпеки чи безпеки. У цьому ж контексті важливими є й відповіді на питання: які явища є неминучими, а які випадковими, а також, які з потенційних можливостей розвитку є реальними, тобто такими, що уособлюють закономірну та суттєву тенденцію розвитку явища. Отримані висновки, які ґрунтуються на філософській концепції розвитку, дозволяють значною мірою розкрити діалектичну сутність явищ, які позначають концептами "безпека" та "небезпека". Проте сьогодні при визначенні траєкторій безпечного розвитку предметів (об'єктів, процесів) необхідно використовувати й наукові положення інших теорій (концепцій), які досліджують системи. Тому перспективи подальших досліджень вбачаються у розробці засад удосконалення механізмів реагування на різке зростання соціальної ентропії та розкриття діалектичної сутності явищ, які позначають концептами "безпека" та "небезпека" з використанням основних положень теорії хаосу та синергетики.

ЛІТЕРАТУРА:

1. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол. С. І. Пирожков, О. М. Майборода, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, В. А. Смолій, О. В. Скрипнюк, С. В. Стоєцький / Інст. політ. і етнонац. дослідж. ім. І. Ф. Кураса НАН України. К.: 2022. 552 с.
2. Качинський А.Б. Безпека складних систем: моногр. / за ред. С.О. Довгого. К.: ТОВ "Видавництво "ЮСТОН", 2017. 468 с.
3. Berger, P. L., & Luckmann, T. (1966). The Social Construction of Reality: A Treatise in the Sociology of Knowledge. New York: Anchor Books. URL: https://ia903203.us.archive.org/4/items/BergerSocialConstructionOfReality_201901/Berger%20social-construction-of-reality.pdf
4. Hidens E. (2008). Transformatsiia suspilstva: Sotsiolohiia bezpeky ta ryzyku. [Transforming Society: The Sociology of Security and Risk]. K.: Vydavnytstvo "KM Akademiia". 368 s.
5. Орел М.Г. Теоретичні основи державного управління у сфері політичної безпеки: моногр. К.: "Поліграф плюс", 2019. 320 с.
6. Безпекове середовище 2033: моногр. К.: НУОУ імені Івана Черняхівського, 2022. 117 с.
7. Актуальні виклики та загрози економічній безпеці України в умовах воєнного стану. К.: НІСД. URL: <https://niss.gov.ua/publikatsiyi/analitichni-dopovidi/aktualni-vyklyky-ta-zahrozy-ekonomichniy-bezpetsi-ukrayiny-v>.
8. Бех В. П. Безпека життєдіяльності: теоретичні основи. К.: Видавництво "Знання", 2008. 415 с.
9. Тоффлер Е. Шок майбутнього / Пер. з англ. К.: Вид-во "Всесвіт", 1997. 557 с.
10. Радченко О. О. Екологічна безпека сучасних держав в умовах глобальних викликів і загроз // Публічне урядування, 2022. №3 (28) С. 73-81. [https://doi.org/10.32689/2617-2224-2021-3\(28\)-11](https://doi.org/10.32689/2617-2224-2021-3(28)-11)
11. Національна безпека України у викликах новітньої історії : колективна монографія / авт.-уклад. В. І. Шпак; кер. авт. кол. С. І. Табачников. К. : ДП "Експрес-об'ява", 2020. 464 с.
12. Дуліна О.В., Ровинська К.І., Сліпенюк В.В. Політико-правові заходи для підвищення стійкості критичної інфраструктури України в контексті адаптації до глобальних викликів // Національні інтереси. 2024. №6. С.73-86. URL: [https://doi.org/10.52058/3041-1793-2025-1\(6\)-73-86](https://doi.org/10.52058/3041-1793-2025-1(6)-73-86)
13. Ковальчук Л. В. Епідеміологічні загрози: сучасні виклики та шляхи протидії: монографія. К.: НМУ імені О. О. Богомольця, 2020. 312 с.
14. Екологічна та біологічна безпека України: колективна монографія / за науковою редакцією О.І. Дребот, А.І. Парфенюк. К.: Видавництво НУБІП України, 2022. 322 с.
15. Бауман З. Глобалізація. Наслідки для людини і суспільства / Пер. з англ. І. Андрущенко; за наук. ред. М. Винницького. К.: Вид. дім "Києво-Могилянська академія", 2008. 109 с.
16. Дроздова М.А. Регіональні особливості соціальних уявлень студентської молоді про безпеку й небезпеку // Науковий вісник ХДУ Серія Психологічні науки. 2019. № 1. С.211-216. URL: <https://doi.org/10.32999/ksu2312-3206/2019-1-35>
17. Ананьїн В.О., Горлинський В.В. Суспільство ризику: соціокультурний вимір безпеки //Мультиверсум. Філософський альманах. 2023. Випуск 2(178). Том 1. С.34-50. DOI 10.35423/2078-8142.2023.2.1.2
18. Ризики в сучасному нестабільному суспільстві: соціальні і культурні виміри: монографія / за ред. Л.Г. Скокової. К.: Ін-т соціології НАН України 2021. 295 с.
19. Філософський енциклопедичний словник / В. І. Шинкарук (гол. редкол.) та ін ; Інститут філософії імені Григорія Сковороди НАН України. К.: Абрис, 2002. 742 с.
20. Гегель Г. В. Ф. Наука логіки. К.: Юніверс, 2001. 496 с.
21. Вебер. М. Соціологія. Загальноісторичні аналізи. К.: Політика, 1998. 321 с.
22. Гарькавець С.О. Соціальні конфлікти: словник-довідник, Сєвєродонецьк: Вид-во СНУ ім. В. Даля, 2020. 120 с.
23. Берталанфі Л. Загальна теорія систем. К.: Вид-во "Либідь", 2000. 320 с.
24. Вернадський В. І. Біосфера і ноосфера. К.: Наукова думка, 1989. 262 с.
25. Соціологія: словник термінів і понять / Є.А.Біленький, В.М.Дебой, М.А.Козловець та ін. [уклад.] / за заг. ред. Біленького Є.А. і Козловця М.А. К.: Кондор, 2006. 372 с.
26. Гегель Г. В. Ф. Феноменологія духу. К.: Вид-во Соломії Павличко "Основи", 2004. 548 с.
27. Пригожин І., Стенгерс І. Порядок із хаосу: Новий діалог людини з природою. К.: Наукова думка, 1994. 296 с.

REFERENCES:

1. Pyrozhkov, S.I., Maiboroda, O.M., Khamitov, N.V., Holovakha, Ye.I., Dembitskyi, S.S., Smolii, V.A., Skrypniuk, O.V., & Stoietyskyi, S.V. (Eds.). (2022). *Natsionalna stiikist Ukrainy: stratehiia vidpovidi na vyklyky ta vyperedzhennia hibrydnykh zahroz: natsionalna dopovid* [National resilience of Ukraine: strategy for responding to challenges and preventing hybrid threats: national report]. Kyiv: Inst. polit. i etnonats. doslidzh. im. I. F. Kurasa NAN Ukrainy. 552 s. [in Ukrainian].
2. Kachynskyi A.B. *Bezpeka skladnykh system: monohr. / za.red. S.O. Dovhoho. K.: TOV "Vydavnytstvo "IuSTON", 2017. 468 s. [in Ukrainian].*
3. Berger, P. L., & Luckmann, T. (1966). *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. New York: Anchor Books. URL: https://ia903203.us.archive.org/4/items/BergerSocialConstructionOfReality_201901/Berger%20social-construction-of-reality.pdf [in English].
4. Hidens E. (2008). *Transformatsiia suspilstva: Sotsiologiia bezpeky ta ryzyku. [Transforming Society: The Sociology of Security and Risk]*. K.: Vydavnytstvo "KM Akademiia". 368 s. [in English].
5. Orel M.H. *Teoretychni osnovy derzhavnoho upravlinnia u sferi politychnoi bezpeky: monohr. K.: "Polihraf plius", 2019. 320 s. [in Ukrainian].*
6. *Bezpekove seredovyshe 2033: monohr. (2022) [Security environment 2033: monograph]*. K.: NUOU imeni Ivana Cherniakhovskoho. 117 s. [in Ukrainian].
7. *Aktualni vyklyky ta zahrozy ekonomichnii bezpetsi Ukrainy v umovakh voiennoho stanu [Actual challenges and threats for economic security of Ukraine in conditions of martial law]*. (n.d.). Natsionalnyi instytut stratehichnykh doslidzen – National Institute for Strategic Studies. Retrieved from <https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/aktualni-vyklyky-ta-zahrozy-ekonomichniy-bezpetsi-ukrayiny-v> [in Ukrainian].
8. Бех В. П. *Безпека життєдіяльності: теоретичні основи*. К.: Видавництво "Знання", 2008. 415 с.
9. Тоффлер Е. *Шок майбутнього / Пер. з англ. К.: Вид-во "Всесвіт", 1997. 557 с.*
10. Radchenko O. O. (2022). *Ekolohichna bezpeka suchasnykh derzhav v umovakh hlobalnykh vyklykiv i zahroz [Environmental security of modern states in the face of global challenges and threats]*. // *Publichne uriaduvannia. №3 (28). S. 73-81. URL: [https://doi.org/10.32689/2617-2224-2021-3\(28\)-11](https://doi.org/10.32689/2617-2224-2021-3(28)-11) [in Ukrainian].*
11. Shpak, V. I., S. I. Tabachnikov. K. et. al. (Eds.) (2020). *Nationalna bezpeka Ukrainy: vyklyky suchasnoii ostorii [National security of Ukraine in the challenges of modern history]*. kolektyvna monohrafiia: DP "Ekspres-obiava". 464 s. [in Ukrainian].
12. Dulina O.V., Rovynska K.I., Slipeniuk V.V. (2024) *Polityko-pravovi zakhody dlia pidvyshchennia stiikosti krytychnoi infrastruktury Ukrainy v konteksti adaptatsii do hlobalnykh vyklykiv [Policy and legal measures to increase the resilience of Ukraine's critical infrastructure in the context of adaptation to global challenges]* // *Natsionalni interesy. №6. S.73-86. URL: [https://doi.org/10.52058/3041-1793-2025-1\(6\)-73-86](https://doi.org/10.52058/3041-1793-2025-1(6)-73-86) [in Ukrainian].*
13. Kovalchuk L. V. (2020). *Epidemiolohichni zahrozy: suchasni vyklyky ta shliakhy protydii [Epidemiological threats: modern challenges and ways to counter them]*. K.: NMU imeni O. O. Bohomoltsia. 312 s. [in Ukrainian].
14. Drebot O.I., Parfeniuk A.I. (Eds.). (2022) *Ekolohichna ta biolohichna bezpeka Ukrainy. [Social tension in a crisis society]: kolektyvna monohrafiia. K.: Vydavnytstvo NUBIP Ukrainy. 322 s. [in Ukrainian].*
15. Bauman Z. (2008). *Hlobalizatsiia. Naslidky dlia liudyny i suspilstva [Globalization. Consequences for individuals and society] / per. z anh. I. Andrushchenka; za nauk. red. M. Vynnytskoho. K.: Vyd. dim "Kyievo-Mohylianska akademiia". 109 s. [in Ukrainian].*
16. Drozdova M.A. (2019). *Rehionalni osoblyvosti sotsialnykh uiavlen studentskoi molodi pro bezpeku y nebezpeku [Regional features of social perceptions of student youth about safety and danger]* // *Naukovyi visnyk KhDU Serii Psykholohichni nauky. № 1. S.211-216. URL: <https://doi.org/10.32999/ksu2312-3206/2019-1-35> [in Ukrainian].*
17. Ananin V.O., Horlynskyi V.V. (2023). *Suspilstvo ryzyku: sotsiokulturnyi vymir bezpeky. [Risk Society: The Sociocultural Dimension of Security]* // *Multyversum. Filosofskyi almanakh. Vypusk 2(178). Tom 1. S. 34-50. DOI 10.35423/2078-8142.2023.2.1.2[in Ukrainian].*
18. Skokova L.H. (Ed.) (2021). *Ryzyky v suchasnomu nestabilnomu suspilstvi: sotsialni i kulturni vymiry [Risks in a modern unstable society: social and cultural dimensions]: monohrafiia. K.: In-t sotsiologi NAN Ukrainy. 295 s. [in Ukrainian].*

19. Shynkaruk V. I. (Ed. & et. al). (2002). *Filosofskyi entsyklopedychnyi slovnyk* [Philosophical encyclopedic dictionary]. Instytut filosofii imeni Hryhoriia Skovorody NAN Ukrainy. K.: Abrys. 742 s. [in Ukrainian].
20. Hehel H.V.F. (2001). *Nauka lohiky*. [The science of Logic]. K.: Yunivers, 2001. 496 s. [in Ukrainian].
21. Veber M. (1998). *Sotsiologhiia. Zahalnoistorychni analiz*. [Sociology. General historical analyses]. K.: Polityka. 321 s. [in Ukrainian].
22. Harkavets S.O. (2020) *Sotsialni konflikty: slovnyk-dovidnyk*. [Social conflicts: dictionary-reference]. Sievierodonetsk: Vyd-vo SNU im. V. Dalia. 120 s. [in Ukrainian].
23. Bertalanfi, L. (2000). *Zahalna teoriia system*[General theory of systems]. "Lybid" [in Ukrainian].
24. Vernadskyi, V. (1989). *Biosfera i noosfera*[Naukova dumkaBiosphere and noosphere]. Scientific opinion [in Ukrainian].
25. Belenky, E. A., Deboy, V. M., Kozlovets, M. et. al. (2006). *Sotsiologhiia: slovnyk terminiv i poniat* [Sociology: a dictionary of terms and concepts]. Condor [in Ukrainian].
26. Hegel G. (2004). *Fenomenologhiia dukhu*[Phenomenology of spirit], Publishing House of Solomia Pavlychko "Osnovy" [in Ukrainian].
27. Prigozhin, I., & Stengers, I. (1994). *Poriadok iz khaosu: Novyi dialoh liudyny z pryrodou*[Order from Chaos: A New Dialogue between Man and Nature], Naukova dumka [in Ukrainian].

S. A., DSc., prof. Sytnyk H.

DIALECTICAL INTERDEPENDENCE OF THE CONCEPTS 'SECURITY' AND 'DANGER' IN THE CONTEXT OF INTERACTION BETWEEN SYSTEMS OF DIFFERENT NATURES

Abstract. *It is found that the phenomena of "safety" and "danger" in the context of the interaction between the systems of different natures determine the nature of social interaction, affect all aspects of social life, and that danger creates the prerequisites for the development of security mechanisms. It is emphasized that traditional approaches do not take into account the dialectical nature and systemic nature of the influence of physical, biological, and social phenomena, which are denoted by the terms "safety" and "danger", which complicates the development of effective strategies for ensuring the security of systems. It has been proven that the dialectical understanding of safety and danger in social systems allows us to consider them not only as objective factors, but also as social constructs that are subjective in nature and determine social interactions, and that the subjective perception of dangers may not correspond to their real content, primarily because these constructs play a key role in shaping the public perception of safety and danger, which can lead to inadequate management decisions. It is substantiated that it is important to take into account the possible sharp increase in social entropy, which leads to social destabilization, and that the security of the social system depends on the characteristics of social interaction, the ability to adapt to new conditions, and the balance between security and danger is a determining factor of its stability, which should be taken into account when developing appropriate management strategies. The role of the categories "essence" and "phenomenon", the features of the use of the terms "notion" and "concept" in the study of these phenomena, as well as understanding the direction and systematicity of the phenomena that generate these phenomena, is revealed. It is found out that the use of a dialectical approach to revealing the content of the phenomena "safety" and "danger" necessitates the need to understand the category "essence" as the internal, deep, relatively hidden, stable side of the object (process) under study, the consequences of the functioning of which are interpreted as safety or danger, and the phenomenon as a category that reflects its external, more variable and obvious characteristics. The role of the categories "essence" and "phenomenon", the features of the use of the terms "notion" and "concept" in the study of these phenomena, as well as understanding the direction and systematicity of the phenomena that generate these phenomena, is revealed. It is found out that the use of a dialectical approach to revealing the content of the phenomena "safety" and "danger" necessitates the need to understand the category "essence" as the internal, deep, relatively hidden, stable side of the object (process) under study, the consequences of the functioning of which are interpreted as safety or danger, and the phenomenon as a category that reflects its external, more variable and obvious characteristics. Therefore, within the framework of the indicated approach, when revealing the content of phenomena that are interpreted as safety or danger, it is necessary to use the term "concept". The analysis of the content of the dialectical laws of development and paired*

categories (necessity and chance; possibility and reality) allowed us to reach a number of methodological conclusions, in particular, that the change in physical, biological and social phenomena, which are denoted by the above concepts, occurs along an unalternative line of development, which is carried out by its bifurcation into opposite mutually conditioned sides, which are reflected in phenomena, among which some have a safe and others a dangerous influence on the development of the subject, and that the contradiction in the content of "danger" and "safety" reflects the unity of the opposite sides of the tendencies of the development of the subject and is an internal source of its change. It is proven that the concepts of "danger" and "safety" are dichotomous, subordinate to the concept of "development", and their content is determined by the environment of the development of the object and that when crossing the boundary of possible quantitative accumulations within a given quality of the object, a jump occurs, the consequence of which is the possible transformation of "safety" into "danger" and vice versa. Attention is focused on identifying the cause-and-effect relationships of the phenomena denoted by the specified concepts, that is, a clear awareness of which phenomena have or can have a positive or negative impact on the object (process) and therefore are the cause of danger or safety.

Therefore, research prospects are seen in the development of principles for improving mechanisms for responding to a sharp increase in social entropy and further revealing the dialectical essence of the phenomena denoted by the above concepts, using the basic principles of chaos theory and synergetics.

Keywords: security, danger, social construct, system, social interaction, social phenomenon, concept, phenomenon, essence, dialectical approach, dialectical laws.

ІНСТИТУЦІЙНА ІНЕРЦІЯ ТА СТІЙКІСТЬ ПОЛІТИЧНОЇ СИСТЕМИ УКРАЇНИ В УМОВАХ ВІЙНИ: АНАЛІЗ ЧЕРЕЗ ПРИЗМУ PATH DEPENDENCE

Стаття присвячена впливу інституційної інерції та залежності від раніше пройденого шляху (path dependence) на ефективність і стійкість політичної системи України в умовах повномасштабної війни. Обґрунтовано, що радянська адміністративна спадщина, неформальні практики управління, патронально-клієнтельські мережі та централізована модель ухвалення рішень формують довготривалі траєкторії інституційного розвитку, які істотно обмежують адаптивність системи публічного управління та її здатність до швидкого реагування на кризові виклики. Показано, що війна виступає критичною точкою (critical juncture), яка одночасно загострює структурні вразливості політичної системи та відкриває можливості для інституційного оновлення, прискорення цифровізації, реформування сектору безпеки, зміцнення міжвідомчої координації та посилення горизонтальних механізмів взаємодії держави й суспільства.

Особливу увагу приділено ролі децентралізації, громадянської мобілізації, волонтерських мереж і розвитку локальної демократії як ключових чинників формування інституційної резилієнтності, здатної компенсувати негативні ефекти path dependence та забезпечувати стійкість держави в умовах тривалих загроз. На основі аналізу сучасних підходів до resilience, crisis governance, системної безпеки та інституційної спроможності визначено умови, за яких політична система України може подолати інституційні обмеження, підвищити ефективність управління та забезпечити стійкий розвиток у середньо- та довгостроковій перспективі. Практична значущість дослідження полягає у можливості використання його результатів для розроблення політик інституційної стійкості, модернізації публічного управління, удосконалення державної безпекової політики та зміцнення спроможності держави діяти в умовах тривалих воєнних і гібридних загроз.

Триває дискусія щодо того, наскільки path dependence обмежує інституційну трансформацію в умовах війни та чи здатні кризові події стати каталізаторами глибоких змін. Перспективним напрямом подальших досліджень є аналіз взаємодії між інституційною інерцією та механізмами резилієнтності, зокрема ролі цифрових інструментів, локальної демократії, міжвідомчої координації та суспільної мобілізації у подоланні структурних обмежень. Актуальними залишаються питання довгострокової стійкості реформ, інституційного навчання та формування нової управлінської культури, здатної забезпечити ефективне функціонування політичної системи в умовах тривалих воєнних і гібридних загроз.

Ключові слова: політична система, інституційна інерція, path dependence, інституційна стійкість, резилієнтність, публічне управління, безпека, критичні точки, децентралізація, війна.

Вступ та постановка проблеми. Політична система України упродовж трьох десятиліть формувалася під впливом кількох нашарованих історичних траєкторій, серед яких радянська адміністративно-командна спадщина, постсоціалістичні трансформації 1990-х років, хвилі демократизації та періодичні контр демократичні відкати. З 2014 р. розвиток політичної системи України відбувається в умовах тривалої війни, яка з 2022 р. переросла у фазу повномасштабної російсько-української війни. У таких умовах питання її ефективності, стійкості та здатності забезпечувати безперервність державного управління набуває ключового значення для національної безпеки та виживання держави [14, 17].

Ефективність політичної системи у цьому дослідженні розглядається як її спроможність забезпечувати стабільність, керованість, легітимність, результативність прийняття рішень та адаптивність до багатовимірних викликів, включно з воєнними, економічними та соціальними загрозами [11]. У воєнний період ці характеристики набувають додаткового виміру – здатності системи зберігати функціональність під впливом екстремальних стрес-чинників та швидко відновлюватися після них, що відповідає сучасним підходам до інституційної резилієнтності та системної безпеки.

Теорія залежності від раніше пройденого шляху (path dependence) пропонує продуктивну аналітичну рамку для пояснення того, як історично сформовані інститути, управлінські практики та політичні культури визначають межі можливих реформ. Метафори "колії" та "ефекту QWERTY" демонструють, що одного разу обрані інституційні рішення можуть відтворюватися тривалий час, навіть за умов їхньої неефективності, оскільки зміна траєкторії потребує значних політичних, економічних і соціальних ресурсів [10]. Для України це означає, що сучасні управлінські проблеми – від централізації влади до слабкості механізмів підзвітності – мають глибоке коріння у попередніх моделях організації влади [16].

У межах path dependence ефективність політичної системи визначається її здатністю долати інституційну інерцію, адаптуватися до нових умов та забезпечувати результативне управління попри історично сформовані обмеження [22]. Водночас війна та масштабні кризи розглядаються як "критичні точки" (critical junctures), у межах яких можливий перегляд усталених інституційних траєкторій та формування нових моделей управління [7]. Повномасштабна агресія Російської Федерації стала саме таким критичним моментом, що одночасно оголив структурні вразливості політичної системи та активізував процеси інституційного навчання, цифровізації, реформування сектору безпеки й посилення горизонтальних зв'язків між державою та суспільством [5].

У цьому контексті постає ключове дослідницьке питання: чи здатна політична система України, обтяжена історичною інерцією, трансформуватися у напрямі більшої стійкості, ефективності та демократичності, забезпечуючи належний рівень системної безпеки в умовах тривалих воєнних загроз? Відповідь на це питання потребує звернення до сучасних концепцій національної резильєнтності, які трактують стійкість не як пасивну здатність витримувати удари, а як активну модель розвитку держави. Саме тому важливо врахувати підходи, які підкреслюють, що національна стійкість – це не лише здатність держави протистояти гібридним загрозам, а й стратегія їх випередження, зокрема, формуючи пріоритети суб'єктів публічного управління, що передбачає активне формування цивілізаційної суб'єктності країни [28, 29].

Актуальність дослідження зумовлена зростанням ролі інституційної стійкості політичної системи та системної безпеки в умовах тривалих воєнних загроз, що визначають здатність держави забезпечувати безперервність управлінських процесів і підтримувати функціонування ключових інститутів. Сучасні наукові дискусії в безпековій сфері, публічному управлінні, політичній науці дедалі більше фокусуються на питаннях резильєнтності політичних систем, управління в умовах кризи (crisis governance), а також на ролі громадянського суспільства у підтриманні життєздатності держави під час війни [11, 21]. У цьому контексті особливої ваги набуває аналіз того, як інституційна інерція та залежність від раніше пройденого шляху впливають на ефективність і стійкість політичної системи України.

Україна є одним із ключових кейсів для міжнародних досліджень постсоціалістичних трансформацій, демократичних революцій та протидії авторитарній агресії. Її політична система розвивається під впливом тривалих історичних траєкторій, що поєднують радянську адміністративну спадщину, посттрансформаційні інституційні практики та нові моделі взаємодії держави й суспільства, сформовані після 2014 р. [27, 9]. Це робить український випадок важливим не лише в національному, а й у ширшому європейському та глобальному контексті.

Для практики публічного управління критично важливо ідентифікувати, які саме інституційні обмеження, "пастки минулого" та механізми path dependence стримують підвищення ефективності політичної системи, а які – навпаки – можуть бути використані як ресурс для її модернізації та посилення стійкості. В умовах повномасштабної війни ці питання набувають особливої гостроти, оскільки від здатності політичної системи долати інституційну інерцію, адаптуватися до кризових ситуацій та забезпечувати результативне управління залежить не лише якість державної політики, а й загальна спроможність держави протистояти зовнішнім загрозам.

Метою статті є дослідження умов і чинників, що визначають ефективність та інституційну стійкість політичної системи України в контексті теорії залежності від раніше пройденого шляху (*path dependence*), з урахуванням трансформацій, спричинених повномасштабною війною та реформами останнього десятиліття. Особливу увагу приділено аналізу того, як інституційна інерція, історично сформовані управлінські практики та критичні події впливають на здатність політичної системи забезпечувати результативне та безпечне функціонування держави в умовах тривалих загроз.

Об'єктом дослідження виступає політична система України як цілісна сукупність інститутів, норм, процедур, управлінських практик та акторів, що забезпечують формування й реалізацію державної політики та підтримання системної безпеки.

Предметом дослідження є інституційні та соціально-політичні чинники, які визначають ефективність, стійкість і адаптивність політичної системи, а також механізми відтворення або подолання інституційної інерції в умовах війни та кризових трансформацій.

Для досягнення поставленої мети передбачається розв'язати такі завдання: 1) уточнити теоретичні засади застосування концепції *path dependence* до аналізу політичних систем у сфері публічного управління та системної безпеки [22, 24]; 2) виявити ключові елементи інституційної спадковості української політичної системи, що впливають на її ефективність та стійкість [16]; 3) проаналізувати, як війна та пов'язані з нею кризи змінюють траєкторії розвитку політичних інститутів, управлінських практик і взаємодії держави та суспільства [5]; 4) визначити умови та інструменти, що сприяють подоланню негативних ефектів *path dependence* і посиленню інституційної резиліентності політичної системи України в середньо- та довгостроковій перспективі [11, 21]; сформулювати концептуальні засади та практичні орієнтири для розроблення державної політики інституційної стійкості, спрямованої на зміцнення спроможності політичної системи діяти в умовах тривалих безпекових загроз та післявоєнної відбудови.

Аналіз останніх наукових досліджень і публікацій. Проблематика ефективності політичних систем у контексті залежності від раніше пройденого шляху ґрунтується на класичних неоінституційних підходах, у межах яких інститути розглядаються як стійкі структури, що формують "правила гри" та визначають межі можливих політичних рішень [20]. Концепція *path dependence*, започаткована Полом Девідом для пояснення технологічної та інституційної інерції [10], була розвинена у політичній науці завдяки роботам П. Пірсона, Дж. Мегоні та К. Телен, які описали механізми інституційної інерції, критичних точок (*critical junctures*) та поступових змін – *layering*, *conversion*, *drift* [22, 18, 24, 7].

У сучасних дослідженнях публічного управління концепція *path dependence* дедалі частіше поєднується з підходами до аналізу інституційної стійкості [*resilience*], системної безпеки та управління в умовах кризи (*crisis governance*). Значна увага приділяється тому, як політичні системи реагують на шоки – економічні, безпекові, соціальні – та чи здатні вони використовувати кризу як можливість для інституційного оновлення [5, 2, 8]. У цьому контексті війна розглядається як радикальний стрес-тест для інститутів, що оголює структурні вразливості політичної системи, але водночас створює вікна можливостей для реформування сектору безпеки, модернізації управлінських практик та посилення горизонтальних механізмів взаємодії держави й суспільства [13, 3].

Окремий напрям становлять дослідження інституційної резиліентності держав у контексті тривалих безпекових загроз. У роботах OECD, UNDP, а також у новітніх дослідженнях з *governance under uncertainty* підкреслюється, що стійкість політичних систем залежить від здатності інститутів адаптуватися до непередбачуваних подій, підтримувати функціональність під час криз та забезпечувати безперервність державного управління [23, 6].

Україна посідає важливе місце в сучасній літературі про постсоціалістичні трансформації, гібридні режими та демократичні революції. Роботи С. Левицького та Л. Вея, Г. Гейла, А. Д'Аньєрі та Т. Кузьо аналізують український випадок у ширшому контексті конкурентного авторитаризму, регіональних впливів та війни як чинника політичної мобілізації й переосмислення ідентичності [17, 14, 9; 16]. Новітні дослідження підкреслюють, що після 2014 р. в Україні сформувалася гібридна модель інституційної стійкості, у якій

поєднуються державні та громадянські механізми забезпечення безпеки [19, 15]. У сучасних дослідженнях простежується цілісна концепція інституційної стійкості та державної безпеки, релевантна для аналізу ефективності політичної системи України (Пирожков, Ситник та ін. [28-32]), де розглянуто стійкість соціальних систем у контексті безпеки, уточнено зміст категорії "національна стійкість" і визначено пріоритети суб'єктів публічного управління щодо її забезпечення. Крім того, показано взаємозв'язок між інституційною спроможністю, публічною політикою та національною безпекою, продемонстровано безпековий вимір децентралізації як чинника зміцнення локальної стійкості. Обґрунтовано інституційну спроможність як ключову умову ефективності держави та її здатності протидіяти загрозам. Сукупно ці роботи формують сучасну українську наукову рамку, що доповнює міжнародні підходи *resilience* та *crisis governance* і поглиблює розуміння інституційної динаміки України в умовах війни.

Важливим емпіричним підґрунтям для аналізу ефективності політичної системи України є дані міжнародних індексів демократії, верховенства права та стійкості – зокрема, V-Dem, Freedom House, Bertelsmann Transformation Index. Вони фіксують суперечливу динаміку: одночасне посилення громадянської активності, волонтерського руху та самоорганізації суспільства на тлі збереження проблем із корупцією, нерівністю доступу до правосуддя та слабкістю окремих інститутів [26, 12]. Це підтверджує, що українська політична система перебуває у стані напруженої взаємодії між інституційною спадковістю та спробами її подолання, що робить застосування теорії *path dependence* та концепції інституційної стійкості особливо релевантним для аналізу її розвитку в умовах війни.

Методи дослідження. Методологічну основу дослідження становлять інституційний та неоінституційний підходи, концепція залежності від раніше пройденого шляху (*path dependence*), а також сучасні теоретичні рамки аналізу інституційної стійкості та системної безпеки. Використання цих підходів дає змогу дослідити, як історично сформовані інститути, управлінські практики та моделі взаємодії держави й суспільства впливають на ефективність політичної системи в умовах війни та тривалих криз [18, 24, 2]. У межах дослідження застосовано такі методи, як структурно-функціональний аналіз, який дозволяє оцінити здатність політичних інститутів забезпечувати стабільність, керованість і системну безпеку в умовах зовнішніх загроз; порівняльний інституційний аналіз, який дає змогу співвіднести український досвід із практиками інших постсоціалістичних держав та країн, що перебували у стані тривалих конфліктів [13, 3]. Системний підхід у поєднанні зі структурно-функціональним та інституційним аналізом [Ситник, 2024-2026] дозволяє розглядати політичну систему та сектор державної безпеки як складні відкриті системи, що функціонують у взаємодії з динамічним середовищем. Інституційна спроможність держави є системною характеристикою, яка визначається структурою, функціями та ресурсами інститутів, а її аналіз потребує поєднання системного та інституційного підходів. Це дозволяє досліджувати політичну систему як комплексну відкриту систему, здатну або відтворювати інерцію, або адаптуватися до кризових умов [30]. Кейс-стаді спрямований на вивчення ключових інституційних змін після 2014 р., зокрема децентралізації, цифровізації та реформ сектору безпеки. Критичний аналіз нормативно-правової бази дозволяє оцінити відповідність інституційних рішень вимогам системної безпеки та стійкості; аналіз емпіричних даних, включно з результатами соціологічних опитувань, даними міжнародних індексів демократії, верховенства права та інституційної стійкості [26, 12], а також аналітичними звітами OECD (2021-2024) та UNDP (2023). Методологічно важливим є поєднання концепції *path dependence* з підходами до аналізу інституційної резилієнтності, що дозволяє розглядати війну не лише як чинник руйнування, а й як критичну точку, яка відкриває можливості для інституційного оновлення, адаптації та підвищення ефективності публічного управління [5, 8].

Гіпотеза дослідження. Гіпотеза дослідження полягає в тому, що ефективність та інституційна стійкість політичної системи України визначаються взаємодією двох ключових чинників: інституційної інерції, успадкованої від попередніх політичних режимів і закріпленої у практиках державного управління, та здатності держави й суспільства долати цю інерцію під впливом критичних точок розвитку, насамперед повномасштабної війни, реформ публічного

управління та трансформації політичної культури. Передбачається, що війна 2014–2024 років виступає критичною точкою, яка здатна не лише загострювати вразливості політичної системи, а й каталізувати інституційні зміни, спрямовані на підвищення її ефективності, адаптивності та системної безпеки. За умов наявності стійких демократичних інститутів, активного громадянського суспільства та послідовної державної політики такі зміни можуть зменшувати негативні ефекти path dependence та сприяти формуванню інституційної резилієнтності, необхідної для функціонування держави в умовах тривалих безпекових загроз.

Виклад основного матеріалу. Концепція залежності від раніше пройденого шляху (path dependence) є одним із ключових аналітичних інструментів сучасного інституціоналізму, що дозволяє пояснити стійкість політичних інститутів, інерційність управлінських практик та обмеженість можливостей для реформування політичних систем [22, 18]. У сфері публічного управління цей підхід використовується для аналізу того, як історично сформовані моделі державного управління, політичної культури та адміністративні традиції визначають межі адаптивності політичних систем і впливають на їхню здатність забезпечувати системну безпеку [24].

Початкове формулювання path dependence, запропоноване Полом Девідом, демонструє, що одного разу обрані інституційні або технологічні рішення можуть відтворюватися навіть за умов їхньої неефективності, оскільки інституційні траєкторії набувають властивостей самопідсилення та "залипання" [lock-in] [10]. Подальший розвиток цієї концепції у політичній науці пов'язаний із роботами П. Пірсона, який показав, що зміна інституційної траєкторії потребує значних ресурсів, політичної волі та суспільного консенсусу, а тому відбувається переважно під впливом кризових подій або структурних зламів [22, 7].

У межах неоінституціоналізму Дж. Мегоні, К. Телен та В. Стрік підкреслюють, що інституційні зміни можуть мати не лише революційний, а й поступовий характер – через накладання [layering], перетлумачення [conversion], дрейф [drift] або витіснення [displacement] [18, 24]. Для України це особливо релевантно, оскільки більшість реформ відбуваються не одночасно, а через тривалі процеси адаптації, компромісів та часткових змін [15].

Сучасні дослідження стійкості та кризового управління розглядають війни, пандемії та економічні шоки як події, здатні змінювати інституційні траєкторії та створювати умови для інституційного оновлення [5, 1, 8]. У таких умовах політичні системи можуть або відтворювати інституційну слабкість, або демонструвати здатність до інституційного навчання, адаптивного управління та посилення взаємодії з громадянським суспільством [11, 21, 25].

Для України війна стала саме такою критичною точкою, яка одночасно загострила інституційні вразливості та активізувала процеси інституційного оновлення. Повномасштабна агресія сприяла розвитку горизонтальних мереж самоорганізації, реформуванню сектору безпеки, прискоренню цифровізації управління, зміцненню локальної демократії та підвищенню ролі громадянського суспільства у забезпеченні системної безпеки [14, 9, 27, 13, 3].

Отримані результати свідчать, що війна створила умови, за яких інституційна інерція частково руйнується, а нові практики управління та взаємодії держави й суспільства набувають стійкості. Це відкриває можливості для формування інституційної резилієнтності, здатної зменшувати негативні ефекти path dependence та підвищувати ефективність політичної системи в умовах тривалих безпекових загроз.

У дослідженні Ситника, Заворітньої та Павлінець підкреслюється, що ключовим чинником національної стійкості є інституційна спроможність суб'єктів публічного управління, яка визначає здатність держави долати інституційну інерцію та забезпечувати ефективне реагування на загрози [29]. Автори підкреслюють, що стійкість залежить від інституційної спроможності, а не лише від ресурсів чи політичної волі.

У постсоціалістичних державах залежність від раніше пройденого шляху проявляється особливо виразно через спадщину централізованого управління, персоналізовані політичні практики, слабкість механізмів стримувань і противаг, низький рівень довіри до влади та домінування неформальних правил [17]. Ці чинники формують довготривалі інституційні

траєкторії, які складно змінити навіть за умов зовнішнього тиску чи внутрішніх реформ, оскільки вони закріплені у практиках державного управління та політичній культурі.

Інституційна інерція знижує ефективність політичної системи, обмежуючи її здатність адаптуватися до нових викликів, реагувати на безпекові загрози та впроваджувати інноваційні управлінські рішення. Порівняльні дослідження показують, що країни Центральної Європи змогли частково подолати інституційну інерцію завдяки зовнішньому тиску ЄС та стабільним демократичним інститутам, тоді як держави Східного партнерства (Україна, Грузія, Молдова) мають складніші траєкторії через вплив війни, корупції, політичної нестабільності та слабкості інституційної стійкості [14, 23].

Застосування концепції *path dependence* до аналізу ефективності політичної системи України дозволяє пояснити довготривалу природу ключових управлінських проблем та автоматичне відтворення неефективних інституційних практик [22]. Цей підхід також дає змогу визначити, які реформи здатні змінити інституційну траєкторію, а також оцінити, як війна впливає на інституційну стійкість, адаптивність та результативність управління [5, 11, 8].

Таким чином, *path dependence* виступає ключовою теоретичною рамкою для аналізу інституційної інерції та можливостей трансформації політичної системи України в умовах війни та реформ. Вона дозволяє поєднати історичний аналіз із сучасними підходами до *resilience*, *adaptive governance* та інституційного навчання [1, 21, 25].

Політична система України з моменту здобуття незалежності розвивається під впливом складної взаємодії історичної спадщини, соціально-економічних трансформацій, зовнішньополітичних викликів та внутрішніх криз. Інституційна інерція, успадкована від радянського політичного режиму, стала одним із ключових чинників, що визначають траєкторію розвитку державного управління, характер політичних процесів та ефективність функціонування державних інститутів [16, 14]. У цьому контексті концепція *path dependence* пояснює, чому багато структурних проблем української політичної системи зберігаються протягом трьох десятиліть, попри численні спроби реформ [17].

Після 1991 р. Україна успадкувала централізовану, ієрархічну та персоналізовану модель державного управління, що характеризувалася домінуванням виконавчої влади, слабкістю механізмів стримувань і противаг, низьким рівнем автономії місцевого самоврядування, переважанням неформальних практик та патерналістською політичною культурою [14]. Ці елементи стали "інституційною колією", яка визначила логіку розвитку політичної системи у 1990-х і значною мірою зберігається до сьогодні.

Навіть після демократичних зрушень 2004 та 2014 років багато управлінських практик продовжували відтворюватися за інерцією, що свідчить про глибоку структурну залежність від минулого. Відтворення радянських моделей централізованого управління зменшує результативність політичних рішень, уповільнює модернізацію та ускладнює впровадження реформ.

У період до Революції Гідності політична система України демонструвала циклічність, у межах якої демократичні імпульси змінювалися авторитарними тенденціями. Ці коливання не призводили до системних змін, оскільки політичні еліти залишалися носіями радянських управлінських практик, реформи були фрагментарними, інститути – слабкими, а політична конкуренція – персоналізованою [16, 9]. У результаті політична система забезпечувала короткострокову стабільність, але не формувала довгострокової ефективності та стійкості.

Події 2013–2014 років стали першим масштабним критичним моментом, який відкрив можливість для перегляду інституційної траєкторії. Революція Гідності посилила роль громадянського суспільства, актуалізувала запит на верховенство права та започаткувала реформи поліції, державної служби, антикорупційних органів і децентралізацію [15, 21]. Однак інституційна інерція залишалася значною: старі практики адаптувалися до нових умов, а не зникали. Це підтверджує тезу про те, що критичні точки не гарантують зміни траєкторії, а лише створюють можливість для неї [7].

Російська агресія 2014 р. стала першим масштабним стрес-тестом для політичної системи України, оголивши слабкість сектору безпеки, низьку інституційну спроможність

держави та обмеженість механізмів стратегічного планування [27]. Війна активізувала волонтерський рух, сприяла самоорганізації громадян та формуванню горизонтальних мереж взаємодії, які частково компенсували інституційну слабкість держави. Це створило унікальну для постсоціалістичних держав модель, у якій громадянське суспільство виконує функції інституційної підтримки там, де державні структури виявляються неспроможними [5].

Повномасштабне вторгнення 24 лютого 2022 р. стало другою, значно масштабнішою критичною точкою, яка радикально змінила траєкторію розвитку політичної системи. Війна прискорила інституційні зміни, посилила координацію між державою та суспільством, сприяла формуванню нових управлінських практик, підвищила рівень політичної відповідальності та солідарності, а також зміцнила окремі інститути, насамперед сектор оборони [13]. Водночас війна загострила проблеми корупції, кадрової політики та бюрократичної інерції, що свідчить про суперечливий характер інституційної трансформації.

Одним із успішних прикладів подолання інституційної інерції стала реформа децентралізації. Вона посилила спроможність місцевого самоврядування, створила нові інституційні механізми, зменшила залежність громад від центральної влади та сприяла формуванню нової управлінської культури [15, 21]. Децентралізація демонструє, що *path dependence* може бути подолана за умови політичної волі, зовнішньої підтримки та активної участі громад.

Попри значні зміни, інституційна інерція продовжує впливати на політичну систему України. Її проявами є фрагментарність реформ, персоналізація політики, слабкість парламентського контролю, нерівномірність інституційної спроможності, залежність від зовнішньої підтримки та відтворення неформальних практик у кадровій політиці [14]. Водночас зростає роль громадянського суспільства, цифрових інструментів управління та європейської інтеграції як чинників інституційної стійкості.

Повномасштабна війна стала безпрецедентним викликом для політичної системи, перевіряючи її інституційну спроможність, адаптивність та здатність до самовідтворення. Вона одночасно виступає руйнівним чинником, який оголює слабкі місця державного управління, і каталізатором інституційних змін, що здатні змінювати траєкторію розвитку політичної системи [5; 1]. У цьому контексті *path dependence* та *resilience* стають ключовими концептами для аналізу того, як політичні інститути реагують на екстремальні умови.

Війна загострила структурні проблеми, що накопичувалися протягом десятиліть. Їхнє коріння — у радянській спадщині, персоналізованій політиці та слабкості інституцій [17]. Найбільш помітними проявами інституційної слабкості стали дисфункції сектору безпеки до 2022 р.: низька боєздатність армії, корупція в оборонних закупівлях, відсутність стратегічного планування та слабка координація між силовими структурами [9, 27]. Війна також оголила проблему кадрової політики як джерела інституційної інерції: політичні призначення, нестача професійних управлінців, відтворення неформальних практик у державній службі. Це підтверджує, що *path dependence* у кадровій політиці залишається одним із найстійкіших елементів української політичної системи. Зокрема, інституційна спроможність сьогодні розглядається як ключовий чинник ефективності держави, що визначається не лише формальними структурами, а й якістю кадрової політики та управлінських компетенцій [30]. Це підтверджує, що кадрова інерція та слабкість управлінських практик є одними з найстійкіших проявів *path dependence* в українській політичній системі.

Після 2022 р. відбулося швидке оновлення сектору оборони, масштабна цифровізація управління (Dіia, електронні реєстри, автоматизація процедур), посилення координації між центральною та місцевою владою, а також активізація антикорупційних механізмів під тиском ЄС [21]. Ці зміни демонструють, що інституційна інерція може бути частково подолана під впливом екстремальних умов.

Зросла роль громадянського суспільства. Війна спричинила безпрецедентну мобілізацію волонтерського руху, формування горизонтальних мереж взаємодії, підвищення рівня довіри між громадянами та появу нових форм самоорганізації. Це створює альтернативні канали інституційної стійкості, які компенсують слабкість держави та підсилюють її спроможність у кризових умовах.

Важливим чинником зміни інституційної траєкторії є європейська інтеграція. Отримання статусу кандидата в ЄС та початок переговорів посилюють зовнішній тиск на реформи, формують інституційні стандарти та зменшують ризики повернення до старих практик. Європейський Союз виступає "зовнішнім інституційним архітектором", який допомагає долати path dependence, створюючи стимули для модернізації та інституційного оновлення.

Українська інституційна стійкість має гібридний характер. Вона формується не лише державою, а й суспільством, що створює модель resilience, у якій поєднуються державні та громадянські механізми забезпечення системної безпеки. Ця модель включає: 1) державну стійкість – адаптацію управлінських процедур, модернізацію оборонних інститутів, централізацію в умовах воєнного стану; 2) суспільну стійкість – волонтерство, самоорганізацію, локальні ініціативи, психологічну мобілізацію; 3) інституційну взаємодію держави та суспільства, яка є ключовим елементом української моделі resilience.

Інфографіка "Інституційна інерція та стійкість політичної системи України в умовах війни: аналіз через призму path dependence" (рис. 1) демонструє, як path dependence та інституційна інерція формують вразливості політичної системи України, які загострюються під час війни. Повномасштабне вторгнення виступає критичною точкою, що одночасно руйнує застарілі моделі та відкриває можливості для інституційного оновлення. Механізми резилієнтності – децентралізація, цифровізація, міжвідомча координація, громадянська мобілізація та інституційне навчання – забезпечують адаптивність і формують інституційну стійкість держави в умовах тривалих воєнних і гібридних загроз.

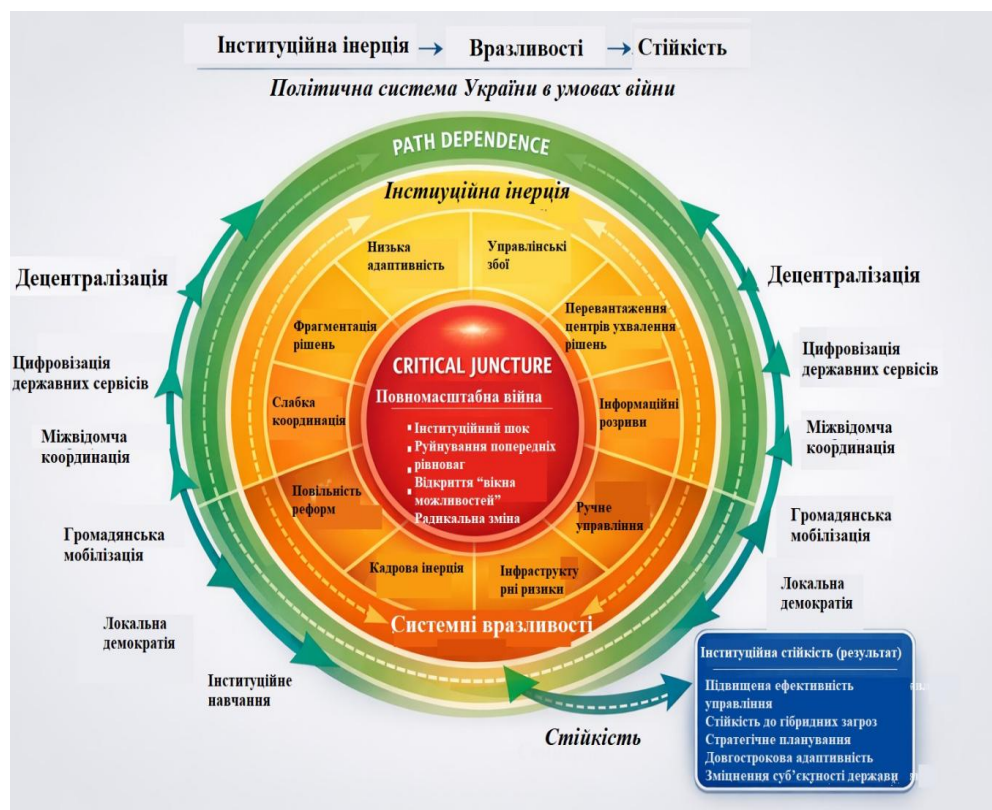


Рисунок 1 – Інституційна інерція та стійкість політичної системи України в умовах війни: аналіз через призму path dependence, авторська розробка

Отже, російсько-українська війна має амбівалентний вплив. Вона одночасно руйнує слабкі інститути та прискорює інституційні зміни, модернізацію, цифровізацію, реформування сектору безпеки та європейську інтеграцію. Це створює ситуацію, коли path dependence одночасно посилюється [через централізацію, кадрову інерцію, бюрократичні практики] і разом з тим, долається [через реформи, тиск ЄС, мобілізацію суспільства]. Майбутня траєкторія політичної системи залежить від того, чи зможе держава перетворити кризові зміни

на системні реформи, а не повернутися до інституційної інерції після завершення війни.

Реформа децентралізації, започаткована в Україні у 2014 році, є одним із найяскравіших прикладів виходу політичної системи за межі усталеної інституційної траєкторії та подолання ефектів залежності від раніше пройденого шляху. На відміну від багатьох реформ, що залишалися фрагментарними або декларативними, децентралізація стала структурною трансформацією, яка змінила логіку публічного управління, перерозподіл владних повноважень та механізми взаємодії між державою й громадянами [15, 21].

До 2014 р. політична система України зберігала значну частину радянської централізованої моделі управління, що характеризувалася домінуванням виконавчої вертикалі, слабкістю місцевого самоврядування, відсутністю фінансової автономії громад та низькою інституційною спроможністю [14]. Ці елементи були класичними проявами *path dependence*, які відтворювали застарілі управлінські практики та обмежували адаптивність політичної системи. Децентралізація стала першим масштабним інституційним зламом, що порушив цю траєкторію.

Реформа забезпечила фінансову автономію громад, скорочення управлінських циклів та наближення прийняття рішень до громадян [21]. Формування об'єднаних територіальних громад стало ключовим механізмом укрупнення та підвищення спроможності місцевих одиниць управління. Це дозволило оптимізувати адміністративно-територіальну структуру, забезпечити громади ресурсами та повноваженнями, а також підвищити якість місцевих послуг [15].

Передача громадам частини податкових надходжень створила умови для фінансової стійкості та стратегічного планування розвитку, зменшивши залежність від центральної влади. Громади отримали реальні інструменти управління освітою, первинною медициною, інфраструктурою, соціальними послугами та місцевим економічним розвитком. Це змінило логіку прийняття рішень – від централізованої до субсидіарної моделі [Council of Europe, 2022].

Важливим результатом реформи стало формування нових управлінських компетенцій на місцевому рівні. Розвиток локальних стратегічних команд та адміністративних кадрів став критичним чинником подолання кадрової інерції – одного з найстійкіших проявів *path dependence*.

Децентралізація порушила кілька ключових інституційних "колій", якщо говорити мовою *path dependence*. Відбувся вихід від централізованої моделі управління. Реформа змінила принцип організації влади: від вертикальної моделі – до мережевої моделі *governance*, у якій громади виступають активними суб'єктами політики [1]. Відбулася трансформація політичної культури на місцях. Громади отримали ресурси, відповідальність і можливість впливати на розвиток територій, що сприяло формуванню культури участі, підзвітності та локальної демократії. І зменшився вплив неформальних практик. Фінансова автономія та прозорість бюджетів зменшили можливості для політичного патронажу та корупційних схем. Натомість підвищення інституційної стійкості громад. Громади стали здатними самостійно реагувати на кризи, мобілізувати ресурси та забезпечувати базові послуги навіть у воєнний час. Децентралізація стала одним із ключових чинників *resilience* під час повномасштабної війни.

Активне громадянське суспільство є одним із ключових чинників підвищення ефективності політичної системи, оскільки забезпечує додаткові канали контролю, мобілізації ресурсів та участі громадян у формуванні політики. Повномасштабне вторгнення 2022 р. стало критичним випробуванням для реформи децентралізації та для здатності громад діяти як осередків інституційної стійкості. Саме громади забезпечували евакуацію населення, гуманітарну допомогу, підтримку Збройних Сил України, відновлення інфраструктури та координацію волонтерських ініціатив. Децентралізація зменшила навантаження на центральну владу, дозволивши державі зосередитися на обороні та стратегічному управлінні, тоді як локальні інститути продемонстрували високу адаптивність і гнучкість.

Війна прискорила інституційне навчання на місцевому рівні. Громади швидко освоювали кризове управління, цифрові інструменти та нові моделі координації. Горизонтальні мережі взаємодії, що сформувалися під час війни, зміцнили інституційну

стійкість і підвищили ефективність політичної системи в умовах тривалих загроз [5]. Водночас інституційна інерція не зникла: реформа виявила нерівномірність спроможності громад, кадровий дефіцит, ризики повторної централізації під час воєнного стану, політичний тиск на місцеве самоврядування та залежність від зовнішнього фінансування [21]. Це свідчить про те, що path dependence частково зберігається, особливо у сферах, де реформа не була завершена.

Громадянське суспільство та політична культура суттєво впливають на траєкторію розвитку політичної системи. У межах теорії path dependence вони можуть виступати як механізмами подолання історично успадкованих моделей, так і чинниками їхнього відтворення. Український випадок є унікальним тим, що громадянське суспільство часто демонструє вищу адаптивність і стійкість, ніж окремі державні інститути, а політична культура перебуває у стані динамічної трансформації, особливо після 2014 та 2022 років.

Упродовж трьох десятиліть незалежності громадянське суспільство розвивалося нерівномірно, але саме воно стало одним із ключових акторів, здатних долати інституційну інерцію. У періоди криз, коли державні інститути не забезпечували ефективне управління, громадянське суспільство виконувало функцію інституційного коректора [16]. Події 2004 та 2013–2014 років продемонстрували здатність суспільства мобілізувати значні ресурси, формувати горизонтальні мережі та впливати на політичні рішення [9].

Після 2014 р., а особливо після 2022 р., громадянське суспільство стало ключовим елементом національної стійкості. Волонтерський рух забезпечував армію та цивільних, локальні ініціативи підтримували громади, громадські організації здійснювали моніторинг влади, а цифрові платформи сприяли прозорості та підзвітності. Це сформувало гібридну модель resilience, у якій держава та суспільство взаємодіють як партнери.

Громадські організації та волонтерські мережі часто впроваджують нові стандарти управління, цифрові інструменти, практики прозорості та моделі локальної демократії, виступаючи інноваторами розвитку. Таким чином, громадянське суспільство стає джерелом інституційних інновацій, що сприяють подоланню path dependence [1].

Політична культура визначає, як громадяни сприймають владу, політичні інститути та власну роль у політичному процесі. Патерналістські установки знижують ефективність політичної системи, оскільки підтримують відтворення неформальних практик і обмежують розвиток демократичних інститутів [14]. В Україні політична культура має змішаний характер, поєднуючи елементи посттоталітарної спадщини, патерналістських очікувань, зростаючої культури участі та нових практик солідарності.

Соціологічні дослідження засвідчують стійкість посттоталітарних елементів політичної культури: недовіру до влади, низький рівень політичної участі поза кризами, толерантність до неформальних практик та персоналізацію політики. Ці елементи є проявами path dependence, що ускладнюють інституційні зміни. Водночас Революція Гідності та повномасштабна війна сприяли формуванню нових цінностей відповідальності, солідарності, горизонтальної взаємодії та готовності до участі в управлінні. Це створює умови для зміни інституційної траєкторії, оскільки політична культура впливає на попит на реформи та якість демократичних інститутів. Війна спричинила зростання довіри до держави та армії, підвищення рівня політичної мобілізації, формування культури взаємної підтримки та зміцнення національної ідентичності.

У сучасних умовах громадянське суспільство та політична культура можуть як підсилювати інституційну інерцію (коли патерналістські установки домінують), так і сприяти її подоланню – якщо громадяни беруть участь у прийнятті рішень, громади формують локальні політики, а громадські організації здійснюють контроль і моніторинг. Україна демонструє саме другий сценарій, особливо після 2022 р.. Громадянське суспільство виступає партнером держави у моделі collaborative governance, у межах якої держава, громадянське суспільство, бізнес і громади спільно формують політики та реалізують рішення [1].

Отже, громадянське суспільство та політична культура відіграють ключову роль у подоланні інституційної інерції. Вони формують нові моделі взаємодії між державою та громадянами, підсилюють інституційну стійкість, створюють попит на реформи та сприяють демократизації й модернізації публічного управління. Український досвід демонструє, що

навіть за умов війни громадянське суспільство та політична культура можуть стати чинниками зміни інституційної траєкторії, відкриваючи можливості для подолання path dependence та формування нової моделі публічного управління.

Висновки. У дослідженні ефективність політичної системи України розглядається як її здатність забезпечувати стабільність, результативність, легітимність та адаптивність до кризових умов. Проведений аналіз засвідчив, що інституційна інерція, кадрові практики, централізація влади та патерналістська політична культура залишаються ключовими чинниками, які знижують ефективність політичної системи та обмежують її спроможність до модернізації й інституційного навчання [22]. Натомість децентралізація, активне громадянське суспільство, цифровізація та європейська інтеграція формують умови для подолання path dependence та розвитку стійкої моделі публічного управління [15, 21].

Політична система України у 1991-2024 рр. розвивалася під впливом глибокої інституційної інерції, успадкованої від радянської моделі управління. Вона проявлялася у централізації влади, персоналізації політичних рішень, слабкості механізмів стримувань і противаг, нерівномірності інституційної спроможності та домінуванні неформальних практик [14]. Концепція path dependence виявилася продуктивною для пояснення тривалості цих структурних проблем.

Водночас дослідження показало, що критичні точки – Революція Гідності, війна на Донбасі та повномасштабне вторгнення 2022 р. – стали каталізаторами інституційних змін. Війна оголила слабкі місця політичної системи, але водночас активізувала процеси інституційного навчання, модернізації сектору безпеки, цифровізації управління, посилення координації між рівнями влади та мобілізації громадянського суспільства [5].

Особливе значення має реформа децентралізації, яка стала прикладом успішного подолання інституційної інерції. Вона змінила архітектуру публічного управління, посилила спроможність громад, створила нові механізми локальної демократії та забезпечила стійкість територій у воєнний час [15].

Громадянське суспільство та політична культура відіграли ключову роль у зміні інституційної траєкторії. Самоорганізація громадян, волонтерський рух, горизонтальні мережі та нові практики солідарності стали фундаментом інституційної стійкості України. Політична культура поступово зміщується від патерналістської до культури участі, відповідальності та взаємодії.

Таким чином, українська політична система демонструє гібридну модель інституційної стійкості, у якій держава та суспільство взаємодіють як партнери. Проте ризики повернення до інституційної інерції залишаються високими, особливо в умовах війни, централізації влади та кадрових обмежень.

Дискусії та перспективи подальших досліджень. У сучасній науковій літературі триває активна дискусія щодо того, яким чином політичні системи, обтяжені інституційною інерцією та path dependence, здатні трансформуватися під впливом кризових подій, зокрема воєн, революцій та масштабних реформ. Частина дослідників наголошує на жорсткості інституційних траєкторій і схильності політичних систем до відтворення усталених практик [22, 18, 24], тоді як інші підкреслюють роль критичних точок, інституційного навчання та адаптивного управління як механізмів подолання інерції [5, 8]. Окремий напрям дискусій стосується resilience та wartime governance, де аналізується, чи може війна виступати каталізатором інституційних змін, чи навпаки – посилювати централізацію, бюрократичну інерцію та неформальні практики [13]. Значна увага приділяється також ролі громадянського суспільства та локальних інститутів у забезпеченні стійкості держави в умовах тривалих безпекових загроз. У цьому контексті український випадок розглядається як унікальний емпіричний приклад взаємодії держави та суспільства, де формується гібридна модель resilience, що демонструє можливість виходу за межі інституційної інерції навіть у надзвичайно складних умовах війни. Пирожков, Божок і Хамітов розширюють наукову дискусію про resilience, трактуючи її як цивілізаційну суб'єктність держави та стратегію випередження гібридних загроз, що доповнює інституційно-орієнтовані підходи західних дослідників [28]. Також стійкість розглядається як інтегральна наукова категорія (національна

стійкість, зокрема), яка поєднує інституційні, соціальні та управлінські компоненти й визначає здатність держави функціонувати та розвиватися в умовах тривалих загроз [29]. Перспективи подальших досліджень пов'язані з аналізом довгострокових наслідків повномасштабної війни для інституційної архітектури України, оцінкою стійкості реформ після завершення воєнного стану та вивченням того, чи зможе політична система конвертувати кризові зміни у сталу інституційну модернізацію.

ЛІТЕРАТУРА:

1. Ansell C., Sørensen E., Torfing J. Public governance as cocreation: A strategy for revitalizing the public sector. Cambridge : Cambridge University Press, 2021. 305 p.
2. Ansell C., Trondal J. Governing tumultuous times: Rethinking the nature of resilience. *Governance*. 2018. Vol. 31, No. 1. P. 5–20.
3. Bachmann V., Bruns B. War and resilience in Ukraine: Institutional and social perspectives. 2023.
4. Bertelsmann Stiftung. Bertelsmann Transformation Index 2024. Gütersloh: Bertelsmann Stiftung, 2024.
5. Boin A., 't Hart P., Stern E., Sundelius B. The politics of crisis management: Public leadership under pressure. 2nd ed. Cambridge : Cambridge University Press, 2017. 182 p.
6. Bruns B., Migliorati M. Governance under uncertainty: The case of Ukraine. 2024.
7. Capoccia G., Kelemen R. D. The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism. *World Politics*. 2007. Vol. 59, No. 3. P. 341–369.
8. Comfort L. K., Kapucu N., Ko K., Menoni S., Siciliano M. Crisis Management Revisited: A Research Agenda for a Volatile World. *Public Administration Review*. 2020.
9. D'Anieri P. Ukraine and Russia: From civilised divorce to uncivil war. Cambridge : Cambridge University Press, 2019.
10. David P. A. Clio and the Economics of QWERTY. *The American Economic Review*. 1985. Vol. 75, No. 2. P. 332–337.
11. Duit A. Resilience thinking: Lessons for public administration. *Public Administration*. 2016. Vol. 94, No. 2. P. 364–380.
12. Freedom House. Freedom in the World 2024. Washington, DC : 12.
13. Greitens S. C. National Security and Institutional Resilience. 2022.
14. Hale H. E. Patronal Politics: Eurasian Regime Dynamics in Comparative Perspective. Cambridge : Cambridge University Press, 2015.
15. Krawchenko T. Decentralization and Resilience in Ukraine. 2023.
16. Kuzio T. Putin's War Against Ukraine: Revolution, Nationalism, and Crime. Toronto : Chair of Ukrainian Studies, 2017.
17. Levitsky S., Way L. A. Competitive Authoritarianism: Hybrid Regimes After the Cold War. Cambridge : Cambridge University Press, 2010.
18. Mahoney J. Path dependence in historical sociology. *Theory and Society*. 2000. Vol. 29, No. 4. P. 507–548.
19. Murtazashvili I., Murtazashvili J. B. Self-governance and resilience: The case of Ukraine. 2021.
20. North D. C. Institutions, Institutional Change and Economic Performance. Cambridge : Cambridge University Press, 1990.
21. OECD. Building Resilience: Lessons from Ukraine. Paris : OECD Publishing, 2022.
22. Pierson P. Increasing Returns, Path Dependence, and the Study of Politics. *The American Political Science Review*. 2000. Vol. 94, No. 2. P. 251–267.
23. Siddi M. Governance and resilience in the European neighborhood. 2023.
24. Thelen K. Historical Institutionalism in Comparative Politics. *Annual Review of Political Science*. 1999. Vol. 2. P. 369–404.
25. UNDP. Resilience and Recovery in Ukraine. 2023.
26. V-Dem Institute. Democracy Report 2024: Democracy Winning and Losing at the Ballot Box. Gothenburg : University of Gothenburg, 2024.
27. Way L. A. Pluralism by Default: Weak Autocrats and the Rise of Competitive Politics. Baltimore : Johns Hopkins University Press, 2015.
28. Пирожков С. І., Божок Є. П., Хамітов Н. В. Цивілізаційна суб'єктність України: від потенцію до реальності. Київ : Наукова думка, 2021.

29. Ситник Г. П., Заворітня Г., Павлінець А. Національна стійкість як наукова категорія та пріоритети суб'єктів публічного управління щодо її забезпечення. Публічне управління та адміністрування в Україні. 2025. № 2. С. 211–223.

30. Ситник Г. П., Комаха Л. Г., Зубчик О. А. Концептуальне осмислення інституційної спроможності держави: публічно-управлінський аспект. Науковий часопис НПУ імені М. П. Драгоманова. 2024.

31. Ситник Г. П., Комаха Л., Ткаченко І. Системний аналіз публічного управління та адміністрування у контексті зв'язку публічної політики, національної безпеки та інституційної спроможності держави. Публічне управління та адміністрування в Україні. 2024. № 4. С. 18–29.

REFERENCES:

1. Ansell, C., Sørensen, E. & Torfing, J. (2021) *Public governance as co-creation: A strategy for revitalizing the public sector*. Cambridge: Cambridge University Press.
2. Ansell, C. & Trondal, J. (2018) 'Governing tumultuous times: Rethinking the nature of resilience', *Governance*, 31(1), pp. 5-20.
3. Bachmann, V. & Bruns, B. (2023) *War and resilience in Ukraine: Institutional and social perspectives*.
4. Bertelsmann Stiftung (2024) *Bertelsmann Transformation Index 2024*. Gütersloh: Bertelsmann Stiftung.
5. Boin, A., 't Hart, P., Stern, E. & Sundelius, B. (2017) *The politics of crisis management: Public leadership under pressure*. 2nd ed. Cambridge: Cambridge University Press.
6. Bruns, B. & Migliorati, M. (2024) *Governance under uncertainty: The case of Ukraine*.
7. Capoccia, G. & Kelemen, R.D. (2007) 'The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism', *World Politics*, 59(3), pp. 341–369.
8. Comfort, L.K. et al. (2020) 'Crisis Management Revisited: A Research Agenda for a Volatile World', *Public Administration Review*.
9. D'Anieri, P. (2019) *Ukraine and Russia: From civilised divorce to uncivil war*. Cambridge: Cambridge University Press.
10. David, P.A. (1985) 'Clio and the Economics of QWERTY', *The American Economic Review*, 75(2), pp. 332–337.
11. Duit, A. (2016) 'Resilience thinking: Lessons for public administration', *Public Administration*, 94(2), pp. 364–380.
12. Freedom House (2024) *Freedom in the World 2024*. Washington, DC.
13. Greitens, S.C. (2022) *National Security and Institutional Resilience*.
14. Hale, H.E. (2015) *Patronal Politics: Eurasian Regime Dynamics in Comparative Perspective*. Cambridge: Cambridge University Press.
15. Krawchenko, T. (2023) *Decentralization and Resilience in Ukraine*.
16. Kuzio, T. (2017) *Putin's War Against Ukraine: Revolution, Nationalism, and Crime*. Toronto: Chair of Ukrainian Studies.
17. Levitsky, S. & Way, L.A. (2010) *Competitive Authoritarianism: Hybrid Regimes After the Cold War*. Cambridge: Cambridge University Press.
18. Mahoney, J. (2000) 'Path dependence in historical sociology', *Theory and Society*, 29(4), pp. 507–548.
19. Murtazashvili, I. & Murtazashvili, J.B. (2021) *Self-governance and resilience: The case of Ukraine*.
20. North, D.C. (1990) *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press.
21. OECD (2022) *Building Resilience: Lessons from Ukraine*. Paris: OECD Publishing.
22. Pierson, P. (2000) 'Increasing Returns, Path Dependence, and the Study of Politics', *American Political Science Review*, 94(2), pp. 251–267.
23. Siddi, M. (2023) *Governance and resilience in the European neighborhood*.
24. Thelen, K. (1999) 'Historical Institutionalism in Comparative Politics', *Annual Review of Political Science*, 2, pp. 369-404.
25. UNDP (2023) *Resilience and Recovery in Ukraine*.
26. V-Dem Institute (2024) *Democracy Report 2024: Democracy Winning and Losing at the Ballot Box*. Gothenburg: University of Gothenburg.
27. Way, L.A. (2015) *Pluralism by Default: Weak Autocrats and the Rise of Competitive Politics*. Baltimore: Johns Hopkins University Press.

28. Pyrozhekov, S.I., Bozhok, Y.P. & Khamitov, N.V. (2021) Civilizational subjectivity of Ukraine: From potential to reality. Kyiv: Naukova Dumka.

29. Sytnyk, H.P., Zavoritnia, H. & Pavlinets, A. (2025) 'National resilience as a scientific category and the priorities of public administration actors in ensuring it', Public Administration and Administration in Ukraine, (2), pp. 211–223.

30. Sytnyk, H.P., Komakha, L.H. & Zubchuk, O.A. (2024) 'Conceptual understanding of the institutional capacity of the state: A public administration perspective', Scientific Journal of NPU Dragomanov.

31. Sytnyk, H.P., Komakha, L. & Tkachenko, I. (2024) 'System analysis of public administration and administration in the context of the relationship between public policy, national security and institutional capacity', Public Administration and Administration in Ukraine, (4), pp. 18–29.

S. A., DSc., prof. Zubchuk O., PhD. Assoc. prof Lynchenko M.

INSTITUTIONAL INERTIA AND THE RESILIENCE OF UKRAINE'S POLITICAL SYSTEM UNDER WARTIME CONDITIONS: A PATH DEPENDENCE PERSPECTIVE

Abstract. The article examines the impact of institutional inertia and path dependence on the effectiveness and resilience of Ukraine's political system during the full-scale war. It argues that the Soviet administrative legacy, informal governance practices, patron–client networks, and a centralized decision-making model have shaped long-term trajectories of institutional development that significantly constrain the adaptability of the public administration system and its ability to respond rapidly to crisis challenges. The analysis demonstrates that the war functions as a critical juncture that simultaneously exacerbates structural vulnerabilities of the political system and opens opportunities for institutional renewal, accelerated digitalization, security sector reform, strengthened interagency coordination, and the expansion of horizontal state–society interaction.

Special attention is devoted to the role of decentralization, civic mobilization, volunteer networks, and the development of local democracy as key factors in building institutional resilience capable of offsetting the negative effects of path dependence and ensuring state stability under prolonged threats. Drawing on contemporary approaches to resilience, crisis governance, systemic security, and institutional capacity, the study identifies the conditions under which Ukraine's political system can overcome institutional constraints, enhance governance effectiveness, and ensure sustainable development in the medium and long term. The practical relevance of the research lies in its applicability for designing institutional resilience policies, modernizing public administration, improving state security policy, and strengthening the state's capacity to operate under prolonged wartime and hybrid threats.

The ongoing scholarly debate concerns the extent to which path dependence limits institutional transformation during war and whether crisis events can serve as catalysts for profound structural change. A promising direction for further research is the analysis of interactions between institutional inertia and resilience mechanisms, particularly the role of digital tools, local democracy, interagency coordination, and civic mobilization in overcoming structural constraints. Equally important are questions of long-term reform sustainability, institutional learning, and the formation of a new governance culture capable of ensuring the effective functioning of the political system under protracted military and hybrid threats.

Keywords: political system, institutional inertia, path dependence, institutional resilience, resilience, public administration, security, critical junctures, decentralization, war.

СЕРЕДОВИЩНО-ЦЕНТРИЧНА ПАРАДИГМА УПРАВЛІННЯ БЕЗПЕКОЮ: КОНЦЕПТУАЛЬНА ЗАСАДА РОЗВИТКУ КОНТРОДРОННИХ СИСТЕМ

Стаття присвячена протидії дронним загрозам, спричинені застосуванням безпілотних систем у військових цілях, виходить далеко за межі суто технологічної задачі, сягаючи виміру державного управління у сфері військової безпеки. Масове впровадження і стрімке поширення технології роїння безпілотних літальних апаратів (БПЛА) висуває нові вимоги до організації сенсорних мереж алгоритмів обробки інформації та прийняття рішень у системах раннього попередження. Відтак питання їхньої ефективності слід розглядати не лише як інженерну проблему, але і як завдання формування нової парадигми у безпековому управлінні. У статті запропоновано концептуальну засаду для побудови архітектур систем виявлення безпілотних загроз на базі аналізу реакції навколишнього середовища на присутність або активність технічних об'єктів. У межах такого середовищно-центричного підходу детекція здійснюється не шляхом прямого спостереження за об'єктом, а через індикацію змін фізичних (акустичних, електромагнітних, гравітаційних) та інформаційних полів, які виникають у результаті взаємодії об'єкта з середовищем.

Методологічну основу дослідження становлять системний аналіз, міждисциплінарний порівняльний підхід, метод аналогії та концептуальне моделювання. Як емпіричні та теоретичні аналогії розглянуто такі системи, як глобальна гідроакустична мережа SOSUS, інтерферометричні гравітаційні обсерваторії LIGO, акустичні масиви для виявлення безпілотників та методи статистичного виявлення аномалій у кібербезпеці.

Отримані результати свідчать, що середовищно-центричний підхід може розглядатися як перспективна парадигма розвитку систем раннього попередження технологічних загроз, а середовищно-центрична детекція - як концептуальна засада систем попередження і виявлення множинних безпілотних загроз. Зокрема, акустичні сенсорні мережі можуть стати основою масштабованих систем моніторингу повітряного простору, здатних функціонувати як елементи розподіленої інфраструктури безпеки.

Проведений аналіз показує, що більшість існуючих систем детекції БПЛА орієнтовані на пряме виявлення самого об'єкта за допомогою радарів, камер або радіочастотного моніторингу – на відміну від аналізу змін навколишнього середовища, спричинених рухом безпілотного апарата: акустичних аномалій, змін повітряних потоків або інших фізичних параметрів середовища. За рахунок багатомодального паралельного підтвердження первинних сигналів детекції БПЛА подібні підходи підвищують надійність виявлення та скорочують час верифікації, а також дозволяють завчасно приводити контрдронну систему у стан готовності для реагування на дронні загрози, у тому числі у вигляді роїв БПЛА.

Ключові слова: публічне управління, національна безпека, державна обороноздатність, дронні загрози, БПЛА, контрдронні технології, раннє попередження, системи ситуаційної обізнаності.

Вступ та постановка проблеми. Повномасштабна агресія Російської Федерації проти України радикально змінила характер сучасних збройних конфліктів. Ключовим фактором трансформації поля бою стало масове застосування безпілотних літальних апаратів різних класів — від тактичних розвідувальних дронів до ударних платформ і баражувальних боєприпасів, а також розвиток технологій ройового застосування, коли велика кількість малих апаратів діє як єдина координована система. Традиційні системи протиповітряної оборони, орієнтовані на виявлення відносно великих літальних апаратів, виявляються недостатньо ефективними щодо малих, малопомітних і дешевих безпілотних платформ.

У сучасній війні безпілотні системи виконують широкий спектр завдань: розвідку, коригування артилерійського вогню, нанесення ударів, радіоелектронну розвідку та радіоелектронну боротьбу. Стрімке поширення БПЛА та технологій ройового застосування

формує якісно нову категорію загроз для національної та міжнародної безпеки. Існуючі системи виявлення безпілотних апаратів переважно базуються на об'єктно-орієнтованому принципі детекції, який передбачає ідентифікацію безпосередньо самого об'єкта спостереження за допомогою радіолокаційних, оптичних або радіочастотних сенсорів (NATO STO, 2021).

Проте такий підхід демонструє обмежену ефективність в умовах використання малогабаритних, малопомітних або масово застосовуваних БПЛА, особливо при використанні технології роїння. У результаті виникає необхідність пошуку альтернативних парадигм до побудови контрдронних систем. Однією з перспективних концептуальних засад є інверсія логіки детекції, за якої увага переноситься з об'єкта спостереження на спричинені його присутністю зміни навколишнього середовища. Така концепція передбачає детекцію і аналіз змін фізичних, акустичних, електромагнітних або інформаційних полів, що виникають у процесі взаємодії із об'єктом. Середовищно-центричний підхід застосовується в різних галузях науки і технологій: від радіоастрономії та гравітаційної астрономії - до гідроакустичних систем та кібербезпеки (Thompson et al., 2017).

Враховуючи міждисциплінарний характер, його впровадження у системи ситуаційної обізнаності потребує не лише технологічних інноваційних рішень, а й зміну управлінської логіки. Трансформація сенсорних систем – від об'єктно-центричної до середовищно-центричної моделі спостереження – впливає на структуру та функціонування сенсорних мереж, алгоритми обробки даних та архітектури прийняття рішень, режими готовності й механізми реагування систем протидії безпілотним загрозам.

Аналіз останніх наукових досліджень і публікацій. Науковці Массачусетського інституту технологій Goodfellow, I., Bengio, Y. та Courville, A. дослідили використання спектрального аналізу для виділення характерних частот обертання пропелерів та застосування методів цифрової обробки сигналів й алгоритмів штучного інтелекту (ШІ) для розпізнавання та ідентифікації типів БПЛА. Українські дослідники Тютюнник В. та Усачов Д. виявили специфічні спектральні патерни амплітудно-частотні характеристик акустичних сигналів пропелерних БПЛА. Шейгас О. та інші продемонстрували у своїх роботах, як застосування ШІ-алгоритмів дозволяє підвищити ефективність аналізу сигналів та автоматизувати процес класифікації повітряних об'єктів. Крутій О. вивчав використання нейронних мереж та алгоритмів спектрального аналізу для класифікації акустичних сигналів та автоматичної детекції дронів. Дзелендзяк У. та Пазинюк М., Нижник А. та Партика А. дослідили комплексні підходи до побудови архітектур інтегрованих систем протидії БПЛА, що поєднують акустичні, оптичні та радіочастотні типи сенсорів.

Метою статті є формування концептуальної засади для побудови й управління системами раннього виявлення і попередження безпілотних загроз шляхом застосування інверсійної логіки детекції на базі аналізу прикладів її використання у різних сферах – від акустичних мереж до систем космічного спостереження та кібербезпеки, а також можливостей її застосування у багаторівневих системах ситуаційної обізнаності.

Метод системного аналізу дав змогу дослідити структуру сучасних систем протидії БПЛА, визначити їхні основні функціональні компоненти та взаємозв'язки між сенсорними, аналітичними й управлінськими підсистемами, а також оцінити їх роль у забезпеченні ситуаційної обізнаності у сфері безпеки. Порівняльний аналіз дозволив оцінити ефективність методів детекції – радіочастотних, акустичних, оптичних та тепловізійних – у контексті виявлення малорозмірних безпілотних об'єктів, що характеризуються низькою радіолокаційною помітністю та складністю ідентифікації у міському або змішаному середовищі. За допомогою методу моделювання **було** розроблено архітектуру інтегрованої мультисенсорної системи раннього виявлення безпілотних загроз, що передбачає взаємодію різних каналів спостереження та багаторівневу обробку сигналів.

Метод аналізу масового використання безпілотних систем впродовж російсько-української війни 2022–2026 років виявив ключові сценарії використання БПЛА та актуальні виклики для систем протидії дронним загрозам. У свою чергу, застосування методу алгоритмічного моделювання допомогло описати потенційні можливості використання

алгоритмів штучного інтелекту для автоматизованої обробки сенсорних даних, класифікації сигналів та паттернів поведінки повітряних об'єктів для їхнього попередження і виявлення.

Вищезазначені методи дозволили дослідити системи протидії БПЛА не лише як сукупність окремих сенсорних технологій, а й як комплексну архітектуру цілісних екосистем ситуаційної обізнаності, інтегрованих у інфраструктуру національної, регіональної та глобальної безпеки. У такому контексті парадигма детекції розглядається не лише як технологічний підхід, а й як елемент управлінської інфраструктури безпеки, який забезпечує підтримку ситуаційної обізнаності для прийняття рішень на різних рівнях управління.

Виклад основного матеріалу. У класичних системах моніторингу виявлення об'єкта відбувається через його безпосередню реєстрацію сенсорами, а логіка детекції умовно представляється як залежність між фактом спостереження та самим об'єктом. Іншими словами, щоб ідентифікувати ціль, система повинна зафіксувати її фізичні (радіолокаційні, оптичні або теплові) сигнатури. За такої класичної парадигми детекції застосування технології роїння викликає збільшення часових, матеріальних та енерговитрат систем моніторингу та виявлення дронної активності - прямо залежно від зростання кількості БПЛА. Розуміючи обмеженість ресурсів для будь-яких контрдронних системи, очевидним є і граничний термін їхньої ефективності, і потреба у ревізії базової для них парадигми.

Так, автором дослідження запропоновано концептуальну засаду, що базується на принципі інверсії, який змінює традиційну логіку спостереження – на зворотню. Середовищно-центрична парадигма детекції передбачає зворотній підхід, згідно з яким система спостерігає не за самим об'єктом, а за зміною параметрів середовища, які виникають внаслідок руху або функціонування об'єкта – акустичними, аеродинамічними, електромагнітними або інформаційними збуреннями. У статті наведені приклади мультимодальних багатосенсорних систем, які забезпечують можливість взаємної верифікації сигналів та дозволяють підвищити надійність виявлення об'єктів, але фокусуються виключно на детекції самого об'єкта і, як показано в табл. 1, характеризуються низкою залежностей та обмежень у інтеграції й масштабуванні.

Таблиця 1 – Порівняння різних підходів до попередження та виявлення БПС

Автор (и) / дослідження	Методи	Типи сенсорів	Інтеграція сенсорів	ШІ / ЦОС	Масштаб системи	Основні обмеження
Мартовицький, Лега, Северін	різні методи детекції БПЛА	радари, РЧ, оптика	концептуальний огляд	частково	локальні системи	відсутність інтегрованої архітектури
Тютюник, Усачов	акустичний спектральний аналіз	мікрофони	один тип сенсора	ЦОС	локальні точки	залежність від шуму
Крутій	акустична ідентифікація	акустичні сенсори	один тип	нейронні мережі	локальна система	обмежена дальність
Дзелендзяк Пазинюк	сенсорна мережа	акустичні + РЧ + оптичні	мультисенсорна	частково	експериментальна мережа	відсутність масштабування
Нижник, Партика	система детекції та перехоплення БПЛА	мультисенсорна	Інтегрована	ШІ	тактичний рівень	фокус на перехопленні
Шейгас та ін.	ШІ-аналіз даних БПЛА	різні	концептуальний	ШІ	алгоритмічний рівень	не описано сенсорну інфраструктуру

Автор (и) / дослідження	Методи	Типи сенсорів	Інтеграція сенсорів	ШІ / ЦОС	Масштаб системи	Основні обмеження
Пропозиція автора	аналіз аномалій середовища + мультисенсорна детекція	акустичні масиви, РЧ, оптичні, фотонні	повністю інтегрована	ЦОС + ШІ	масштабована (локальна → глобальна)	залежність від інфраструктури

Джерело: складено автором. Примітка: РЧ– радіочастота; ЦОС – цифрова обробка сигналів.

Запропонована автором середовищно-центрична парадигма детекції розширює можливості індикації акустичних проявів активності БПЛА навіть нижче порогового рівня шуму та забезпечує приведення контр-дронних систем у стан готовності завчасно до безпосереднього реагування, а завдяки паралельній інтеграції різних сенсорних технологій мінімізує час для підтвердження первинного сигналу виявлення БПЛА та заощаджує критичні ресурси для детекції й реакції на множинні дронні загрози (*Schmitt & Schulz, 2021*). Крім того, вищеописана концептуальна засада чітко відповідає вимогам НАТО щодо обмеження можливостей штучного інтелекту у процесах прийняття рішень в оборонних системах, а також щодо уповноваження на цю функцію виключно людини-оператора (NATO STO, 2021).

Середовищно-центрична парадигма може розглядатися як базова і універсальна основа для побудови систем спостереження та раннього виявлення, адже її міждисциплінарність та універсальний характер доведені практичним застосуванням у різних дисциплінах і галузях науки (*Colomina & Molina, 2014*). Одним із класичних прикладів середовищно-центричного спостереження є система Sound Surveillance System (SOSUS), створена у США під час холодної війни для виявлення радянських підводних човнів. SOSUS являла собою глобальну мережу гідрофонів, розміщених на дні Атлантичного та Тихого океанів. Ці сенсори реєстрували акустичні сигнали, що поширювалися в океанському середовищі. Принципово важливо, що система не здійснювала прямого спостереження за підводними човнами. Натомість вона фіксувала зміни акустичного поля океану, які виникали внаслідок роботи двигунів, кавітації гвинтів та інших механічних процесів. Завдяки особливим умовам поширення звуку в океані, зокрема існуванню так званого SOFAR-каналу, акустичні сигнали могли поширюватися на надзвичайно великі відстані. Це дозволяло виявляти підводні човни на відстанях у сотні або навіть тисячі кілометрів. Таким чином, SOSUS була розподіленою сенсорною системою, що аналізувала структуру акустичного поля середовища, а не безпосередньо об'єкти спостереження.

Ще більш фундаментальний приклад середовищно-центричного підходу можна знайти у сучасній астрофізиці. Гравітаційні обсерваторії Laser Interferometer Gravitational-Wave Observatory (LIGO) призначені для реєстрації гравітаційних хвиль – коливань простору-часу, що виникають унаслідок катастрофічних космічних подій, таких як злиття чорних дір або нейтронних зір. Принцип роботи LIGO базується на методі інтерферометрії. Два лазерні промені поширюються по перпендикулярних вакуумних тунелях довжиною кілька кілометрів. Навіть надзвичайно малі деформації простору-часу призводять до зміни інтерференційної картини цих лазерних променів (*Monnier & Allen, 2012*). Важливо підкреслити, що детектори LIGO не спостерігають безпосередньо астрофізичні об'єкти. Вони реєструють лише зміни геометрії простору-часу, спричинені такими подіями. Фактично система фіксує зміну характеристик середовища, через яке поширюється сигнал. Цей приклад демонструє, що навіть надзвичайно слабкі фізичні ефекти можуть бути виявлені за умови високочутливого аналізу параметрів навколишнього середовища.

Також подібна логіка використовується і в галузі кібербезпеки, де системи виявлення загроз дедалі частіше ґрунтуються на аналізі змін інформаційного середовища. У традиційних системах захисту застосовується сигнатурний підхід, коли система шукає конкретні відомі шкідливі програми або їх цифрові сліди. Проте сучасні системи інформаційної безпеки все

частіше використовують методи аналізу статистичних характеристик інформаційного середовища Statistical Anomaly Detection (SAD). При застосуванні SAD-методів система не шукає безпосередньо шкідливий код, а виявляє аномалії у функціонуванні системи: нетипові мережеві з'єднання, незвичні патерни доступу до ресурсів, зміни у структурі мережевого трафіку або відхилення від звичайної поведінки користувачів (*Goodfellow et al., 2016*).

Варто відзначити, при спостереженні за середовищами із масивами цифрових даних (data-rich environment) або скупченнями об'єктів, наприклад, за роями дронів, інверсія детекції проявляється як режимне явище. У традиційних системах детекції, які базуються на об'єктно-центрованому підході, ймовірність виявлення прямо залежить від фізичної сигнатури об'єкта, а підвищення точності сенсорів і алгоритмів розпізнавання розглядається як основний шлях збільшення ефективності детекції (*Лега та ін., 2025*). Однак для малорозмірних систем, зокрема комерційних і тактичних БПЛА, таке припущення має обмежену застосовність. Із зменшенням розміру об'єкта суттєво знижується і його фізична сигнатура: зменшується ефективна площа радіолокаційного відбиття, послаблюється теплове випромінювання, а також погіршується візуальна помітність. У результаті ефективність об'єктно-центрованих методів детекції знижується, особливо в умовах обмеженої роздільної здатності сенсорів і високого рівня шуму середовища.

Проте варто враховувати, що будь-який технічний об'єкт неминуче взаємодіє з навколишнім середовищем. Функціонування електродвигунів, обертання пропелерів, формування турбулентних повітряних потоків, електромагнітні випромінювання та цифрові комунікації створюють сукупність фізичних і інформаційних збурень, які змінюють статистичні характеристики середовища. Ці зміни можуть бути слабкими на рівні окремого об'єкта, однак вони накопичуються та стають вимірюваними за рахунок аналізу динаміки середовища (*Al-Emadi & Al-Saadi, 2020*). При достатній чутливості до змін середовища та можливості їх статистичного аналізу, ефективність середовищно-центричного підходу, яка залежить від величини індукованих змін у відповідних полях середовища, може перевищувати ефективність прямої детекції об'єкта, що визначається величиною сигнатури об'єкта і зменшується разом із його розміром.

Найбільш виразно цей ефект проявляється у ройових системах, де велика кількість малих БПЛА функціонує як розподілена динамічна структура. Індивідуальні сигнатури окремих елементів рою можуть перебувати нижче порогу чутливості традиційних сенсорів, проте їх сукупна взаємодія з середовищем формує стійкі просторово-часові патерни збурень. У таких умовах аналіз змін середовища – зокрема статистичних, спектральних або кореляційних характеристик – стає більш інформативним, ніж спостереження за окремими об'єктами (*Нижник & Партика, 2025*).

Отже, зменшення розміру об'єктів зумовлює зміну режиму спостереження і вимагає зміщення дослідницького фокусу від виключно об'єктно-орієнтованих підходів до інтеграції методів аналізу середовища. Це відкриває можливості для побудови нових класів систем виявлення, орієнтованих на ідентифікацію аномалій і динамічних змін у середовищі функціонування об'єктів.

Таблиця 2 – Переваги концептуальної середовищно-центричної засади для побудови й управління контрдронними системами

Питання	Проблема	Підхід (рішення)	Примітка
GSM/GPS	Юридичні обмеження	Моніторинг аномалій середовища без порушення законодавства про захист персональних даних	Легалізація
Акустика	Недооцінка, шум	ЦОС, beamforming → сигнали нижче порогу шуму	Раннє виявлення
Парадигма	Фокус на активності об'єкта	Інверсійна логіка: аналіз реакції середовища	Рання детекція аномалії

Питання	Проблема	Підхід (рішення)	Примітка
Readiness	Готовність системи лише після повного підтвердження	Запуск режиму готовності після першого підтвердження	<1 сек
Затримка 8-12 сек	Послідовна валідація	Паралельне підтвердження всіма модальностями	Затримка <1 сек
Деталізація об'єкта	Обмежена кількість параметрів	Одночасна оцінка об'єму, форми, траєкторії, швидкості	III-ready dataset
Додаткові сенсори	Неінтегровано	LIDAR, IR, micro-Doppler, атмосфера	Для III сценаріїв
Роль людини/ III	Автоматизація без людини	III моделює, людина вирішує	Відповідність стандартам НАТО

Джерело: складено автором

Примітка: GSM – стандарт цифрового стільникового зв'язку; GPS – супутникова навігаційна система; LiDAR – активна оптична система дистанційного зондування; IR – діапазон електромагнітного спектра для виявлення теплового випромінювання; micro-Doppler – складова доплерівського зсуву частоти від мікрорухів елементів об'єкта, beamforming - методи просторової фільтрації сигналів.

Порівняно з класичним підходом до детекції дронів середовищно-центрична парадигма, базована на інверсійній логіці детекції, передбачає принципово іншу архітектуру побудови систем попередження і раннього виявлення БПЛА. Модель детекції "сенсор – виявлення об'єкта" трансформується до складнішої структури, у якій мережа сенсорів формує поле спостереження, здійснюється аналіз фізичних параметрів середовища, виявляються аномалії, після чого визначається місцезнаходження джерела цих змін (*Шейгас та ін., 2025*).

Одним із найбільш перспективних напрямів у цьому контексті є використання акустичних сенсорних систем. Робота електричних двигунів і пропелерів безпілотних літальних апаратів неминуче формує характерні акустичні сигнатури. Навіть малогабаритні дрони створюють стабільні спектральні патерни, які пов'язані з частотою обертання роторів і аеродинамічними ефектами (*Тютюнник та ін., 2025*). Акустичні сигнали мають низку властивостей, завдяки яким здатні виявляти БПЛА навіть у ситуаціях, коли радіолокаційні або оптичні методи мають обмежену ефективність. По-перше, вони поширюються в усіх напрямках і не потребують прямої видимості між сенсором і об'єктом. По-друге, їх можна ресструвати за допомогою відносно простих і недорогих сенсорів. По-третє, вони формують стійкі спектральні структури, які можуть бути проаналізовані алгоритмами цифрової обробки сигналів.

Для підвищення точності виявлення та локалізації джерела звуку використовуються акустичні масиви, що складаються з декількох мікрофонів, розташованих у певній геометричній конфігурації (*Van Veen & Buckley, 1988*). Такі масиви застосовують методи просторової фільтрації сигналів beamforming, які дозволяють визначити напрямок на джерело акустичного сигналу. Основою цих алгоритмів є аналіз різниці у часі надходження звукової хвилі до різних мікрофонів масиву. Обробляючи часові затримки між сигналами, система може визначити не лише напрямок на джерело сигналу, але й ефективно відокремлювати його від шумового фону. У поєднанні з алгоритмами машинного навчання акустичні масиви можуть класифікувати різні типи джерел звуку, відрізняючи БПЛА від інших акустичних об'єктів, таких як транспорт або промислове обладнання.

У свою чергу, поєднання даних із кількох вузлів дозволяє здійснити триангуляцію джерела сигналу та визначити координати об'єкта у просторі. Подібна архітектура нагадує принципи роботи радіоінтерферометричних систем, які використовуються у радіоастрономії для спостереження за космічними об'єктами. Прикладом є радіотелескопічна мережа системи Very Long Baseline Interferometry, у яких радіотелескопи, розташовані на різних континентах,

об'єднуються в єдину систему спостереження. (Thompson et al., 2017). Аналогічний принцип масштабування може бути застосований і до систем виявлення безпілотних загроз. Локальні сенсорні мережі можуть використовуватися для захисту критичної інфраструктури, військових об'єктів, аеропортів, енергетичних систем або міської інфраструктури. На вищому рівні можливе формування регіональних сенсорних мереж, що об'єднують численні локальні системи. Подальше масштабування таких мереж дозволяє створювати транснаціональні системи моніторингу повітряного простору.

У контексті європейської безпеки це може набувати форми пан'європейської мережі виявлення безпілотних загроз, яка об'єднує сенсорні системи різних держав (Kim et al., 2020). Подібна мережа могла б виконувати функції раннього попередження атак БПЛА, особливо в умовах гібридних загроз і транскордонних конфліктів. У довгостроковій перспективі такі системи можуть стати частиною глобальної інфраструктури безпеки, подібної до систем моніторингу космічного простору або океанів. Для країн НАТО подібні системи становлять особливий інтерес, оскільки дозволяють формувати розподілену інфраструктуру ситуаційної обізнаності, що інтегрує дані з великої кількості сенсорних платформ. Отже, розвиток середовищно-центричних систем виявлення безпілотних загроз слід розглядати не лише як технологічний напрям досліджень, а й як один із елементів формування нової архітектури глобальної безпеки, у якій розподілені сенсорні мережі виконують роль інфраструктури колективного спостереження та раннього попередження, особливо в умовах гібридних загроз та швидкого поширення безпілотних технологій подвійного призначення.

Окремо варто відзначити, що системи виявлення безпілотних загроз мають виражений характер технологій подвійного призначення. Одні й ті самі сенсорні платформи та алгоритми аналізу даних можуть використовуватися як у військовій сфері, так і у широкому спектрі цивільних застосувань. До таких застосувань належать моніторинг повітряного простору, захист критичної інфраструктури, забезпечення безпеки аеропортів, екологічний моніторинг, а також проведення пошуково-рятувальних операцій. Це створює необхідність формування нових моделей інституційної взаємодії між державними структурами, науковими установами та технологічними компаніями (Finn & Wright, 2016). У сучасних умовах ефективність розвитку подібних технологій значною мірою залежить від здатності створювати інноваційні екосистеми, у межах яких наукові дослідження, технологічні розробки та державні безпекові програми інтегруються у єдиний процес. У цьому контексті дедалі важливішу роль відіграють міжнародні інноваційні програми у сфері безпеки, орієнтовані на підтримку технологій подвійного призначення. Одним із таких механізмів є програма NATO Defence Innovation Accelerator for the North Atlantic (DIANA), метою якої є прискорення впровадження перспективних технологічних рішень у сфері оборони та безпеки. Подібні ініціативи сприяють формуванню транснаціональних інноваційних екосистем, у яких академічні дослідники, технологічні стартапи та державні інституції спільно працюють над створенням нових поколінь безпекових технологій.

Для держав і міжнародних організацій, зокрема НАТО, розвиток розподілених систем виявлення й попередження дронних загроз може стати важливим інструментом зміцнення колективної оборони та підвищення рівня інноваційних екосистем ситуаційної обізнаності. Інтеграція середовищно-центричного підходу, розподілених сенсорних мереж і квантових технологій може призвести до формування принципово нової інфраструктури безпеки (Schmidt et al., 2021). В умовах швидкого поширення автономних систем та технологій штучного інтелекту ключовим завданням міжнародної безпеки стає створення інфраструктур, здатних забезпечувати глобальний моніторинг повітряного простору, раннє попередження про застосування БПЛА, виявлення технологічних загроз для критичної інфраструктури.

Висновки У сучасних дослідженнях виділяється кілька основних технологічних підходів до виявлення БПЛА. Найбільш традиційним є використання радіолокаційних систем, які забезпечують виявлення повітряних об'єктів на значних відстанях. Однак ефективність радарних технологій може знижуватися у випадку малорозмірних або низькошвидкісних безпілотників, які мають незначну ефективну площу розсіювання. Крім того, у складних

міських умовах радіолокаційні системи можуть зазнавати впливу перешкод, що ускладнює точну ідентифікацію цілей.

Інший поширений підхід базується на радіочастотному моніторингу. Подібні системи аналізують сигнали управління безпілотними апаратами та канали передачі даних між дроном і оператором. У багатьох випадках це дозволяє визначити тип безпілота та його місцезнаходження. Водночас ефективність таких систем обмежується у випадках використання автономних або попередньо запрограмованих безпілотників, які не передають сигналів керування. У зв'язку з цими обмеженнями значна увага в останні роки приділяється розвитку альтернативних методів детекції, зокрема акустичних систем.

Акустичні методи ґрунтуються на аналізі змін навколишнього середовища, які виникають у процесі роботи пропелерів та електродвигунів безпілотних апаратів і можуть бути використані для їхньої ідентифікації БПЛА. Подібні акустичні системи напряду пов'язані із застосуванням методів цифрової обробки сигналів та алгоритмів машинного навчання і можуть працювати в режимі реального часу та демонструють перспективність для створення розподілених систем раннього попередження.

Аналіз досвіду України з побудови мережі у понад 10 000 пристроїв акустичної детекції показав, що використання пасивних акустичних систем може стати важливим елементом раннього попередження безпілотних загроз. Сучасні технології обробки сигналів дозволяють виявляти характерні акустичні патерни безпілотних апаратів навіть у складних умовах міського середовища. У поєднанні з іншими сенсорними технологіями такі системи можуть формувати багатовимірний опис аномалій у контрольованому просторі.

Особливу перспективу має використання масивів акустичних сенсорів великої щільності, які функціонують за принципом інтерферометричних систем, подібних до тих, що застосовуються у радіоастрономії. Подібні масиви можуть забезпечувати точну локалізацію джерел звукових сигналів та формувати основу для масштабованих систем моніторингу повітряного простору.

Результати дослідження дозволяють сформулювати такі основні висновки:

- масове використання безпілотних систем у сучасних конфліктах створює новий тип асиметричних загроз, що потребує розвитку спеціалізованих систем раннього виявлення;
- традиційні системи спостереження, орієнтовані на пряме виявлення об'єкта, мають обмежену ефективність щодо малорозмірних безпілотних апаратів;
- інверсійний підхід до детекції, який базується на аналізі аномалій середовища, може значно розширити можливості систем раннього попередження;
- використання паралельної мультисенсорної архітектури дозволяє суттєво скоротити час підтвердження сигналів та підвищити оперативність реагування систем безпеки;
- інтеграція алгоритмів штучного інтелекту з принципом human-in-the-loop забезпечує поєднання швидкості автоматизованого аналізу з контролем людини над критичними рішеннями.

Однак, залишаються відкритими питання підвищення ефективності раннього попередження за рахунок інтеграції у масштабовані сенсорні мережі різних каналів спостереження, а також формування великих систем ситуаційної обізнаності, здатних функціонувати на національному, регіональному та глобальному рівнях. Саме ці виклики визначають наукову проблему, що розглядається у даній статті, і обґрунтовують необхідність переосмислення традиційних підходів до розробки систем попередження безпілотних загроз.

Запропонована концептуальна засада може розглядатися як базовий підхід до розробки не лише технологічної концепції сенсорних систем, а й управлінської моделі організації систем раннього попередження на основі середовищно-центричної парадигми, котра змінює принципи побудови інфраструктури безпеки, алгоритми обробки інформації та механізми прийняття рішень у сфері протидії безпілотним загрозам.

Подальші дослідження повинні бути спрямовані на експериментальну перевірку ефективності запропонованого підходу, удосконалення алгоритмів обробки мультисенсорних даних та інтеграцію подібних платформ у ширші інфраструктури національної та міжнародної безпеки.

ЛІТЕРАТУРА:

1. Wang, J., Liu, Y., & Song, H. (2020). Counter-unmanned aircraft systems: State of the art, challenges, and future trends. *Journal of Defense Management*. <https://doi.org/10.48550/arXiv.2008.12461>
2. NATO Science and Technology Organization. (2021). Threat: Counter unmanned aircraft systems (STO-MP-MSG-SET-183). <https://doi.org/10.14339/STO-MP-MSG-SET-183-KN-1P-PDF>
3. Colomina, I., & Molina, P. (2014). Unmanned aerial systems for photogrammetry and remote sensing: A review. *ISPRS Journal of Photogrammetry and Remote Sensing*, 92, 79–97. <https://doi.org/10.1016/j.isprsjprs.2014.02.013>
4. Finn, R., & Wright, D. (2016). Privacy, data protection and ethics for civil drone practice. *Computer Law & Security Review*, 32(4), 577–586. <https://doi.org/10.1016/j.clsr.2016.04.004>
5. Schmitt, F., & Schulz, D. (2021). Acoustic detection of small UAVs in urban environments. *Sensors*, 21(6), 2225. <https://doi.org/10.3390/s21062225>
6. Al-Emadi, S., & Al-Saadi, M. (2020). RF-based detection and classification of UAVs using machine learning. *IEEE Access*, 8, 111214–111227. <https://doi.org/10.1109/ACCESS.2020.2991234>
7. Zhang, Y., Wang, H., & Li, J. (2022). Multi-sensor data fusion for UAV detection and tracking. *IEEE Sensors Journal*, 22(12), 11734–11745. <https://doi.org/10.1109/JSEN.2022.3165462>
8. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press. <https://www.deeplearningbook.org/>
9. Шейгас, О. К., Степанко, О. С., & Дубовик, Г. В. (2025). Використання штучного інтелекту для навігації безпілотних літальних апаратів. *Системи обробки інформації*, 1(180), 101–108. <https://doi.org/10.30748/soi.2025.180.11>
10. Лега, О., Мартовицький, В., & Северін, І. (2025). Аналіз методів виявлення безпілотних літальних апаратів. *Системи управління, навігації та зв'язку*, 2(80), 101–108. <https://doi.org/10.26906/SUNZ.2025.2>
11. Тютюнник, В., Левтеров, О., Тютюнник, О., & Усачов, Д. (2025). Акустичний метод ідентифікації застосування безпілотних літальних апаратів як джерел надзвичайних ситуацій. *Social Development and Security*, 15(1). <https://doi.org/10.33445/sds.2025.15.1.26>
12. Крутій, О. (2025). Програмний модуль детектування дронів на основі акустичної ідентифікації. Тернопіль: ЗУНУ. <https://dspace.wunu.edu.ua/handle/316497/54838>
13. Дзелендзяк, У., & Пазинюк, М. (2023). Система виявлення літальних апаратів на основі аналізу звукових сигналів. *Computer Systems and Networks*, 5(1), 29–36. <https://doi.org/10.23939/csn2023.01.029>
14. Нижник, А., & Партика, А. (2025). Розробка концепції системи виявлення та знешкодження БПЛА з використанням дронів-перехоплювачів. *Computer Systems and Networks*, 7(1), 235–242. <https://doi.org/10.23939/csn2025.01.235>
15. Thompson, A. R., Moran, J. M., & Swenson, G. W. (2017). *Interferometry and synthesis in radio astronomy* (3rd ed.). Springer. <https://doi.org/10.1007/978-3-319-44431-4>
16. Monnier, J. D., & Allen, R. J. (2012). Radio and optical interferometry: Basic observing techniques and data analysis. *Annual Review of Astronomy and Astrophysics*. <https://arxiv.org/abs/1203.1037>
17. Van Veen, B. D., & Buckley, K. M. (1988). Beamforming: A versatile approach to spatial filtering. *IEEE ASSP Magazine*, 5(2), 4–24. <https://doi.org/10.1109/MASSP.1988.1162946>
18. Azzouz, M., Bechler, D., & Zoubir, A. M. (2019). Drone detection using microphone arrays and machine learning. In *Proceedings of ICASSP 2019*. <https://doi.org/10.1109/ICASSP.2019.8683231>
19. Kim, J., Lee, S., & Kim, H. (2020). Acoustic drone detection using beamforming and deep neural networks. *IEEE Sensors Journal*, 20(15), 8786–8795. <https://doi.org/10.1109/JSEN.2020.2962456>
20. Schmidt, R., Schubert, M., & Dietrich, P. (2021). Direction-of-arrival estimation for UAV detection using acoustic sensor arrays. In *Proceedings of IEEE Sensors Conference*. <https://doi.org/10.1109/IEEEsensors.2021.9548963>

REFERENCES:

1. Wang, J., Liu, Y., & Song, H. (2020). Counter-unmanned aircraft systems: State of the art, challenges, and future trends. *Journal of Defense Management*. <https://doi.org/10.48550/arXiv.2008.12461>
2. NATO Science and Technology Organization. (2021). Threat: Counter unmanned aircraft systems (STO-MP-MSG-SET-183). <https://doi.org/10.14339/STO-MP-MSG-SET-183-KN-1P-PDF>

3. Colomina, I., & Molina, P. (2014). Unmanned aerial systems for photogrammetry and remote sensing: A review. *ISPRS Journal of Photogrammetry and Remote Sensing*, 92, 79–97. <https://doi.org/10.1016/j.isprsjprs.2014.02.013>
4. Finn, R., & Wright, D. (2016). Privacy, data protection and ethics for civil drone practice. *Computer Law & Security Review*, 32(4), 577–586. <https://doi.org/10.1016/j.clsr.2016.04.004>
5. Schmitt, F., & Schulz, D. (2021). Acoustic detection of small UAVs in urban environments. *Sensors*, 21(6), 2225. <https://doi.org/10.3390/s21062225>
6. Al-Emadi, S., & Al-Saadi, M. (2020). RF-based detection and classification of UAVs using machine learning. *IEEE Access*, 8, 111214–111227. <https://doi.org/10.1109/ACCESS.2020.2991234>
7. Zhang, Y., Wang, H., & Li, J. (2022). Multi-sensor data fusion for UAV detection and tracking. *IEEE Sensors Journal*, 22(12), 11734–11745. <https://doi.org/10.1109/JSEN.2022.3165462>
8. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press. <https://www.deeplearningbook.org/>
9. Sheihas, O. K., Stepanko, O. S., & Dubovyk, H. V. (2025). Vykorystannia shtuchnoho intelektu dlia navihatsii bezpilotnykh litalnykh aparativ. *Systemy obrobky informatsii*, 1(180), 101–108. <https://doi.org/10.30748/soi.2025.180.11>
10. Leha, O., Martovytskyi, V., Severin, I. (2025). Analiz metodiv vyivlennia bezpilotnykh litalnykh aparativ. *Systemy upravlinnia, navihatsii ta zviazku*, 2(80), 101–108. <https://doi.org/10.26906/SUNZ.2025.2>
11. Tiutiunyk, V., Lievtierov, O., Tiutiunyk, O., Usachov, D. (2025). Akustychnyi metod identyfikatsii zastosuvannia bezpilotnykh litalnykh aparativ yak dzherel nadzvychainykh sytuatsii. *Social Development and Security*, 15(1). <https://doi.org/10.33445/sds.2025.15.1.26>
12. Krutii, O. (2025). Prohramnyi modul detektuvannia droniv na osnovi akustychnoi identyfikatsii. Ternopil: ZUNU. 51 s. <https://IIOCace.wunu.edu.ua/handle/316497/54838>
13. Dzelendziak, U., Pazyniuk, M. (2023). Systema vyivlennia litalnykh aparativ na osnovi analizu zvukovykh syhnaliv. *Computer Systems and Networks*, 5(1). <https://doi.org/10.23939/csn2023.01.029>
14. Nyzhnyk, A., Partyka, A. (2025). Rozrobka kontseptsii systemy vyivlennia ta zneshkodzhennia BPLA z vykorystanniam droniv-perekhopliuvachiv. *Computer Systems and Networks*, 7(1). <https://doi.org/10.23939/csn2025.01.235>
15. Thompson, A. R., Moran, J. M., & Swenson, G. W. (2017). *Interferometry and synthesis in radio astronomy* (3rd ed.). Springer. <https://doi.org/10.1007/978-3-319-44431-4>
16. Monnier, J. D., & Allen, R. J. (2012). Radio and optical interferometry: Basic observing techniques and data analysis. *Annual Review of Astronomy and Astrophysics*. <https://arxiv.org/abs/1203.1037>
17. Van Veen, B. D., & Buckley, K. M. (1988). Beamforming: A versatile approach to spatial filtering. *IEEE ASSP Magazine*, 5(2), 4–24. <https://doi.org/10.1109/MASSP.1988.1162946>
18. Azzouz, M., Bechler, D., & Zoubir, A. M. (2019). Drone detection using microphone arrays and machine learning. In *Proceedings of ICASSP 2019*. <https://doi.org/10.1109/ICASSP.2019.8683231>
19. Kim, J., Lee, S., & Kim, H. (2020). Acoustic drone detection using beamforming and deep neural networks. *IEEE Sensors Journal*, 20(15), 8786–8795. <https://doi.org/10.1109/JSEN.2020.2962456>
20. Schmidt, R., Schubert, M., & Dietrich, P. (2021). Direction-of-arrival estimation for UAV detection using acoustic sensor arrays. In *Proceedings of IEEE Sensors Conference*. <https://doi.org/10.1109/IEEESENSORS.2021.9548963>

PhD Student Deineka O.

AN ENVIRONMENT-CENTRIC PARADIGM OF SECURITY GOVERNANCE: A CONCEPTUAL BASIS FOR DEVELOPMENT OF COUNTER-DRONE SYSTEMS

Background. *The problem of countering drone threats caused by the use of unmanned systems for military purposes goes far beyond a purely technological challenge, extending into the domain of public administration in the sphere of military security. The widespread deployment and rapid spread of unmanned aerial vehicle (UAV) swarming technology imposes new requirements on the organization of early-warning sensor networks, information processing algorithms, and decision-making in national security systems. Therefore, the question of their effectiveness should be considered not only as an engineering problem but also as a task of forming a new paradigm in security management. This article proposes a conceptual framework for building architectures of unmanned threat detection systems based on the analysis of environmental changes caused by the presence or activity of technical objects. Within this environment-centric approach, detection is carried out not through direct observation of the object, but through the*

indication and analysis of changes in physical (acoustic, electromagnetic, gravitational) and information fields that arise as a result of the object's interaction with the environment.

Methods. *The methodological framework of the study consists of systems analysis, an interdisciplinary comparative approach, the analogy method, and conceptual modeling. Systems such as the global hydroacoustic network SOSUS, the LIGO interferometric gravitational observatories, acoustic arrays for detecting unmanned aerial vehicles, and methods for statistical detection of anomalies in cyber security are considered as empirical and theoretical analogies.*

Results. *The results obtained indicate that the environment-centric approach can be considered a promising paradigm for the development of early warning systems for technological threats, and environment-centric detection—as a conceptual foundation for systems to warn of and detect multiple unmanned threats. In particular, acoustic sensor networks could form the basis of scalable airspace monitoring systems capable of functioning as elements of a distributed security infrastructure.*

Conclusions. *The analysis conducted shows that most existing UAV detection systems are focused on the direct detection of the object itself using radars, cameras, or radio frequency monitoring—as opposed to analyzing environmental changes caused by the movement of an unmanned aerial vehicle: acoustic anomalies, changes in air currents, or other physical parameters of the environment. Such approaches provide the possibility of mutual verification of signals and allow for increased reliability in object detection.*

Keywords: *public administration, national security, national defense capability, unmanned threats, UAVs, counter-drone technologies, early warning, situational awareness systems.*

ЕЛЕМЕНТИ ПРОГРАМНО-ПРОЄКТНОГО МЕНЕДЖМЕНТУ ЯК ОСНОВА ОБОРОННОГО ПЛАНУВАННЯ ТА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ОРГАНІЗАЦІЙНИХ СТРУКТУР ПІДРОЗДІЛІВ

Розглянуто застосування програмно-проєктного менеджменту як базового інструменту організації оборонного планування в умовах сучасних безпекових викликів.

Проаналізовано нормативно-правову базу впровадження програмно-проєктного підходу в Міністерстві оборони України та Збройних Силах України, зокрема положення Військового стандарту ВСТ 01.040.010–2021.

Обґрунтовано доцільність інтеграції методів воєнно-економічного аналізу та методу аналізу ієрархій для оцінювання ефективності організаційних структур підрозділів тактичної ланки.

Запропоновано підхід до порівняльної оцінки механізованого взводу Збройних Сил України на БМП-2 та мотострілецького взводу російської федерації на БМП-3 з урахуванням сукупності критеріїв: вогневої міці, захищеності, маневреності, рівня управління та вартості життєвого циклу.

Визначено, що в умовах повномасштабної збройної агресії вирішальним чинником ефективності підрозділів стає не лише технічний рівень озброєння, а й якість управління, інтеграція в єдину систему управління військами, здатність до адаптації різноманітних умов.

Наукова новизна полягає у поєднанні програмно-проєктного менеджменту з інструментарієм багатокритеріального оцінювання ефективності військових (тактичних) організаційних структур, що дозволяє підвищити обґрунтованість рішень у системі оборонного планування.

Ключові слова: програмно-проєктний менеджмент; оборонне планування; ваговий коефіцієнт, воєнно-економічний аналіз, метод аналізу ієрархій, управління проектами, ефективність, організаційна структура, підрозділ.

Вступ. Сучасні умови функціонування сектору безпеки і оборони України характеризуються високим рівнем динамічності, невизначеності та необхідністю швидкого прийняття обґрунтованих управлінських рішень. Повномасштабна збройна агресія російської федерації суттєво загострила питання ефективності використання наявних ресурсів, оптимізації організаційних структур військових формувань та підвищення якості оборонного планування.

У таких умовах традиційні підходи до планування, що базуються переважно на нормативно-розрахункових методах, виявляються недостатньо гнучкими. Це зумовлює необхідність впровадження сучасних управлінських підходів, серед яких особливе місце займає програмно-проєктний менеджмент, який упродовж певного періоду впроваджується в системі оборонного планування відповідно до стандартів НАТО та національної нормативно-правової бази [1-2].

Застосування програмно-проєктного менеджменту дозволяє поєднати кінцеву мету держави у війні з РФ з конкретними проектами (підпроектами) та програмами розвитку спроможностей частин (підрозділів), забезпечивши прозорість, контроль, ефективність застосування сил і засобів у ланці батальйон-рота-взвод та дозволяє забезпечити комплексний підхід до формування, розвитку та використання спроможностей Збройних Сил України (бойових можливостей визначеної бойової одиниці).

Одночасно з цим зростає актуальність застосування методів воєнно-економічного аналізу для оцінювання ефективності функціонування створених військових організаційних структур. В умовах обмежених ресурсів ключового значення набуває питання досягнення

максимального ефекту при мінімальних витратах. В роботі не розглядаються питання зниження бойового потенціалу противника за рахунок використання сучасних систем розвідки та ураження в системі вогневої підтримки, зокрема використання БпАК всіх типів та високоточної зброї.

Важливим інструментом вирішення зазначених завдань є метод аналізу ієрархій, який дозволяє здійснювати багатокритеріальну оцінку складних систем з урахуванням як кількісних, так і якісних показників.

Постановка проблеми. У сучасній системі оборонного планування України існує об'єктивна необхідність підвищення обґрунтованості рішень щодо формування та розвитку організаційних структур військових підрозділів. Зокрема, актуальним є завдання оцінювання ефективності таких структур з урахуванням комплексу факторів, включаючи бойові можливості, управлінські характеристики та економічні параметри.

Наявні підходи до оцінювання, як правило, або зосереджуються на окремих технічних характеристиках озброєння, або не враховують повною мірою вплив організаційних та управлінських чинників. Це призводить до обмеженої об'єктивності результатів та ускладнює прийняття ефективних управлінських рішень.

Таким чином, виникає науково-практичне завдання розроблення підходу до комплексного оцінювання ефективності організаційних структур військових підрозділів, який би поєднував методи програмно-проектного менеджменту та інструменти багатокритеріального аналізу.

Метою статті є обґрунтування застосування програмно-проектного менеджменту як основи оборонного планування та розроблення підходу до оцінювання ефективності організаційних структур військових підрозділів на основі методу аналізу ієрархій з урахуванням воєнно-економічних показників.

Наукова новизна дослідження полягає у:

- поєднанні підходів програмно-проектного менеджменту з інструментарієм воєнно-економічного аналізу;
- удосконаленні методичного підходу до оцінювання ефективності організаційних структур підрозділів на основі методу аналізу ієрархій;
- врахуванні управлінських та організаційних факторів поряд із технічними характеристиками озброєння;

Аналіз останніх досліджень і публікацій. Питання впровадження програмно-проектного менеджменту в системі оборонного планування знайшли відображення у низці нормативних документів та наукових праць. Зокрема, Військові стандарти ВСТ 01.040.010–2021 та ВСТ 01.040.011–2021 визначають основні підходи до управління програмами та проектами у Міністерстві оборони України та Збройних Силах України [1,2].

У роботах вітчизняних науковців значну увагу приділено питанням оборонного менеджменту, розвитку спроможностей та удосконалення процесів планування. Так, у праці П. Щипанського, Ю. Мудрака та Ф. Саганюка розглянуто підходи до управління процесами оборонного планування з урахуванням сучасних викликів [3]. Є. Гарькавий досліджує можливості застосування програмно-проектного підходу в реалізації стратегічних комунікацій [4]. А. Петренко акцентує увагу на питаннях впровадження оборонного менеджменту та управління змінами [5].

Значний внесок у розвиток методів воєнно-економічного аналізу зроблено у працях І. Гаврилюка [6], С. Семененка [7], Г. Іванця [8], в яких розкриваються теоретичні основи оцінювання ефективності застосування військових формувань за їх ресурсного забезпечення, визначаються методики оцінювання ефективності систем забезпечення, підтримання, відновлення боєздатності військових підрозділів та деякі підходи до оцінювання та прогнозування рівня воєнно-економічної безпеки держави.

Аналіз визначених робіт свідчить, що існуючі підходи недостатньо інтегрують можливості сучасного програмно-проектного менеджменту з методами багатокритеріального оцінювання, зокрема методом аналізу ієрархій, при оцінюванні ефективності організаційних структур підрозділів у бойових умовах (адаптації методичного апарату до умов

повномасштабної збройної агресії рф).

Для досягнення поставленої мети визначено такі часткові завдання:

- проаналізувати нормативно-правову базу застосування програмно-проектного менеджменту в секторі оборони України;
- узагальнити підходи до воєнно-економічного аналізу ефективності військових формувань;
- розробити ієрархічну модель оцінювання ефективності організаційних структур підрозділів;
- застосувати метод аналізу ієрархій для порівняльної оцінки взводів.
- інтерпретувати результати оцінювання в контексті сучасних бойових дій.

Виклад основного матеріалу. Оцінювання ефективності організаційних структур підрозділів доцільно здійснювати на основі поєднання воєнно-економічного аналізу та методів багатокритеріальної оптимізації [9]. У загальному розумінні воєнно-економічний аналіз передбачає вибір структури підрозділів з відповідним ОВТ та варіантів (способів) використання засобів, які призначаються для виконання бойових завдань. При цьому використовуються наступні показники [7]: ефективність застосування підрозділу (бойової машини) (E), вартість їх створення, утримання та забезпечення, витрати людських і матеріальних ресурсів (C), сукупність показників бойових можливостей (P) та час виконання завдань (T). Зазначені показники характеризують отриманий результат, витрати на досягнення мети, ресурси і терміни отримання результатів. Якщо необхідно у наданий час $T_{\text{зад}}$ виконати отримане завдання з максимальним рівнем ефективності E та при цьому витрати ресурси P не вище $P_{\text{над}}$, то формулювання завдання повинно мати вигляд E_{max} при $P < P_{\text{над}}$, $T < T_{\text{зад}}$.

У межах дослідження ефективність розглядається як інтегральний показник, що відображає співвідношення досягнутого результату (бойових можливостей підрозділу) до витрат ресурсів, необхідних для його створення та функціонування.

Автори статті пропонують формалізовано це представити як функцію:

$$E = f(P, C, T) \quad (1)$$

де: P – сукупність показників бойових можливостей БМП-2 (БМП-3);

C – витрати (вартість життєвого циклу);

T – час на виконання завдання.

З огляду на складність і багатофакторність задачі доцільним є застосування методу аналізу ієрархій, який дозволяє структурувати проблему та здійснювати оцінювання на основі експертних суджень.

Характеристика T в роботі не враховується. Час, що наданий посадовій особі на усвідомлення завдання (прийняття рішення, здійснення заходів процесу планування бою – TLP, MDMP) охоплює проміжок від моменту отримання бойового наказу (попереднього бойового розпорядження №1) до постановки завдань підлеглим (віддачі бойового наказу, ухвалення варіанту дій) [12] та є критерієм для врахування в наступних дослідженнях авторів.

Застосування методу аналізу ієрархій, який передбачає декомпозицію складної задачі на ієрархічні рівні, що включають мету, критерії та альтернативи [10].

Формування ієрархії.

Рівень 1 – мета: оцінювання ефективності організаційної структури взводу.

Рівень 2 – альтернативи: A_1 – механізований взвод ЗС України на БМП-2; A_2 – мотострілецький взвод рф на БМП-3.

Рівень 3 – критерії оцінювання: K_1 – вогнева міць; K_2 – захищеність; K_3 – маневреність; K_4 – управління та взаємодія; K_5 – вартість життєвого циклу.

Визначення вагових критеріїв. На основі експертного оцінювання встановлено вагові коефіцієнти: $K_1 = 0,3$; $K_2 = 0,2$; $K_3 = 0,2$; $K_4 = 0,2$; $K_5 = 0,1$.

Оцінювання альтернатив. Порівняння альтернатив здійснюється за шкалою Сааті [11], як інструмент методу аналізу ієрархій з подальшою нормалізацією отриманих значень.

Результати оцінювання свідчать, що:

- за критерієм вогневої міці перевагу має БМП-3;
- за критерієм управління та взаємодії – підрозділи ЗСУ;
- за критерієм вартості – БМП-2 є економічно доцільнішою.

Отримані часткові оцінки використовуються для подальшого розрахунку інтегрального показника ефективності.

Порівняльна оцінка ефективності організаційних структур взводів та інтерпретація результатів. На основі визначених критеріїв, їх вагових коефіцієнтів та нормалізованих оцінок альтернатив здійснено розрахунок інтегрального показника ефективності організаційних структур взводів.

Інтегральний показник в статті, з багатьох можливих варіантів буде визначений за формулою:

$$E = \sum_{i=1}^n y_i \cdot a_i \quad (2)$$

де: y_i – ваговий коефіцієнт i -го критерію;

a_i – нормалізована оцінка альтернативи за i -тим критерієм.

Результати оцінювання альтернатив.

A_1 – механізований взвод ЗС України (БМП-2):

Вогнева міць: $0,30 \times 0,25 = 0,075$

Захищеність: $0,20 \times 0,40 = 0,08$

Маневреність: $0,20 \times 0,45 = 0,09$

Управління: $0,20 \times 0,70 = 0,14$

Вартість: $0,10 \times 0,65 = 0,065$

Інтегральний показник: $EA_1 = 0,45$

A_2 – мотострілецький взвод рф (БМП-3):

Вогнева міць: $0,30 \times 0,75 = 0,225$

Захищеність: $0,20 \times 0,60 = 0,12$

Маневреність: $0,20 \times 0,55 = 0,11$

Управління: $0,20 \times 0,30 = 0,06$

Вартість: $0,10 \times 0,35 = 0,035$

Інтегральний показник: $EA_2 = 0,55$

Порівняльний аналіз результатів. Отримані результати свідчать, що за умов базового розподілу вагових коефіцієнтів мотострілецький взвод рф на БМП-3 має вищий інтегральний показник ефективності (0,55) порівняно з механізованим взводом Збройних Сил України на БМП-2 (0,45).

Зазначена перевага зумовлена, насамперед, вищими показниками вогневої міці та частково захищеності бойової машини піхоти БМП-3.

Разом з тим, аналіз окремих критеріїв показує, що підрозділи Збройних Сил України мають перевагу за показником управління та взаємодії, що обумовлено: наявністю бойового досвіду в умовах сучасної війни; впровадженням принципів децентралізованого управління; інтеграцією безпілотних систем та цифрових засобів управління.

З урахуванням особливостей ведення бойових дій у період 2022–2026 років автори пропонують переглянути вагомість окремих критеріїв, зокрема підвищити значущість критерію управління та взаємодії.

Вивчення бойового досвіду, його всебічний аналіз дозволяє констатувати, що створення взводних тактичних груп (бронегруп, кількістю до 4 бойових броньованих машин) при організації єдиного управління між структурними елементами Сил оборони, завчасної організації взаємодії за основними етапами бою (тактичних дій) дозволяє підвищити ефективність (як мінімум – зберегти бойові можливості) механізованого взводу, ані ж використовувати його як окрему тактичну одиницю.

У разі збільшення ваги критерію К₄ до 0,30 інтегральні показники змінюються на користь механізованого взводу Збройних Сил України.

Це свідчить про те, що в умовах сучасної війни:

- зростає роль управління, взаємодії та інформаційної переваги;
- ефективність підрозділу визначається не лише технічними характеристиками озброєння;
- вирішальне значення має здатність підрозділу діяти у складі єдиної системи управління військами.

Отримані результати дозволяють зробити узагальнюючий висновок, що ефективність організаційної структури військового підрозділу тактичної ланки є багатофакторною характеристикою, яка формується під впливом як технічних, так і організаційно-управлінських чинників.

Застосування методу аналізу ієрархій у поєднанні з воєнно-економічним аналізом забезпечує підвищення обґрунтованості управлінських рішень у системі оборонного планування.

Висновки. У статті обґрунтовано доцільність застосування програмно-проектного менеджменту як методологічної основи оборонного планування в сучасних умовах функціонування сектору безпеки і оборони України.

Встановлено, що впровадження програмно-проектного підходу, відповідно до вимог Військових стандартів, забезпечує підвищення ефективності управління процесами формування та розвитку спроможностей Збройних Сил України, а також сприяє оптимізації використання обмежених ресурсів.

У результаті дослідження використано методичний підхід до оцінювання ефективності організаційних структур військових підрозділів шляхом інтеграції воєнно-економічного аналізу та методу аналізу ієрархій. Це дозволяє здійснювати комплексне оцінювання з урахуванням як технічних, так і організаційно-управлінських чинників.

Проведена порівняльна оцінка механізованого взводу Збройних Сил України на БМП-2 та мотострілецького взводу російської федерації на БМП-3 показала, що за базових умов технічна перевага може належати більш сучасним зразкам озброєння. Водночас результати дослідження підтверджують, що в умовах повномасштабної збройної агресії вирішального значення набувають показники управління, взаємодії та адаптивності підрозділів.

Доведено, що підвищення вагомості управлінських факторів у моделі оцінювання призводить до зміни результатів на користь підрозділів, які ефективно інтегровані в єдину систему управління військами та застосовують сучасні підходи до ведення бойових дій.

Практичне значення отриманих результатів полягає у можливості їх використання під час обґрунтування рішень у системі оборонного планування, зокрема при визначенні доцільності розвитку організаційних структур, формуванні програм розвитку спроможностей та розподілі ресурсів.

Подальші дослідження доцільно спрямувати на розширення переліку критеріїв оцінювання, врахування факторів бойового досвіду та уточнення економічних показників життєвого циклу озброєння і військової техніки.

ЛІТЕРАТУРА:

1. Військовий стандарт ВСТ 01.040.010–2021(01) "Оборонне планування. Програмно-проектний менеджмент. Управління програмою / підпрограмою проєктів". Міністерство оборони України. URL: <https://mod.gov.ua/diynalist/normativno-pravova-baza/vijskovij-standart-vst-01-040-010-2021-01-oboronne-planuvannya-programno-proyektnij-menedzhment-upravlinnya-programoyu-pidprogramoyu-proyektiv>
2. Військовий стандарт ВСТ 01.040.011–2021(01) "Оборонне планування. Програмно-проектний менеджмент. Управління проєктами". МОУ. URL: <https://mod.gov.ua/diynalist/normativno-pravova-baza/vijskovij-standart-vst-01-040-011-2021-01-oboronne-planuvannya-programno-proyektnij-menedzhment-upravlinnya-proektami>

3. Щипанський П.В., Саганюк Ф.В., Мудрак Ю.М., Оборонний менеджмент: підходи до управління процесами оборонного планування. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ №1, С.52-58, 2021. URL: http://nbuv.gov.ua/UJRN/Znpcvds_2021_1_10
4. Гарькавий Є. М. Використання підходів програмно-проектного менеджменту в реалізації стратегічних комунікацій. Політичне життя, №1, 2024. URL: <https://doi.org/10.31558/2519-2949.2024.1.13>
5. Петренко А. Г. Щодо впровадження оборонного менеджменту та управління змінами в Міністерстві оборони України. Наука і оборона, №2, 2019. URL: <https://doi.org/10.33099/2618-1614-2019-7-2-03-08>
6. Гаврилюк І. Аналіз наявних підходів до оцінювання та прогнозування рівня воєнно-економічної безпеки держави: закордонний та вітчизняний досвід. The Central Research institute of the Armed Forces of Ukraine Military Science. №2, 2025 URL: <https://doi.org/10.62524/msj.2025.3.14>
7. Семененко С. Метод оцінювання ефективності виконання програми (планів) розвитку Збройних Сил України з урахуванням повноти та своєчасності їх фінансування. Збірник наукових праць Харківського національного університету Повітряних Сил. DOI: 10.30748/zhups.2017.51.10
8. Іванець, Г., Горелишев, С. Методика оцінювання ефективності комплексної системи забезпечення, підтримання та відновлення боєздатності військових підрозділів. Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, (1(23)), с. 7-18. DOI: 10.37701/dndivsovt.23.2025.01.
9. Методичні рекомендації з фінансово-економічного обґрунтування вартості повного життєвого циклу спроможностей з урахуванням принципів та стандартів НАТО, затверджені тимчасово виконуючим обов'язки Міністра оборони України 09.06.2020. URL: <https://mod.gov.ua/diynalist/normativno-pravova-baza/metodichni-rekomendaczii-z-finansovo-ekonomichnogo-obgruntuvannya-vartosti-povnogo-zhitteвого-cziklu-spromozhnostej-z-urahuvannyam-princzipiv-ta-standartiv-nato>
10. Методи розв'язання багатокритеріальних задач оптимізації. URL: <https://studfile.net/preview/7185500/page:15/>
11. Saaty T. L. Decision Making with the Analytic Hierarchy Process. International Journal of Services Sciences, Vol. 1, No. 1, 2008 URL: <chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://www.rafikulislam.com/uploads/resourses/197245512559a37aadea6d.pdf>
12. СБП 3-(01,02,04).56(57) Бойовий статут "Механізованих і танкових військ СВ Збройних Сил України" (частина II, батальйон, рота), вересень 2025 (зі змінами від 30.12.2016 №605; від 11.11.2017 №564; від 02.08.2018 №454; від 05.05.2023 №253; від 04.10.2023 №628од; від 18.09.2025 №634/нагд) Командування підготовки командування СВ ЗСУ спільно з Національною академією Сухопутних військ імені Петра Сагайдачного, 2025

REFERENCES:

1. Ministry of Defense of Ukraine. (2021). Military Standard VST 01.040.010–2021 (01). Defense Planning. Program and Project Management. Program / Subprogram of Projects Management. Kyiv. URL: <https://mod.gov.ua/diynalist/normativno-pravova-baza/vijskovij-standart-vst-01-040-010-2021-01-oboronne-planuvannya-programno-proyektnij-menedzhment-upravlinnya-programoyu-pidprogramoyu-proyektiv>
2. Ministry of Defense of Ukraine. (2021). Military Standard VST 01.040.011–2021 (01). Defense Planning. Program and Project Management. Project Management. Kyiv. URL: <https://mod.gov.ua/diynalist/normativno-pravova-baza/vijskovij-standart-vst-01-040-011-2021-01-oboronne-planuvannya-programno-proektnij-menedzhment-upravlinnya-proektami>
3. Shchypansky P.V., Saganyuk F.V., Mudrak Y.M., Defense Management: Approaches to Managing Defense Planning Processes. Collection of Scientific Papers of the Center for Military and Strategic Studies of the National University of Ukraine No. 1, pp. 52-58, 2021. URL: http://nbuv.gov.ua/UJRN/Znpcvds_2021_1_10
4. Garkavy E. M. Using program and project management approaches in the implementation of strategic communications. Political Life, No. 1, 2024. URL: <https://doi.org/10.31558/2519-2949.2024.1.13>
5. Petrenko A. G. On the implementation of defense management and change management in the Ministry of Defense of Ukraine. Science and Defense, No. 2, 2019. URL: <https://doi.org/10.33099/2618-1614-2019-7-2-03-08>

6. Gavriluk I. Analysis of existing approaches to assessing and forecasting the level of military-economic security of the state: foreign and domestic experience. The Central Research institute of the Armed Forces of Ukraine Military Science. №2, 2025 URL: <https://doi.org/10.62524/msj.2025.3.14>
7. Semenenko S. Method of assessing the effectiveness of the implementation of the program (plans) for the development of the Armed Forces of Ukraine, taking into account the completeness and timeliness of their financing. Collection of scientific works of the Kharkiv National University of the Air Force. DOI: 10.30748/zhups.2017.51.10
8. Ivanets, G., Gorelyshev, S. Methodology for assessing the effectiveness of a comprehensive system for ensuring, maintaining and restoring the combat capability of military units. Collection of scientific works of the State Research Institute for Testing and Certification of Armaments and Military Equipment, (1(23), pp. 7-18. DOI: 10.37701/dndivsovt.23.2025.01.
9. Methodological recommendations on the financial and economic justification of the cost of the full life cycle of capabilities taking into account NATO principles and standards, approved by the Acting Minister of Defense of Ukraine on 09.06.2020. URL: <https://mod.gov.ua/diyalnist/normativno-pravova-baza/metodichni-rekomendaczii-z-finansovo-ekonomichnogo-obgruntuvannya-vartosti-povnogo-zhittevogo-cziklu-spromozhnostej-z-urahuvannyam-princypiv-ta-standartiv-nato>
10. Methods for solving multi-criteria optimization problems. URL: <https://studfile.net/preview/7185500/page:15/>
11. Saaty T. L. Decision Making with the Analytic Hierarchy Process. International Journal of Service Sciences, Vol. 1, No. 1, 2008 URL: <https://www.rafikulislam.com/uploads/resourses/197245512559a37aadea6d.pdf>
12. CMP 3-(01,02,04).56(57) Combat regulations of the "Mechanized and tank troops of the Central Military District of the Armed Forces of Ukraine" (part II, battalion, company). September 2025 (as amended on 30.12.2016 No. 605; on 11.11.2017 No. 564; on 02.08.2018 No. 454; on 05.05.2023 No. 253; on 04.10.2023 No. 628od; on 18.09.2025 No. 634/nagd) Training Command of the Central Military District of the Armed Forces of Ukraine jointly with the Petro Sahaidachny National Academy of the Land Forces, 2025

Ph.D Zaitsev D., PhD Melnyk Y., Mykolaichuk O.

ELEMENTS OF PROGRAM AND PROJECT MANAGEMENT AS A BASIS FOR DEFENSE PLANNING AND ASSESSMENT OF THE EFFICIENCY OF ORGANIZATIONAL STRUCTURES OF UNITS

The application of program and project management as a basic tool for organizing defense planning in the context of modern security challenges is considered.

The regulatory and legal framework for the implementation of the program and project approach in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine is analyzed, in particular the provisions of the Military Standard VST 01.040.010–2021.

The feasibility of integrating the methods of military-economic analysis and the method of hierarchy analysis for assessing the effectiveness of organizational structures of tactical units is substantiated.

An approach to the comparative assessment of the mechanized platoon of the Armed Forces of Ukraine on the BMP-2 and the motorized rifle platoon of the Russian Federation on the BMP-3 is proposed, taking into account a set of criteria: firepower, protection, maneuverability, level of control and life cycle cost.

It has been determined that in conditions of full-scale armed aggression, the decisive factor in the effectiveness of units is not only the technical level of weapons, but also the quality of management, integration into a single system of command and control of troops, and the ability to adapt to various conditions.

The scientific novelty lies in the combination of program and project management with the tools of multi-criteria assessment of the effectiveness of military (tactical) organizational structures, which allows to increase the validity of decisions in the defense planning system.

Keywords: program and project management; defense planning; weighting coefficient, military-economic analysis, method of analysis of hierarchies, project management, efficiency, organizational structure, unit.

ДАНІ ПРО АВТОРІВ

Богданович Володимир Юрійович, доктор технічних наук, професор, Центральний науково дослідний інститут Збройних Сил України, м. Київ, Україна, ORCID: 0000-0003-0481-9454.

Гуляк Олег Вікторович кандидат юридичних наук, доцент Акціонерне товариство "Українська оборонна промисловість", м. Київ, Україна, ORCID: 0000-0002-4588-5979.

Гурковський Володимир Ігорович доктор наук з державного управління, професор Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна, ORCID: 0000-0003-2021-5204.

Дейнека Олег Володимирович, аспірант науково-навчального інституту публічного управління та державної служби Київський національний університет імені Тараса Шевченка, м. Київ, Україна, ORCID: 0009-0003 3296-8710.

Зайцев Дмитро Володимирович, кандидат військових наук, доцент, доцент кафедри, факультет післядипломної освіти Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0002-3784-5790.

Зубчик Олег Анатолійович, доктор наук з державного управління, кандидат філософських наук, доцент, професор кафедри державного управління Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 000-0001-6480-409X.

Іценко Дмитро Сергійович, начальник відділу планування наукової та науково-технічної діяльності, Центральне управління військової освіти і науки Генерального штабу Збройних Сил України, м. Київ, Україна, ORCID: 0000-0002-3545-215X.

Карпенко Андрій Олексійович, науковий співробітник науково-дослідного центру Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0001-7389-7259.

Коваль Мирослав Олександрович, доктор філософії, старший науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0002-8374-7390.

Коренець Олександр Володимирович, кандидат географічних наук, ТВО начальника науково-дослідного науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0001-6352-9591.

Кравченко Олександр Іванович, кандидат педагогічних наук, старший науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0002-7865-5870.

Линченко Максим Миколайович, кандидат філософських наук, доцент, Центральноукраїнський національний технічний університет, м. Кропивницький, Україна, ORCID: 0000-0002-4272-6147.

Лоза Віталій Миколайович, кандидат технічних наук, старший дослідник, начальник науково-дослідного відділу проблем інформаційного протидіювання науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0002-8050-3614.

Лукіянчук Анатолій Анатолійович, старший науковий співробітник науково-дослідної лабораторії супроводження інноваційних проєктів науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0002-5757-6196.

Машков Олег Альбертович доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, провідний науковий співробітник, Державна наукова установа "Інститут екологічного відновлення та розвитку України", м. Київ, Україна, ORCID: 0000-0001-9227-4647.

Мельник Ярослав Іванович, кандидат психологічних наук, начальник кафедри загальновійськової підготовки, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна ORCID: 0000-0003-3704-2856.

Миколайчук Олена Михайлівна, провідний науковий співробітник науково-дослідного відділу інформаційного протидіювання науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0001-9208-7665.

Мірошніченко Олег Вікторович, кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник науково-дослідного відділу проблем інформаційного протидіювання науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0002-3969-9758.

Пампуха Ігор Володимирович, кандидат технічних наук, доцент, заслужений винахідник України, начальник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0002-4807-3984.

Поздняк Валерій Павлович, старший науковий співробітник Харківського національного університету Повітряних Сил (ХНУПС) ім. І. Кожедуба, м. Харків, Україна, ORCID: 0000-0001-7247-9944.

Савков Павло Анатолійович, кандидат технічних наук, доцент, Корпорація "Науковий парк Київський університет імені Тараса Шевченка", м. Київ, Україна, ORCID: 0000-0002-0197-0610.

Ситник Григорій Петрович, кандидат технічних наук з державного управління, професор, заслужений діяч науки і техніки України, завідувач кафедри глобальної та національної безпеки, Навчально-науковий інститут публічного управління та державної служби Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0002 3083-5733.

Тищук Сергій Олександрович, кандидат технічних наук, доцент, професор кафедри електромагнітної боротьби, Національний університет оборони України, м. Київ, Україна, ORCID: 0000-0002-9661-5493.

Цибізов Андрій Леонідович кандидат військових наук, старший дослідник Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна ORCID: 0000-0001-6555-5005.

Шамрай Назар Миколайович, провідний науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0001-8387-3277.

Яцук Петро Петрович, кандидат технічних наук, доцент, Міжнародний Європейський Університет, Київ, Україна, кафедра інформаційних технологій, Корпорація "Науковий парк Київський університет імені Тараса Шевченка", м. Київ, Україна, ORCID: 0009-0002-7124-4849.

АЛФАВІТНИЙ ПОКАЗЧИК

Богданович В.Ю.	58	Лукіяничук А.А.	37
Гуляк О.В.	58	Машков О.А.	26
Гурковський В.І.	64	Мельник Я.І.	115
Дейнека О.	104	Миколайчук О.М.	115
Зайцев Д.В.	115	Мірошніченко О.В.	18
Зубчик О.А.	90	Пампуха І.В.	7
Іценко Д.С.	18	Поздняк В.П.	7
Карпенко А.О.	47	Савков П.А.	7
Коваль М.О.	47	Ситник Г.П.	74
Коренець О.В.	37	Тищук С.О.	7
Кравченко О.І.	47	Цибісов А.Л.	58
Линченко М.М.	90	Шамрай Н.М.	47
Лоза В.М.	18	Яцук П.П.	7

РЕДАКЦІЙНА ПОЛІТИКА ТА ЕТИЧНІ НОРМИ ПРИНЦИПИ ФОРМУВАННЯ ТА ДОСТУП ДО ЗМІСТУ "ЗБІРНИКА ВІКНУ"

Редакційна політика "Збірника ВІКНУ" заснована на принципах об'єктивності та неупередженості під час відбору статей для публікації; високих вимог до якості наукових досліджень; обов'язковості та конфіденційності рецензування статей; додержання колегіальності у відборі до публікації статей; доступності та оперативності у спілкуванні з авторами; суворого дотримання авторських і суміжних прав. Запобігання протизаконним публікаціям є відповідальністю кожного автора, редактора, рецензента, видавця.

До друку приймаються оригінальні рукописи, які не були опубліковані раніше та не відправлялись до інших редакцій, які повністю відповідають вимогам стосовно оформлення та порядку подання статей.

У "Збірнику ВІКНУ" сформовані наступні рубрики: військова техніка і технології подвійного призначення, інформаційні технології, загальні питання.

Редакція підтримує політику відкритого доступу та принципи вільного поширення наукової інформації. Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, у бібліотеці Військового інституту та інших бібліотеках України. Електронна версія розміщена на сайті інституту, на сайтах наведених бібліотек та на сайтах "Збірника ВІКНУ": <http://miljournals.knu.ua/index.php/zbirnuk>; <http://mil.univ.kiev.ua/page/lib/31>

ЕТИКА ПУБЛІКАЦІЙ

Редакційна колегія журналу вимагає від авторів наслідувати формальним та етичним правилам підготовки і публікації наукових робіт, які вони подають до редакції журналу. Ці норми зумовлено стандартами якості наукових статей, прийнятими у світовому науковому співтоваристві, зокрема публікаційними принципами Publishing Ethics Resource Kit (PERK), рекомендаціями Elsevier, Комітету з етики публікацій (Committee on Publication Ethics, COPE), етичним кодексом вченого України, а також досвідом роботи іноземних та українських професіональних спільнот, наукових організацій, редколегій та редакцій видань.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ РЕДАКЦІЙНОЇ КОЛЕГІЇ ЖУРНАЛУ

Редакційна колегія у своїй діяльності

- керується принципами неупередженості, наукової етики рецензування, захисту інтелектуальної власності;
- несе відповідальність за рівень наукового наповнення журналу;
- виступає проти фальсифікації, плагіату, направлення автором одного рукопису до кількох журналів, багаторазового копіювання тексту статті в різних місцях, введення громадськості в оману щодо реального внеску кожного автора в опубліковану наукову роботу;
- залишає за собою право направити рукопис на розгляд сторонньому рецензенту, в тому числі ретельний відбір через "сліпе" рецензування, відхилити статтю або повернути її на доопрацювання;
- може відхилити рукопис, якщо вважає, що він не відповідає профілю журналу, чи не відповідає етиці та правилам оформлення;
- має право вилучити вже опубліковану статтю в разі виявлення порушення будь-чиїх прав або загальноприйнятих норм наукової етики, про цей факт вилучення статті редакція повідомляє як автору статті, так і організації, де було виконано дослідження та повідомляє про це у наступному номері.

Співробітники редакції не надають іншим особам інформації, пов'язаної із змістом рукописів, що перебувають на розгляді, крім осіб, які беруть участь у її фаховій оцінці.

Згідно з міжнародним законодавством щодо додержання авторського права на електронні інформаційні ресурси, матеріали сайту, електронного журналу або проєкту не

можуть бути відтворені повністю або частково у будь-якій формі (електронній чи друкованій) без попередньої письмової згоди редакції журналу. Під час використання опублікованих матеріалів у контексті інших документів обов'язково необхідними є посилання на першоджерело.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ АВТОРА

Автор:

- несе відповідальність за новизну і достовірність наведених у статтях результатів, тактико-технічних та економічних показників, коректність висловлювань, а також за те, що в матеріалах не міститься інформація з обмеженим доступом;

- повинен цитувати ті публікації, які мали визначальний вплив на суть викладеного у статті, а також ті, які можуть швидко ознайомити читача з більш ранніми працями, важливими для розуміння цього дослідження, необхідно також належним чином вказувати джерела принципово важливих матеріалів, використаних у цій роботі, якщо вони не були отримані самим автором;- забезпечує недопустимість плагіату та подання до публікації раніше надрукованих матеріалів, у випадку виявлення зазначених фактів відповідальність несе автор поданих матеріалів.

Співавторами статті мають бути всі особи, що зробили вагомий науковий внесок у подану роботу і поділяють відповідальність за отримані результати. Автор, який подає рукопис до публікації, відповідає за те, щоб до списку співавторів були включені тільки ті особи, які відповідають критерію авторства, та бере на себе відповідальність за згоду інших авторів статті на її публікацію в журналі.

УВАГА!

Для авторів статей дещо доопрацьовані вимоги щодо особистих даних.

Ці дані подаються українською та англійською мовами в такій послідовності: Прізвище

Ім'я_по - батькові. Науковий ступінь та вчене звання. Місце роботи та посада

ORCID 0000-0001-3215-4400

SCOPUS ID 57193059215 (за наявності) Індекс DBLP 10 (за наявності)

e-mail: __ моб. телефон

Надсилати скановані рисунки, формули та таблиці не допускається.

Вся стаття оформлюється одним шрифтом **Times New Roman**, вказаними нижче розмірами, зверніть увагу на формули, таблиці та рисунки.

РЕДАКЦІЙНА КОЛЕГІЯ "ЗБІРНИКА ВІКНУ" ЗДІЙСНЮЄ НЕЗАЛЕЖНЕ ("СЛІПЕ" ЕКСПЕРТНЕ РЕЦЕНЗУВАННЯ НАДАНИХ ДО ДРУКУ РУКОПИСІВ ТА ПЕРЕВІРКУ ЇХ НА ПЛАГІАТ. РЕЦЕНЗУВАННЯ ЗДІЙСНЮЄТЬСЯ ЗА АНОНІМНОЮ ФОРМОЮ ЯК ДЛЯ АВТОРІВ, ТАК І ДЛЯ РЕЦЕНЗЕНТІВ.

**ЯКІСНІ ПОКАЗНИКИ ЧЛЕНІВ РЕДАКЦІЙНОЇ КОМІСІЇ ПРАЦЬ ВІСНУ
НА 18.12.25 РОКУ**

			Scopus	Index Hirsha	DBLP
Ленков С.В.	д.т.н., проф. ВІСНУ	Lienkov Serhii	25 (21)	5 (4)	7 (6)
Анісімов А.В.	д. ф-м н., проф., член-кор. НАНУ, КНУ	Anisimov Anatoliy	121 (114)	9	40 (38)
Барабаш О.В.	д.т.н., проф. НТУУ "КПІ"	Barabash Oleg	60 (54)	20 (18)	6(5)
Гунченко Ю.О.	д.т.н., проф.ОНУ	Gunchenko Yurii	25 (23)	6	5
Жиров Г.Б.	к.т.н. с.н.с., КНУ	Zhyrov Gennadiy	14 (12)	3	3 (1)
Заславський В.А.	д.т.н., проф., КНУ	Zaslavsky Volodymyr	33 (25)	3	11 (10)
Карпінський М.П.	д.т.н., проф., УНТ Краків (Польща)	Karpinski Mikolaj	122 (111)	12 (11)	61 (51)
Лепіх Я.І.	д. ф-м н., проф.,ОНУ	Lepikh Yaroslav	59 (57)	4	0
Петров О.С.	д.т.н., проф., УНТ Краків (Польща)	Petrov Oleksandr	19	4	1
Погорілий С.Д.	д.т.н., проф., КНУ	Pogorilyy S.D.	30 (29)	8	11 (7)
Толок І.В.	к.пед. наук, доц., НУЦЗС	Tolok Igor	13 (9)	3	2
Хайрова Н.Ф.	д.т.н., проф., Umea, U(Sweden)	Khairova Nina	46 (39)	7	40 (34)
Хлапонін Ю.І.	д.т.н., проф., КНУБА	Khlaponin Yurii	38 (32)	5 (4)	21 (18)
Шаронова Н.В.	д.т.н., проф., НТУ "ХПІ"	Sharonova N.V.	29 (24)	5	31 (25)

**ПОРЯДОК ПОДАННЯ І ОФОРМЛЕННЯ СТАТЕЙ ДО "ЗБІРНИКА НАУКОВИХ
ПРАЦЬ ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА"**

До друку приймаються оригінальні рукописи, які не були опубліковані раніше, не були відправлені до інших редакцій та повністю відповідають вимогам щодо оформлення та порядку подання статей.

Загальні вимоги до технічного оформлення статей:

Обсяг рукопису - рекомендується **не менше 12 повних аркушів** українською або англійською мовами.

Формат аркуша - **A4 (210 x 297 мм).**

Розмір полів: верхнє, нижнє, праве, ліве - **2 см.**

Шрифт тексту - **Times New Roman №12**, через міжрядковий інтервал - **1,0**.

Абзац має становити **10 мм.**

Стаття повинна мати такі необхідні елементи:

УДК;

назва статті, яка лаконічно відображає зміст та новизну статті;

анотація та ключові слова;

вступ та постановка задачі чи проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано **розв'язання цієї проблеми** і на які спирається автор, визначення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття, формулювання мети статті;

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів, практичних рішень та експериментів;

висновки з цього дослідження і перспективи подальшого розвитку в цьому напрямку,

список літератури,

References,

дані про авторів двома мовами.

Анотація до статті виконується українською та англійською мовами загальний обсяг кожної не менш ніж **1800** знаків, включаючи ключові слова.

Вона повинна містити коротке повторення структури статті, що включає вступ, цілі і завдання, методи, результати, висновки.

Анотацію друкують курсивом, шрифт Times New Roman, №11. Після анотації розміщуються **ключові слова** (5–7 термінів).

Список літератури (References) повинен включати не менш 12 джерел, з яких 50 % видані за останні 10 років. При цьому не менш 25 % джерел повинно відноситися до іноземної періодики. Самоцититування авторів у списку літератури повинно бути, як правило, не більш за 25 %.

Якщо основною мовою статті є українська, то оформляються два списки літератури: перший (список літератури мовою оригіналу джерела) – згідно з наказом МОН від 12.01.2017 № 40 та відповідно до ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання: загальні положення та правила складання";

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН від 12.01.2017 № 40 та міжнародного Гарвардського стилю BSI (British Standards Institution).

На адресу редколегії (03022, м. Київ, вул. Ю. Здановської, 81, тел.: +38 (044) 521 - 33 - 82) мають бути надіслані наступні матеріали:

експертний висновок про можливість відкритого публікування, завірений печаткою, сканкопія надсилається на e-mail: lenkov_s@ukr.net

Вимоги до оформлення References

References потрібно приводити окремим блоком, повторюючи послідовність попередньо наведеного Списку літератури. Джерела при цьому оформлюються за такими основними правилами (Harvard style оформлення BSI: British Standards Institution):

– запис завжди починається з прізвища автора, потім кома, ініціали (між ініціалами пропуски не ставляться), за якими в дужках вказується дата видання; два автори відокремлюються "and" без коми; кілька авторів розділяються комами, але останнє прізвище повинно бути відокремлене "and" без коми;

– витяги з публікацій, тобто назви статей журналів, глав в книгах наводяться в "лапках";

– назва журналу або книги завжди виділяється курсивом;

– ім'я видавця вказується перед місцем видання;

– коми використовують для поділу елементів запису;

– для джерел українською або російською мовами, що наводяться у References, назви статей журналів, глави з книг наводяться латиницею (транслітерацією) в "лапках" та перекладаються англійською мовою в квадратних дужках. Онлайн-конвертер з української мови для транслітерації: <http://translit.kh.ua/?passport>.

Приклади оформлення References за стилем Harvard British Standards Institution

Книга (ДСТУ 8302:2015)

Інформаційно-психологічна боротьба у воєнній сфері: монографія / Г.В. Пєвцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Х.: Вид. Рожко С.Г., 2017. 276 с.

Книга (Harvard style BSI)

Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017), "Informatsiino-psykholohichna borotba u voiennii sferi: monohrafiia" [The information and psychological struggle in the military sphere], Rozhko S.H., Kharkiv, 276 p.

Стаття із періодичного видання (ДСТУ 8302:2015)

Карпенко, Д.В. Стан та перспективи розвитку зенітного ракетного озброєння Повітряних Сил Збройних Сил України / Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2(27). С. 75–78.

Стаття із періодичного видання (Harvard style BSI)

Karpenko, D.V. (2017), "Stan ta perspektyvy rozvytku zenitnoho raketnoho ozbroiennia Povitrianykh Syl Zbroinykh Syl Ukrainy" [The state and perspectives of the development of anti-aircraft missile armaments in the Air Force of Ukraine], Science and Technology of the Air Force of Ukraine, No. 2(27), pp. 75–78.

Дисертація (ДСТУ 8302:2015)

Белозеров, І.В. Религиозная политика: дис. ... канд. ист. наук: 07.00.02; захищена 22.01.02; утв. 15.07.02 / Белозеров Иван Валентинович. К., 2002. 215 с.

Дисертація (Harvard style BSI)

Belozerov, I.V. (2002), "Relyhyoznaia polityka: dissertation" [The religious policy: dissertation], Kiev, 215 p.

Джерела електронного ресурсу віддаленого доступу (ДСТУ 8302:2015)

Романов В. К вопросу о путях достижения национальной безопасности в условиях глобализации: проблемы теории и практики в контексте внешней политики России и Польши [Електронний ресурс] Безопасность и оборона, 2016. № 1(2), С. 7–15. Режим доступа до журн.: http://www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf.

Джерела електронного ресурсу віддаленого доступу (Harvard style BSI)

Romanov, V. (2016), "K voprosu o putyakh dostizheniya natsionalnoy bezopasnosti v usloviyakh globalizatsii: problemy teorii i praktiki v kontekste vneshney politiki Rossii i Polshi" [To the question about the ways to achieve national security in the context of globalization: the problems of theory and practice in the context of the foreign policy of Russia and Poland], Security and Defence Journal, No. 1(2), pp. 7–15, www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf (accessed 12 July 2017). (примітка: при наведенні URL "http: //" має бути виключено).

Більш детальну інформацію щодо оформлення бібліографічних посилань за стилем Harvard British Standards Institution можна знайти на сайті *Національної бібліотеки України імені В.І. Вернадського* та онлайн генератора посилань *Cite This For Me*.

Редакційна колегія: e-mail: lenkov_s@ukr.net

Шрифт

СХЕМА ОФОРМЛЕННЯ СТАТЕЙ У "ЗБІРНИКУ НАУКОВИХ ПРАЦЬ ВІКНУ"

УДК

науковий ступінь, вчене звання
ініціали та прізвище автора (співавторів)
місце роботи автора (співавторів)

12 пт

УДК 32.973.202:07.681

д.т.н., проф. Степанов С.В. (ВІКНУ)
к.т.н., с.н.с. Українець О.В. (ВІКНУ)
Саленко В.Д. (ВІКНУ)

12 пт
жирний

КЕРУВАННЯ ЕЛЕКТРОННИМИ ПРИСТРОЯМИ ЗА ДОПОМОГОЮ ЖЕСТІВ

Анотація до статті виконується українською та англійською мовами (загальний обсяг кожної не менш, ніж **1800** знаків, включаючи ключові слова).

11 пт
курсив,
жирний

Для керування електронними пристроями, для сучасного користувача важливими ітеріями є такі, як: зручність та простота керування. Для того, щоб надати истувачеві такі можливості та зручності в використанні, є досить доцільною робка системи, яка б надавала такі можливості. Керування системою, яка працює на юві жестів, є надзвичайно перспективним, та може суттєво полегшити истувачеві роботу з нею, тому що жести, які потрібні для керування системою, жуть бути інтуїтивно зрозумілими користувачеві, порівняно з іншими системами, які ищують за допомогою комбінацій клавіш.

Для вирішення задач керування за допомогою жестів, пропонується програмно-іратний комплекс, який побудований на основі різних модулів, кожен з яких в свою чергу онує відповідну роль в системі, наприклад, знаходить точку інтересу з множини чи аховує глибину сцени. Також у системі є ядро, яке відповідає за аналіз модифікаторів та стів. На основі даних модулів стає можливо створити систему, яка б працювала основі жестів. Але для створення цієї системи, потрібно вирішити певні задачі, кі як: сегментація, скелетизація, спостереження. Кожна з яких містить в собі повідні математичні моделі та визначення. Запропонований програмно-апаратний иплекс для керування природніми жестами. Суть програмно-апаратного комплексу иягає в тому, щоб забезпечити користувача таким інтерфейсом, щоб він виконував юту знаходячись частково віддалено від робочого місця, чи маніпулював трументами на відстані, тобто за допомогою жестів. Використання запропонованого іграмно- апаратного комплексу дозволить покращити показники стерильності в іраційних, підвищити технічну безпеку під час виконання безпосередньої роботи истувача з приладами.

Ключові слова: штучний інтелект, контролери, модулі, жести, глибина сцени, чка інтересу, аналіз модифікаторів, аналіз жестів, сегментація, скелетизація, истерезження.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ СТАТТІ

12 pt **НЕОБХІДНІ ЕЛЕМЕНТИ СТАТТІ:** вступ та постановка проблеми (задачі) у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями; аналіз останніх досліджень і публікацій, в яких започатковано розв'язання цієї проблеми і на що спирається автор, виділення невирішених раніше частин загальної проблеми, яким присвячується ця стаття, формулювання цілей статті (постановка завдання), виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів; їх практичного значення та результатів експеримента чи впровадження; висновки з дослідження і перспективи подальших досліджень у цьому напрямку. **Література. References.**

УВАГА! Таблиці і рисунки друкують після посилань. Якщо у статті кілька таблиць чи рисунків - їх нумерують. Заголовки таблиць і рисунків необхідно розміщувати по центру, а нумерацію таблиць праворуч від таблиці (стиль **normal**, шрифт - **Times New Roman № 12**).

Рисунки повинні бути виконані за допомогою редактора Word, згруповані і являти собою один графічний об'єкт. Формули та позначення по тексту обов'язково набирати за допомогою Equation Editor - редактора формул Word, а не у текстовому режимі. У редакторі формул мають бути встановлені такі параметри - розміри: загальний.

12 pt. великі індекси – **10 pt**, малі індекси – **7 pt**, великі символи – **14 pt**, малі символи.

10 pt: стиль: текст, функції, змінні, матриці-вектори, числа – шрифт Times New Roman, для решти стилів – шрифт Symbol, при цьому: строк. грецькі – прямі. Великі за розміром вирази та рівняння необхідно записувати у кілька рядків.

ЛІТЕРАТУРА

Перший (список літератури на мові оригіналу джерела) – згідно з наказом МОН № 40 від 12.01.2017 та відповідно до ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання: загальні положення та правила складання";

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН № 40 від 12.01.2017 та міжнародного Гарвардського стилю BSI (British Standards Institution).

ЛІТЕРАТУРА:

11 pt

ЗРАЗОК

1. Ленков С.В., Толлок І.В., Цицарєв В.М., Ленков Є.С. Моделювання процесів витрачання та поповнення ресурсу угруповання технічних об'єктів. Системи озброєння і військова техніка. Харків. 2018. Вип. 1(53). С. 155 – 162.

2. Жиров Г.Б., Ленков Є.С., Цицарєв В.М., Проценко Я.М. Моделювання процесу відмов об'єктів, що відновлюються з ієрархічною конструктивною структурою. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ. 2017. Вип. 55. С. 30-39.

REFERENCES:

11 pt

ЗРАЗОК

1. Lienkov, S.V., Tolok, I.V., Tsytsarev, V.N. and Lenkov, Ye.S. (2018), "Modeliuvannia protsesiv vytrachannia ta popovnennia resursu uhrupuvannia tekhnichnykh obiektiv" [Modeling of processes of expenditure and resource replenishment grouping of technical objects], Systems of Arms and Military Equipment, No. 1(53), pp. 155-162.

2. Zhyrov, G.B., Lenkov, Je.S., Cycarjev, V.M. and Procenko, Ja.M. (2017), "Modeljuvannja procesu vidmov ob'ektiv, shho vidnovljujut'sja z ijerarhichnoju konstruktyvnoju strukturoju" [Simulation of the process of failure of objects that are restored with a hierarchical constructive structure], Zbirnyk naukovykh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, No. 55, pp. 30-39

CONTROL ELECTRONIC DEVICES USING GESTURES

For management of electronic devices, for today's user important criteria are: convenience and ease of management. In order to provide the user with such opportunities and usability to use, it is quite reasonable to develop a system that would provide such opportunities. Managing a gesture-based system is extremely promising, but can greatly facilitate the user to work with it, because the gestures that are needed to manage the system can be intuitive to the user, compared to other systems that operate using keyboard shortcuts. To solve the problems of managing using gestures, a software-hardware complex is proposed that is based on different modules, each of which in turn plays an appropriate role in the system, for example, finds a point of interest from a plurality or calculates the depth of a scene. Also, the system has a kernel that is responsible for analyzing modifiers and gestures. Based on the data of the modules it becomes possible to create a system that would work on the basis of gestures. But for the creation of this system, it is necessary to solve certain problems, such as: segmentation, skeletalization, observation. Each of them contains the corresponding mathematical models and definitions. Proposed hardware and software complex for management of natural gestures. The essence of the software and hardware complex is to provide the user with such an interface that he was performing work while being partially remote from the workplace, or manipulating tools at a distance, that is, using gestures. The use of the proposed software-hardware complex will improve the sterility parameters in the operating system, increase the technical safety during the direct work of the user with the devices.

Keywords: artificial intelligence, controllers, modules, gestures, depth of the scene, point of interest, analysis of modifiers, gesture analysis, segmentation, skeletonization, observation.

Дані про авторів див. стор. 122

ДЛЯ НОТАТОК

Наукове видання



ЗБІРНИК НАУКОВИХ ПРАЦЬ

**Військового інституту
Київського національного університету імені Тараса Шевченка**

№ 89

Усі матеріали надруковані в авторській редакції

Підписано до друку 18.12.2025 р.

Авт. друк. арк. 8,00. Формат 60х90/8 Безкоштовно. Замовлення № 64-25.

Надруковано у навчальному тренувальному комплексі ВІКНУ
Київ, вул. Ю. Здановської, 81

тел. (044) 521-32-89

