ВОЄННА СТРАТЕГІЯ MILITARY STRATEGY and Technology та технології

№ 2(2)/2025

UKRAÍNE

Громадська організація
"Центр воєнної стратегії і технологій"

ВОЄННА СТРАТЕГІЯ І ТЕХНОЛОГІЇ

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

№ 2(2)/2025

ISSN (online): 3083-6476

Науково-практичний журнал "Military strategy and technology" № 2(2) / 2025

УДК 355.4(082)

DOI: 10.63978/3083-6476.2025.2.2

ISSN (online): 3083-6476

Засновник і видавець: Громадська організація "Центр воєнної стратегії і технологій"

Рішенням Національної ради України з питань телебачення і радіомовлення від 10.04.2025 № 804 зареєстрований суб'єктом у сфері онлайн-медіа, ідентифікатор медіа R40-05944.

Видається з травня 2025 року, чотири рази на рік.

Журнал відображає новітні знання та результати фундаментальних, пошукових та прикладних наукових досліджень з проблематики розвитку, застосування та забезпечення національної безпеки, історії війн та інформаційних систем і технологій. У галузі військових та оборонних технологій, озброєння і військової техніки та безпеки журнал відображає прогрес у дослідженнях і розробках, досвід проведення військових місій та операцій із врегулювання кризових ситуацій та підтримує впровадження новітніх знань у оборонну промисловість та військову практику.

Журнал призначений для фахівців з державного, військового управління, воєнної стратегії, воєнного мистецтва, історії війн та технологій, наукових працівників, викладачів, докторантів, ад'юнктів, аспірантів.

Науковий профіль видання:

К3 – Національна безпека (за окремими сферами забезпечення і видами діяльності);
F6 – Інформаційні системи і технології;
B9 – Історія та археологія

Адреса:
вул. Саксаганського, буд. 41,
м. Київ, 01033, Україна

Телефон:
+38(093) 407-02-08
+38(067) 426-11-05

E-mail редколегії:
technical.sciences2025@gmail.com

Інформаційний сайт видання:
https://journals.uran.ua/milstratech

Усі статті, що публікуються в журналі, проходять обов'язкове рецензування, яке здійснюється за анонімною формою як для авторів, так і для рецензентів (подвійне сліпе рецензування).

За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор.

КООРДИНАЦІЙНА РАДА

Голова Координаційної ради:

Залужний Валерій Федорович, доктор філософії

Заступник голови Координаційної ради:

Шаптала Сергій Олександрович

Члени Координаційної ради:

Додонов Олександр Георгійович, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України

Забродський Михайло Віталійович

Кириленко Олександр Миколайович

Коваль Володимир Валерійович, кандидат військових наук, старший науковий співробітник, лауреат Національної премії України імені Бориса Патона

Кучеренко Віктор Віталійович

Мойсюк Євген Георгійович

Пєвцов Геннадій Володимирович, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України

ОСНОВНІ ТЕМАТИЧНІ НАПРЯМИ ЖУРНАЛУ:

Національна безпека

- національна і глобальна безпека;
- теоретичні аспекти та методологічні проблеми забезпечення національної безпеки;
- методи та механізми забезпечення національної безпеки;
- технології та інструменти забезпечення національної безпеки;
- експертно-аналітичні розробки та дослідження

Інформаційні системи і технології

- кібербезпека в силах безпеки і оборони;
- розробка та інтеграція інформаційних систем для військових потреб;
- захист інформаційних систем від кібератак;
- моделювання бойових ситуацій за допомогою ІТ;
- використання штучного інтелекту (ШІ)

Військова історія

- розвиток методології воєнно-історичної науки;
- технічні досягнення минулого;
- вивчення історії війн, стратегії, воєнного мистецтва, техніки, окремих воєнних кампаній та операцій;
- дослідження досвіду будівництва, бойової, організаційної і мобілізаційної підготовки сил безпеки і оборони;
- історичний досвід застосування сил безпеки і оборони

Non-Governmental Organization
"Center for Military Strategy and Technologies"

MILITARY STRATEGY AND TECHNOLOGY

SCIENTIFIC AND PRACTICAL JOURNAL

№ 2(2)/2025

ISSN (online): 3083-6476

Scientific and practical journal "Military strategy and technology" № 2(2) / 2025

UDC 355.4(082)

DOI: 10.63978/3083-6476.2025.2.2

ISSN (online): 3083-6476

Founder and publisher:
Non-Governmental organization "Center for Military Strategy and Technologies"

By the Decision of the National Council of Ukraine on Television and Radio Broadcasting dated 10.04.2025 № 804 registered as an entity in the field of online media, media identifier R40-05944

Founded in May 2025, 4 times a year.

The journal reflects the latest knowledge and results of fundamental, exploratory and applied scientific research on the issues of development, application and ensuring national security, history of wars and information systems and technologies. In the field of military and defense technologies, weapons and military equipment and security, the journal reflects progress in research and development, experience in conducting military missions and operations to resolve crisis situations and supports the introduction of the latest knowledge into the defense industry and military practice.

The collection is intended for specialists in state, military management, military strategy, military art, history of wars and technologies, scientists, teachers, doctoral students, associate professors, postgraduate students.

Scientific profile of the publication:

K3 – National Security (by individual areas of support and types of activities);
F6 – Information Systems and Technologies;
B9 – History and Archaeology

Address:
41 Saksahanskoho St.,
Kyiv city, 01033, Ukraine

Phone:
+38(093) 407-02-08
+38(067) 426-11-05

Editorial Board E-mail:
technical.sciences2025@gmail.com

Information website of the publication:
https://journals.uran.ua/milstratech

All articles published in the journal undergo mandatory peer review, which is carried out anonymously for both authors and reviewers (double-blind peer review).

The author is responsible for the reliability of the facts, quotes and other information presented.

COORDINATION COUNCIL

Chairman of the Coordination Council:

Valeriy Zaluzhny, Philosophy Doctor in Law

Deputy Chairman of the Coordination Council:

Serhiy Shaptala

Members of the Coordination Council:

Oleksandr Dodonov, Doctor in Technical Sciences, Professor, Honored Scientist and Technologist of Ukraine, Winner of the State Prize of Ukraine

Mykhailo Zabrodsky

Oleksandr Kyrylenko

Volodymyr Koval, Philosophy Doctor in Military Sciences, Senior Researcher, Winner of the National Prize of Ukraine named after Borys Paton

Viktor Kucherenko

Yevhen Moysiuk

Gennady Pevtsov, Doctor in Technical Sciences, Professor, Honored Scientist and Technologist of Ukraine, Winner of the State Prize of Ukraine

MAIN THEMATIC AREAS OF THE JOURNAL:

National Security

- national and global security;
- theoretical aspects and methodological problems of ensuring national security;
- methods and mechanisms of ensuring national security;
- technologies and tools of ensuring national security;
- expert and analytical developments and research

Information systems and technologies

- cybersecurity in security and defense forces;
- development and integration of information systems for military needs;
- protection of information systems from cyberattacks;
- modeling of combat situations using IT;
- use of artificial intelligence (AI)

Military history

- military-historical science's methodology development;
- technical achievements of the past;
- study of the wars' history, strategy, military art, technology, individual military campaigns and operations;
- the construction, combat, organizational and mobilization training of security and defense forces experience researchf;
- historical experience of the use of security and defense forces

EDITORIAL BOARD

ЗМІСТ

НАЦІОНАЛЬНА БЕЗПЕКА

ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ

ВІЙСЬКОВА ІСТОРІЯ

НАЦІОНАЛЬНА БЕЗПЕКА

УДК 327.5:007 DOI: 10.63978/3083-6476.2025.2.2.01

Залужний Валерій Федорович
доктор філософії
Надзвичайний та Повноважний Посол України в Сполученому Королівстві Великої Британії і Північної Ірландії
ORCID: 0000-0002-1947-501X

Лисецький Юрій Михайлович
доктор технічних наук, доцент
професор кафедри
Воєнна академія імені Євгенія Березняка
Київ, Україна
e-mail: Yurii.Lysetskyi@snt.ua
ORCID: 0000-0002-5080-1856

НАЦІОНАЛЬНА БЕЗПЕКА ЯК ВІДКРИТА ДИНАМІЧНА СОЦІАЛЬНА СИСТЕМА

Анотація. *Виокремлено та розглянуто три основні теоретичні підходи в розумінні сутності національної безпеки. Наведено складові системи національної безпеки. Досліджено систему національної безпеки з точки зору системного підходу в процесі взаємодії особи, суспільства, органів державної влади та місцевого самоврядування щодо забезпечення національної безпеки з урахуванням взаємозв'язків між ними та середовища їхнього існування як відкритої, динамічної, соціальної системи, функціонування якої спрямоване на захист національних інтересів держави.*

Ключові слова: *національна безпека, система національної безпеки, соціальна система, відкрита система, динамічна система.*

Valeriy Zaluzhnyi
Philosophy Doctor in Law
Extraordinary and Plenipotentiary Ambassador of Ukraine to the United Kingdom of Great Britain and Northern Ireland
ORCID: 0000-0002-1947-501X

Yurii Lysetsyi
Doctor of Engineering Sciences, Associate Professor
Professor of the Department
Yevhenii Bereznyak Military Academy
Kyiv, Ukraine
e-mail: Yurii.Lysetskyi@snt.ua
ORCID: 0000-0002-5080-1856

NATIONAL SECURITY AS AN OPEN AND DYNAMIC SOCIAL SYSTEM

Abstract. *National security is a quantitative and qualitative characteristic of the development of a social system, i.e. it is not only an assessment of a certain security of this system against potential and real threats. It reflects the results of the impact of development trends and conditions of life of the society, its institutions, which ensure the preservation of qualitative certainty of the social system and free functioning that corresponds to its nature. Today, there is a wide variety of definitions of national security, and their authors have their own opinions and approaches to the interpretation of this concept.*

The components of the national security system (NSS) are: subjects of national security; objects of national security; a set of government instruments that can be used to maintain an adequate level of protection of national interests; an array of current national legislation that defines the priorities of the state policy of national security; a set of external and internal factors of national security. Such components of the NSS as a set of subjects and objects of ensuring national security, a set of instruments of power, sources and subjects that pose threats to national interests are to a greater extent structural, while such components as the body of legislation and national security factors that determine the conditions and tasks of the NSS are functional. Some components of the NSS are relatively static, while others are more dynamic in terms of changes in space and time. From the point of view of a systemic approach in the process of interaction between an individual, society, state authorities and local self-government bodies in ensuring national security, taking into account the interrelationships between them and their environment, the NSC can be considered as an open, dynamic, social system, the functioning of which is aimed at protecting the national interests of the state.

Thus, national security is a quantitative and qualitative characteristic of the development of a social system, i.e. it is not only an assessment of a certain degree of protection of this system from potential and real threats. It reflects the results of the impact of development trends and conditions of life of the society, its institutions, which ensure the preservation of qualitative certainty of the social system and free functioning that corresponds to its nature. Thus, the dynamics of the impact of external and internal factors on national security, which simultaneously affect international security, necessitates constant reorganization, creation and elimination of certain components of the system, including those that are simultaneously integrated into the NSS, as well as into departmental, regional and international security systems.

Keywords: *national security, national security system, social system, open system, dynamic system.*

Вступ

Постановка проблеми. В сучасних умовах збройної агресії рф проти України та продовження реалізації росією стратегії гібридної війни в нових формах необхідно суттєво змінювати систему національної безпеки нашої держави [1]. У цьому контексті особливої уваги потребують не тільки військові ризики національної безпеки нашої держави, а й ризики політичні [2].

Україна на собі відчула достовірність тези про те, що воєнно-політична обстановка відіграє найважливішу роль у системі національної безпеки і є одним з основних факторів забезпечення стабільності в державі. Доведеним фактом є досить активна поведінка агресора, який, у свою чергу, не економить ресурсів як на ведення бойових дій, так і на створення сприятливого середовища для продовження гібридної війни на території нашої держави. З огляду на це, необхідність трансформації та удосконалення системи національної безпеки є дуже актуальною та необхідною умовою для протистояння агресії проти нашої держави.

Аналіз останніх досліджень і публікацій. Національній безпеці присвячені наукові праці як зарубіжних, так і вітчизняних дослідників [3-11], однак у сучасних умовах збройної агресії рф проти України та продовження росією реалізації гібридної війни в нових формах питання трансформації та удосконалення системи національної безпеки для підвищення її ефективності залишаються недостатньо дослідженими.

Мета статті – дослідити національну безпеку як відкриту динамічну соціальну систему, функціонування якої спрямоване на захист національних інтересів держави.

Виклад основного матеріалу

Поняття “національна безпека” вживається стосовно широкого кола соціальних систем для характеристики їхнього захисту від різних негативних впливів природного і соціального характеру. Це поняття характеризує ступінь захищеності життєво важливих інтересів, прав і свобод особи, суспільства та держави від зовнішніх і внутрішніх загроз або ступінь відсутності загроз правам та свободам людини, базовим інтересам і цінностям суспільства та держави. Її можна розглядати як специфічну властивість соціальних систем, комплексний критерій оцінки їхньої якості та ефективності [12].

Національна безпека є кількісно-якісною характеристикою розвитку соціальної системи, тобто не лише оцінкою певної захищеності цієї системи від потенційних і реальних загроз. Вона відображає результати впливу тенденцій розвитку та умов життєдіяльності соціуму і його інститутів, за яких забезпечується збереження якісної визначеності соціальної системи та її вільне функціонування, що відповідає її природі.

На сьогодні існує велике розмаїття визначень національної безпеки, і їхні автори мають власні думки й підходи щодо трактування цього поняття.

Глазов О. В. зазначає, що національна безпека – це захищеність життєво важливих інтересів особистості, суспільства і держави в різних сферах життєдіяльності від зовнішніх та внутрішніх загроз, що забезпечує стійкий розвиток країни [3].

Ліпкан В. А. тлумачить її з іншого ракурсу – як сукупність офіційно прийнятих поглядів на цілі та державну стратегію в частині забезпечення безпеки особистості, суспільства та держави від зовнішніх і внутрішніх загроз політичного, економічного, соціального, військового, техногенного, екологічного, інформаційного та іншого характеру з урахуванням наявних ресурсів і можливостей [4].

Національну безпеку також розуміють як здатність нації задовольняти потреби, необхідні для її самозбереження, самовідтворення і самовдосконалення, з мінімальним ризиком збитку для базових цінностей її нинішнього стану. Деякі дослідники визначають безпеку як стан, за якого відсутні загрози.

Виходячи з об’єктно-суб’єктної парадигми національної безпеки, Циганов В. В. характеризує її як міру реального рівня прав і свобод членів людського співтовариства (громадян) держави, що відповідає цьому співтовариству [5].

У Законі України “Про основи національної безпеки України” № 964-IV від 19 червня 2003 р. так розгорнуто тлумачиться це поняття: національна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров’я, охорони дитинства, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, кібербезпеки і кіберзахисту, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових послуг, захисту прав власності, фондових ринків й обігу цінних паперів, податково-бюджетної та митної політики, торгівлі і підприємницької діяльності, ринку банківських послуг, інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, промисловості і сільського господарства, транспорту та зв’язку, інформаційних технологій, енергетики та енергозбереження, функціонування природних монополій, використання надр, земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам”.

Закон України “Про національну безпеку України” № 2469-VIII від 21 червня 2018 р. значно лаконічніше сформулював це поняття без переліку національних інтересів: “національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз”.

Сьогодні виокремлюються принаймні три основні теоретичні підходи в розумінні сутності національної безпеки.

У межах першого підходу, представниками якого є Волферс А., Гадді Д., Даєм Г., Джонсон Дж., Кауфман Д., Коен Р., Міхалка М. та ін., увага акцентується на захисті цінностей суспільства. Серед базових цінностей виокремлюють політичну незалежність, економічний добробут, розвиток, справедливість тощо. При цьому безпека визначається не лише як захищеність національних цінностей, але й як їх безперешкодне поширення. Ці положення закріплені і в Стратегії національної безпеки США, у якій інші держави розглядаються в контексті їхнього ставлення до демократичних цінностей. У ній стверджується, що “з метою захисту нашої нації та поваги до наших цінностей Сполучені Штати прагнуть поширити свободу у всьому світі, очолюючи міжнародні зусилля зі знищення тиранії і підтримки ефективної демократії” [9]. Пояснити цей погляд на безпеку і її забезпечення можна, проаналізувавши думки, висловлені Фукуямою Ф. у праці “Кінець історії та остання людина” і Хантінгтоном С. у роботі “Зіткнення цивілізацій”. Фукуяма Ф. стверджує, що ліберальні демократії не становлять загрозу одна одній, а тому війна між справді демократичними державами фактично неможлива [10]. Що ж до Хантінгтона С., то він вважає, що лінії розлому між цивілізаціями (культурами, системами цінностей) і є лініями фронтів у майбутніх війнах [11]. Проте такий підхід до забезпечення національної безпеки шляхом поширення власних цінностей, навіть за допомогою збройних сил, містить у собі деструктивний потенціал конфліктності. Український науковець у сфері національної безпеки та антитерористичної діяльності Бодрук О. із цього приводу цілком слушно зазначає, що ці положення ґрунтуються на усталених процесах розвитку західного суспільства, ринковій економіці, індивідуалізмі, розвинутій демократії, а тому не завжди відповідають реаліям сьогодення [2].

Представники другого напрямку наголошують на взаємозв’язку національних цінностей та інтересів, необхідності врахування їхньої взаємообумовленості в дослідженні проблем національної безпеки. Серед них можна назвати Величка А., Волощука І., Горбуліна В., Демидова Б., Качинського А., Ліпкана В., Ситника Г. та ін.

Третій напрям наукових розробок полягає в дослідженні національної безпеки в контексті захисту національних інтересів. Представниками цього напряму є низка українських, російських та західних науковців: Бетлер А., Богданович В., Бодрук О., Браун С., Моргентау Г., Хоффман С. та ін. Слід також звернути увагу на розширення змісту поняття “національна безпека”: якщо раніше його забезпечення розглядалося у контексті захисту інтересів насамперед держави, то в сучасних дослідженнях акцент робиться на захисті інтересів особи (громадянина) та суспільства [7]. Зокрема, це положення відображене у вже нечинному Законі України “Про основи національної безпеки України”. Такий підхід, на нашу думку, не зовсім відповідає сучасним вимогам, оскільки зосереджує увагу виключно на інтересах держави, розвитку її економічного та військового потенціалу й підпорядкуванні цим цілям інтересів окремих особистостей, що спричиняє виникнення внутрішньодержавних конфліктів і в кінцевому результаті призводить до дезінтеграційних процесів. Проблема співвідношення інтересів особи, суспільства і держави в політиці національної безпеки остаточно не вирішена на користь інтересів людини. Справа в тому, що в системі забезпечення національної безпеки провідну, системоутворюючу роль відіграє держава. Саме державні органи та посадові особи формують нормативно-правову базу у сфері національної безпеки, приймають рішення щодо запобігання і нейтралізації загроз, виконання яких є обов’язковим.

Важливою також є монополія держави на застосування воєнної організації та здійснення інших передбачених законами заходів примусового характеру щодо забезпечення національної безпеки.

Складовими системи національної безпеки є:

– суб'єкти забезпечення національної безпеки (органи державної влади та місцевого самоврядування, інститути громадянського суспільства, окремі громадяни, засоби масової інформації);

– об'єкти національної безпеки (національні матеріальні й духовні цінності, інтереси особи, суспільства, держави);

– сукупність інструментів влади (воєнних, політичних, економічних, інформаційних тощо), які можуть бути використані для підтримки належного рівня захищеності національних інтересів (силові структури та відомства, спецслужби, розвідувальні органи, підприємства оборонно-промислового комплексу, дипломатичні засоби, державні та мобілізаційні резерви, інші ресурси, які цілеспрямовано призначені на захист національних інтересів);

– масив чинного національного законодавства, який визначає пріоритети державної політики національної безпеки, офіційні погляди щодо підходів, принципів і механізмів захисту національних інтересів, а також джерела та суб'єкти (фізичні й юридичні особи), що породжують загрози їхній реалізації;

– комплекс зовнішніх і внутрішніх факторів національної безпеки (зокрема змінні, які характеризують тенденції, показники, цілі, а також інші системи, наприклад, міжнародні структури безпеки, цілі та наслідки їхньої діяльності).

Такі складові системи національної безпеки (СНБ), як сукупність суб'єктів і об'єктів забезпечення національної безпеки, інструменти влади, джерела та суб'єкти, що породжують загрози національним інтересам, більшою мірою є структурними, а такі складові, як масив законодавства та фактори національної безпеки, які визначають умови та завдання СНБ, – функціональними. Деякі складові СНБ є відносно статичними, а інші – більш динамічними щодо змін у просторі й часі.

СНБ з точки зору системного підходу у процесі взаємодії особи, суспільства, органів державної влади та місцевого самоврядування з урахуванням взаємозв'язків між ними та середовища їхнього існування можна розглядати як відкриту, динамічну, соціальну систему, функціонування якої спрямоване на захист національних інтересів держави.

Під *соціальною системою* зазвичай розуміють сукупність соціальних явищ і процесів, основним елементом яких виступають люди, їхня взаємодія та зв'язки [12]. *Відкрита система,* відповідно до теорії систем, – це така, що безперервно взаємодіє із зовнішнім середовищем, причому ця взаємодія може здійснюватися у формі обміну інформацією або матеріальною трансформацією на межі із системою [13]. *Динамічна система* – система, яка під впливом зовнішніх і внутрішніх чинників змінює свій стан у часі [14]. Її ключовою властивістю є стійкість, тобто здатність зберігати базову структуру й основні функції протягом певного часу навіть за умов зовнішніх впливів і внутрішніх збурень. Розвиток динамічних систем відбувається через зміни їхньої структурної організації, що забезпечує більш ефективне виконання ними своїх функцій [15].

З огляду на вищевикладене, СНБ доцільно розглядати як відкриту динамічну соціальну систему, узагальнена модель якої подана на рис. 1.

При цьому враховується, що СНБ являє собою складний комплекс взаємопов'язаних елементів. Така система характеризується цілісністю, здатністю протидіяти впливам зовнішнього середовища та забезпечувати узгоджену діяльність усіх своїх компонентів для виконання спільного призначення системи.

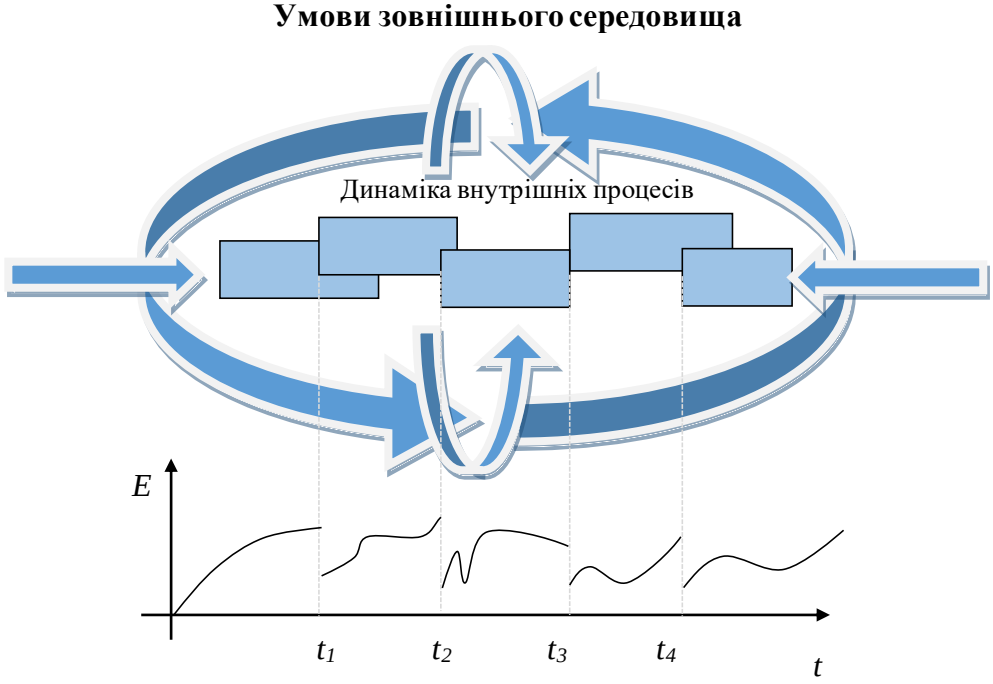


Рис. 1. Модель СНБ як відкритої динамічної соціальної системи

Згідно з визначенням, міра виконання системою свого призначення називається ефективністю. Формально ефективність (E) є функцією якості результату (Q), часу його отримання (T) та витрачених ресурсів (R).

Визначимо вектор внутрішніх параметрів системи через $P = (p_1, p_2 ... p_n)$, вектор параметрів, які визначаються зовнішнім середовищем, – $W = (w_1, w_2 ... w_n)$.

Очевидно, що стан системи, тобто сукупність значень внутрішніх параметрів $p \in P$, залежить від $w \in W$, причому ця залежність здебільшого має лаговий бути передбачуваними або спрогнозованими, виникає необхідність розв'язання завдання щодо об'єктивізації суб'єктивних висновків. Очевидно, що в більшості випадків зміна структури системи призводить до модифікації стратегії управління, тобто

$$C_t = F(S_t, A)$$

де C_t – стратегія (варіант стратегії) управління системою в момент часу t;
S_t – відповідна структура системи;
A – вирішувані завдання;
F – певний функціонал.

Визначення стратегії управління може здійснюватися як відповідно до цієї формули, так і без її врахування, що буде описано нижче.

У випадку, зображеному на рис. 1, у момент часу t_i відбувається структурна або організаційна перебудова, яка певним чином відповідає процесам, що називають "катастрофами" [16]. Відомо, що, виконуючи апроксимацію деяких характеристик, зокрема, ефективності системи, можна визначити момент настання та час розвитку таких "катастрофічних" процесів. За певних умов ці процеси можна попередити, прискорити або виконати інші дії. Водночас у деяких ділянках точок t_i настання "катастрофи" стає невідворотним, і зміна більшості завдань, структури та стратегії управління є детермінованим процесом. Отже, при структурно-функціональному аналізі СНБ, зокрема під час пошуку шляхів оптимізації її структури та уточнення завдань суб'єктів

забезпечення національної безпеки, головна увага має приділятися саме динамічним елементам.

Висновки

Національна безпека є кількісно-якісною характеристикою розвитку соціальної системи. Вона відображає результати впливу тенденцій розвитку та умов життєдіяльності соціуму і його інститутів, за яких забезпечується збереження якісної визначеності соціальної системи та вільне функціонування, що відповідає її природі. Оскільки життя суспільства розгортається в різних сферах (економічній, політичній, екологічній, інформаційній тощо), у кожній із них можливий вплив факторів, які водночас породжують загрози національній безпеці та відкривають можливості для їхньої нейтралізації. Відтак СНБ доцільно розглядати як сукупність взаємопов'язаних складових національної безпеки за вказаними сферами. Динаміка впливу зовнішніх і внутрішніх факторів на національну безпеку, які одночасно позначаються і на міжнародній безпеці, зумовлює потребу в постійній реорганізації системи: створенні та ліквідації окремих її складових, зокрема тих, які водночас інтегровані у СНБ, а також у відомчі, регіональні й міжнародні системи безпеки.

Список літератури

1. Павленко Д. Г., Семенюк Ю. В., Лисецький Ю. М. Виклики гібридної війни та національна безпека : монограіфія. Київ : ЛАТ&К, 2021. 136 с.
2. Бодрук О. С. Структури воєнної безпеки: національний та міжнародний аспекти. Київ, 2001. 300 с.
3. Глазов О. В. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. *Наукові праці Чорноморського державного університету імені Петра Могили. Політологія.* 2011. Вип. 143. Т. 155. С. 42-46.
4. Ліпкан В. А., Ліпкан О. С., Яковенко О. О. Національна і міжнародна безпека в визначеннях та поняттях. Київ : Текст, 2006. 256 с.
5. Циганов В. В. Національна безпека України : посібник. Київ : Національна академія внутрішніх справ України, 2004. 100 с.
6. Лисецький Ю. М., Семенюк Ю. В., Павленко Д. Г. Національна безпека: поняття, складові, чинники впливу. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Державне управління.* 2021. Т. 32 (71). № 3. С. 102-107.
7. Богданович В. Ю., Семенченко А. І., Єгоров Ю.В., Бортник О. О. Теоретико-методологічні засади забезпечення національної безпеки держави у її визначальних сферах : монографія. Київ : Кий, 2007. 370 с.
8. Лисецький Ю. М., Семенюк Ю. В., Павленко Д. Г. Національна безпека України. Організаційно-правові аспекти. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Державне управління.* 2021. Т. 32 (71). № 4. С. 109-117.
9. The National Security Strategy of the United States of America. Washington, 2006. 54 p.
10. Фукуяма Ф. Конец истории и последний человек. СП, 2005. 592 с.
11. Huntington S. P. The Clash of Civilizations and the Remakink of World Order. N.Y. : Simon & Shuster, 1996. 368 p.
12. Luhmann N. Social Systems. Stanford : Stanford University Press. 1995. P. 6-7.
13. Берталанфи Л. История и статус общей теории систем. Москва : Наука, 1973. 364 с.
14. Биркгоф Дж. Динамические системы. Москва : ОГИЗ, 1999. 480 с.
15. Рац О.М. Визначення сутності поняття "ефективність функціонування підприємства". *Економічний простір.* 2008. Вип. 15. С. 275-285.
16. Арнольд В.И. Теория катастроф. Москва : Наука, 1990. 128 с.

УДК 623.093 (351.86) DOI: 10.63978/3083-6476.2025.2.2.02

Білик Артем Сергійович
кандидат технічних наук, доцент
начальник науково-дослідної лабораторії
Науково-дослідний інститут воєнної розвідки Головного управління розвідки Міністерства оборони України
Київ, Україна
e-mail: artem.bilyk@gmail.com
ORCID: 000-0002-9219-920X

Михайловський Денис Віталійович
доктор технічних наук, професор
головний спеціаліст відділу супроводження дослідно-конструкторських робіт з розроблення озброєння та військової техніки та підтримки програм управління організації випробувань та супроводження розроблення озброєння та військової техніки
Центральне управління військової освіти і науки Генерального штабу Збройних Сил України
Київ, Україна
e-mail: d.mykhailovskyi@mil.ua
ORCID: 0000-0003-3151-8630

РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ КОНЦЕПЦІЇ УКРАЇНИ ІЗ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ – "КРАЇНА-ФОРТЕЦЯ"

Анотація. *Повномасштабна агресія рф проти України викликала нові виклики в частині оборони не лише військових об'єктів, а й об'єктів захисту цивільного населення та об'єктів критичної інфраструктури (ОКІ). Ураження ОКІ стратегічного значення для України стало одним із ключових напрямів ведення воєнних дій рф.*

Переважна більшість ОКІ зводилися надземними, без жодних систем інженерного конструктивного захисту для протидії повітряним загрозам, вибухам чи іншим впливам, пов'язаним із військовими діями. На сьогодні в Україні впроваджується державна концепція "Країна-фортеця", згідно з якою передбачено інтегральний захист ОКІ та інших об'єктів стратегічного значення. Це передбачає організацію ешелонованої протиповітряної оборони, аналогічної системам захисту Ізраїлю, США та інших країн, із комплексними заходами цивільного та інженерного захисту, системами радіоелектронної боротьби, встановленням хибних цілей, маскуванням, переходом від створення великих об'єктів стратегічного значення до менших, розосереджених між собою. Також у концепції запропоновано перехід на альтернативні джерела енергії та диверсифікацію енергогенерації, що сприятиме підвищенню стійкості країни до зовнішніх загроз воєнного часу.

У статті розглянуто ключові аспекти впровадження концепції "Країна-фортеця" для захисту ОКІ України та проведено аналіз стійкості ОКІ енергетичного сектору до атак засобів повітряного нападу противника. Окрім того, розглянуто основні загрози, пов'язані зі збільшенням кількості та підвищенням точності засобів повітряного нападу противника.

Ключові слова: *інженерний захист, об'єкти критичної інфраструктури, засоби повітряного нападу, ураження, вибух, будівельні конструкції.*

Artem Bilyk
PhD in Engineering, Associate Professor,
Head of Scientific Research Laboratory
of the Defence Intelligence Research Institute
Kyiv, Ukraine
e-mail: artem.bilyk@gmail.com
ORCID: 0000-0002-9219-920X

Denys Mykhailovskyi
Doctor of Engineering Science, Professor
Chief Specialist of the Department of Support
for Research and Development Works on the
Development of Armaments and Military
Equipment and Support for Programs of the
Department of Organization of Tests and
Support for the Development of Armaments
and Military Equipment of the Central
Directorate of Military Education and Science
General Staff of the Armed Forces of Ukraine
Kyiv, Ukraine
e-mail: d.mykhailovskyi@mil.ua
ORCID: 0000-0003-3151-8630

IMPLEMENTATION OF UKRAINE'S NATIONAL STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION: THE "FORTRESS NATION" CONCEPT

Abstract. *The full-scale aggression of the rf against Ukraine has introduced new challenges in the defense not only for military objects but also for civilian objects and for critical national infrastructure objects (CNIOs).*

Most of CNIOs in Ukraine were constructed above ground without any engineering protection systems to counter air threats, explosions, or other impacts associated with warfare. Currently, Ukraine is actively implementing the state "Fortress Country" concept, which envisions integrated protection of CNIOs and other strategically important facilities. This includes the organization of layered air defense systems, similar to those used by Israel, USA, and other countries, combined with comprehensive measures for civil protection, electronic warfare systems, deception measures. A transition from large centralized strategic facilities to smaller dispersed ones, and renewable energy sources are also proposed. These steps have significantly enhanced the country's resilience to external wartime threats.

This article shows the key aspects of implementing the "Fortress Country" concept for the protection of Ukraine's CNIOs and analyzes the resilience of energy sector infrastructure to air attacks by enemy forces. Additionally, the main threats posed by the increasing quantity and precision of enemy aerial attack weapons are reviewed.

Keywords: *engineering protection, critical national infrastructure, aerial attack means, damage, explosion, engineering defense, structural systems.*

Вступ

Постановка проблеми. В період війни захисні споруди ОКІ від засобів повітряного нападу (ЗПН) противника набувають особливого значення нарівні з протиповітряною обороною (ППО), засобами радіоелектронної боротьби (РЕБ) та іншими заходами захисту. Дуже важливим фактором, який впливає на обороноздатність країни, є оборонно-промисловий комплекс, що не зможе нормально функціонувати без іншої критичної інфраструктури.

Перемога України можлива лише за умов стійкого функціонування всіх галузей економіки країни в цілому. Як казав генерал армії США Першинг Д. під час Першої світової війни: “Піхота виграє битви, логістика виграє війни”. Зведення споруд інженерного захисту – це завжди баланс між часом, наявними ресурсами та рівнем захищеності активів.

Нові ризики, пов’язані з повномасштабним вторгненням росії в Україну, зумовлені застосуванням насамперед безпілотних літальних апаратів (БпЛА)-камікадзе, ракет і керованих авіаційних бомб (КАБ) з відповідними факторами ураження: прямі влучання, близькі вибухи, що спричиняють вибухово-ударну хвилю (ВУХ), осколки, падіння уламків, займання тощо. Усі ці фактори потребують урахування. Ворог постійно вдосконалює свої ЗПН, особливо це стосується БпЛА різних типів. З’являються нові БпЛА оперативного та стратегічного рівнів. Зафіксоване застосування реактивних “Shahed-238” / “Герань-3”, БпЛА “Shahed-136” / “Герань-2” з посиленою бойовою частиною (БЧ) вагою 90 кг і потужністю 100 кг у тротиловому еквіваленті. Крім того, БпЛА споряджаються готовими елементами – осколками для нанесення максимального ураження.

Також ворогом проводяться роботи по удосконаленню ракет. Зокрема, ракети Х-101, які найбільше застосовуються в рф проти України, почали обладнувати подвійною БЧ. Удосконалюються системи наведення ЗПН, що підвищує точності ураження та стійкість до систем РЕБ, а також постійно змінюється тактика їхнього застосування. За таких умов зведення споруд інженерного захисту (СІЗ) набуває ще більшої ваги.

Аналіз останніх досліджень і публікацій. Захисні споруди поділяються на фортифікаційні (застосовні на фронті), споруди цивільного захисту (призначені для укриття населення) та СІЗ, призначені для захисту елементів ОКІ [1-6]. Новітні характеристики БпЛА рф, які застосовуються для ударів по ОКІ в Україні, наведено в табл. 1.

Таблиця 1

Основні характеристики БпЛА рф, які використовуються для ударів по ОКІ в Україні

Тип БпЛА	Довжина, м	Ширина, м	Вага БЧ, кг	Максимальна швидкість, м/с	Стартова маса, кг	Дальність, км
Шахед-131/Герань-1	2,6	2,2	20	30	135	900
Шахед-136/Герань-2/МС 236	3,5	2,5	40-52, є 88	60	200	2000
Шахед-238/Герань-3/ МС 237	3,5	3	50	167	Біля 200	2500
Гербера	1,2	2,5	3...5	34	18	300
Гарпія 3 /ASN-301	2,5	2,41	50	61	135	2000
ZALA Z54	2,3	2,5	20	47	110	200
ПРИВЕТ-120	Біля 1	2	16	44	Біля 50	250
Бандероль*	2,5	2,2	130	125-180	263	420

*БпЛА типу “баражуючий боєприпас” (також відомий як крилата ракета S-8000 Б), застосування почалося в квітні 2025 року

Статистика застосування БпЛА і ракет противником наведена на рис. 1, 2.

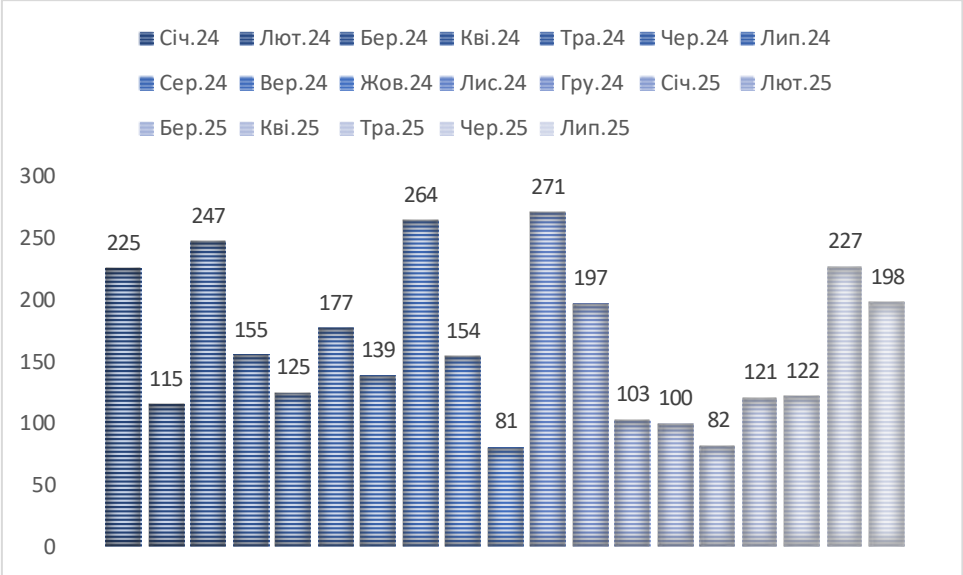


Рис. 1. Застосування ракет противником у 2024 та першому кварталі 2025 року

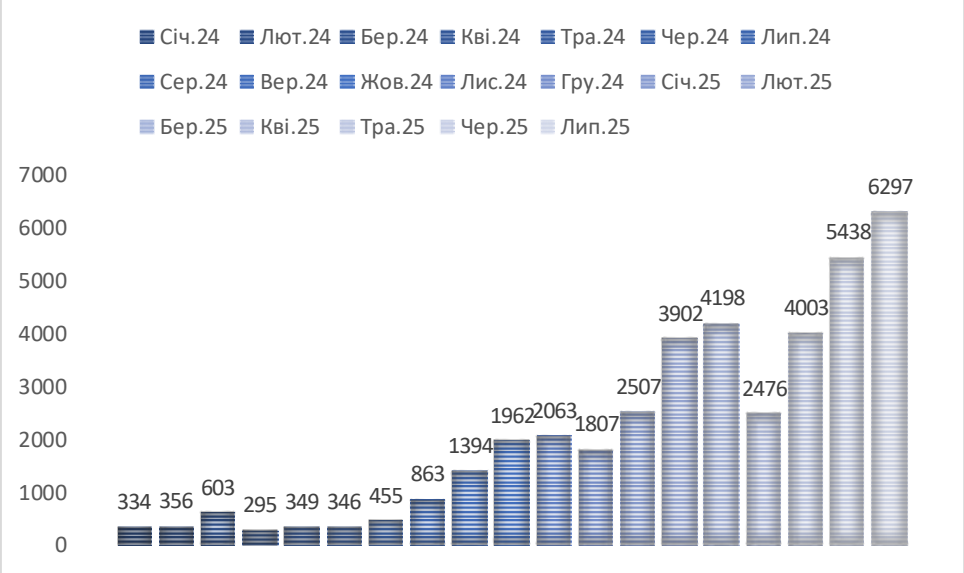


Рис. 2. Застосування БпЛА противником у 2024 та першому кварталі 2025 року

З наведених графіків видно, що кількість застосованого ракетного озброєння залишається приблизно на одному рівні. Водночас ситуація із застосуванням БпЛА змінилася суттєво. Як показано на рис. 2, якщо на початок 2024 року рф застосовувала переважно не більше ніж 400 БпЛА типу “Shahed”, то вже в квітні та червні 2025 року їхня кількість вже перевищила 4000 одиниць на місяць. За розвідувальними даними, росія продовжує нарощувати виробництво БпЛА цього типу, а отже, можна очікувати подальшого їхнього зростання. За три з половиною роки повномасштабної війни рф проти України та щоденних протиповітряних боїв Повітряні Сили України майже вичерпали ресурс ракет радянських зенітних ракетних систем і тепер значною мірою розраховують на підтримку партнерів у контексті продовження поставок західних систем, а головне – ракет до них, для посилення української протиповітряної оборони. Водночас необхідно широко впроваджувати вітчизняні проєкти у сфері ППО.

У 2024-2025 роках спостерігається зниження ефективності ППО у протидії ЗПН противника. Якщо у 2024 році середня ефективність знищення БпЛА становила понад 80%, то з початку 2025 року впала до 55-60%.

Збільшення кількості уражень і масштаб руйнування об'єктів від атак російських БпЛА типу "Shahed" значно зросли. Це пов'язано зі зміною тактики їхнього застосування: противник почав зосереджувати удари на окремих ОКІ, одночасно атакуючи одну ціль багатьма БпЛА, що суттєво ускладнює роботу українських сил ППО та перенавантажує системи. Фіксуються часті випадки тандемного влучання кількох БпЛА фактично в одну точку. Відстань між ураженнями часто не перевищує 3 м. На деяких БпЛА типу "Shahed" виявлені звичайні й тепловізійні камери, а також системи штучного інтелекту.

Слід зазначити, що противник суттєво вдосконалив свої можливості супутникової розвідки. Орбітальне угрупування космічних апаратів, яке використовується в інтересах міністерства оборони росії, станом на початок 2025 року налічує близько 40 супутників (власних, комерційних, китайських та іранських). Це дозволяє противнику здійснювати 51-65 прольотів над територією України на добу, досягнувши циклу зйомки 45-50 хвилин. Така ситуація створює нові виклики щодо переміщення та маскування об'єктів, а також ведення рятувально-відновних робіт.

На рис. 3 наведено статистику ефективності застосування БпЛА противника в окремі періоди.

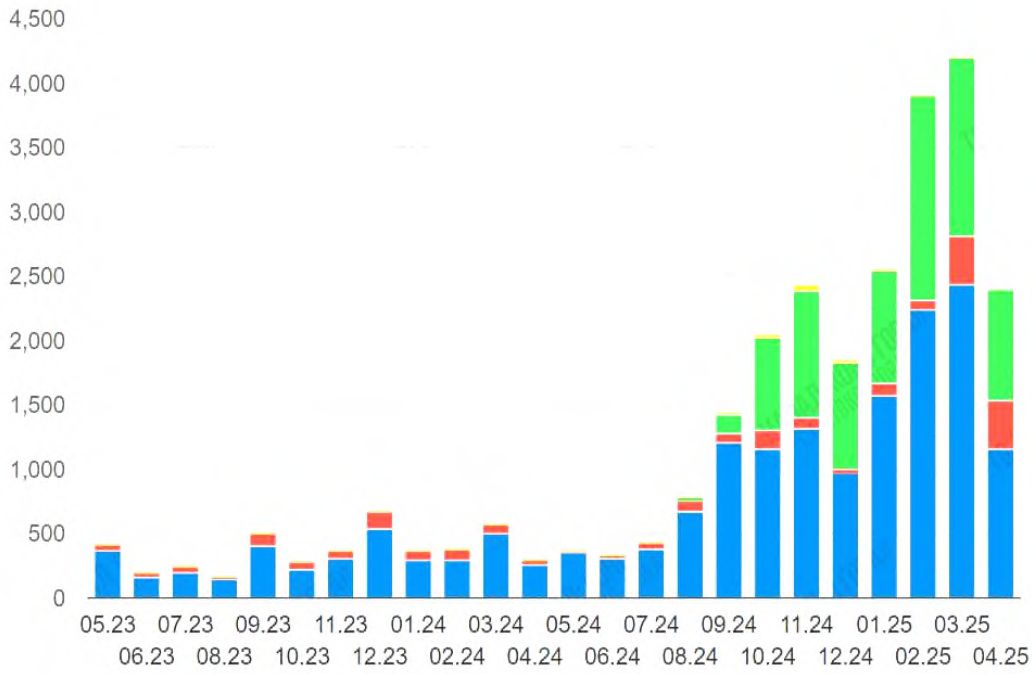


Рис. 3. Статистика ефективності БпЛА противника у окремі періоди: зелений колір – подавлені РЕБ або БпЛА-імітатори, червоні – влучання, синій – збиті, жовтий – улетіли за межі України

Метою статті є аналіз практичного досвіду впровадження державної Концепції України із захисту критичної інфраструктури – "Країна-фортеця", схваленої Постановою Кабінету Міністрів України № 471 від 26.04.2024 [7] (далі – Концепція "Країна-Фортеця"). Матеріали, наведені в статті, спрямовані на обґрунтування доцільності масштабування застосування систем інженерного захисту, запроваджених Концепцією "Країна-фортеця", на всі галузі критичної інфраструктури України, а також поширення окремих її положень на зведення споруд цивільного захисту та різноманітних фортифікаційних споруд.

Виклад основного матеріалу

Концепція "Країна-Фортеця" – концепція інтегрального інженерного захисту ОКІ, розроблена колективом авторів у 2022-2023 роках із фокусом на СІЗ ОКІ енергетики України та розвинена у 2023-2025 роках [2; 4; 7]. Метою Концепції "Країна-фортеця" є визначення єдиного підходу до інженерного захисту ОКІ та підвищення рівня їхнього захищеності для стабільного й безперервного надання життєво важливих функцій і/або послуг. Концепція "Країна-фортеця" покликана забезпечити інтегральний захист території, об'єктів, громадян і суспільства загалом від актуальних загроз, зокрма від факторів ураження ЗПН, що є складовою національної безпеки і оборони України. Строк реалізації Концепції "Країна-фортеця" – 2024-2030 роки.

Найкращі системи активного захисту та протиповітряної оборони, розроблені у світі до цього часу, мають технологічний поріг ефективності застосування у разі знешкодження високоточних, далекобійних і гіперзвукових засобів повітряного нападу противника. Отже, основу безпеки ОКІ мають становити їхня децентралізація, резервування та пасивний інженерний захист елементів ОКІ для підвищення їхньої живучості, безпеки персоналу й стійкого функціонування держави в інтересах забезпечення життєвих потреб суспільства.

Концепція "Країна-Фортеця" в Україні поширюється на існуючі та нові СІЗ, що створюють на ОКІ для захисту їхніх критичних елементів. Існуючі СІЗ в Україні підлягають оцінюванню технічного стану щодо захисних властивостей і фізичної придатності до подальшої експлуатації та, залежно від ухваленого рішення, – заміні, реконструкції або підсиленню з доведенням захисних характеристик до необхідного рівня. Концепція передбачає вимоги та конструктивні рішення для трьох рівнів СІЗ:

перший рівень – захист від поодиноких непрямих влучань БпЛА на відстані понад 5 метрів від СІЗ та поодиноких непрямих влучань ракети на відстані понад 15 метрів від СІЗ; для об'єктів морської та річкової критичної інфраструктури (ОМРКІ) – додатково від поодиноких непрямих влучань безпілотних плавучих апаратів (БпПА) та торпед на відстані понад 5 метрів від СІЗ;

другий рівень – захист від поодиноких прямих влучань БпЛА та поодиноких непрямих влучань ракети на відстані понад 15 метрів від СІЗ; для ОМРКІ – додатково від поодиноких прямих влучань БпПА та торпед;

третій рівень – захист від поодиноких прямих влучань БпЛА та поодиноких прямих влучань ракети у СІЗ; для ОМРКІ – додатково від поодиноких прямих влучань БпПА та торпед.

Окрім цього, Концепцією визначено три категорії відповідальності елементів ОКІ:

категорія А – конструкції та елементи, відмова яких може призвести до повної непридатності ОКІ (або значної його частини) до експлуатації; відновлення триває понад 3 тижні;

категорія Б – конструкції та елементи об'єкту критичної інфраструктури, відмова яких може ускладнити нормальну експлуатацію ОКІ або призвести до відмови інших елементів, що не належать до категорії А; відновлення триває 1-3 тижні;

категорія В – конструкції та елементи, відмови яких не призводить до порушення основної функції ОКІ чи роботи інших конструкцій або їхніх елементів; відновлення триває до 1 тижня.

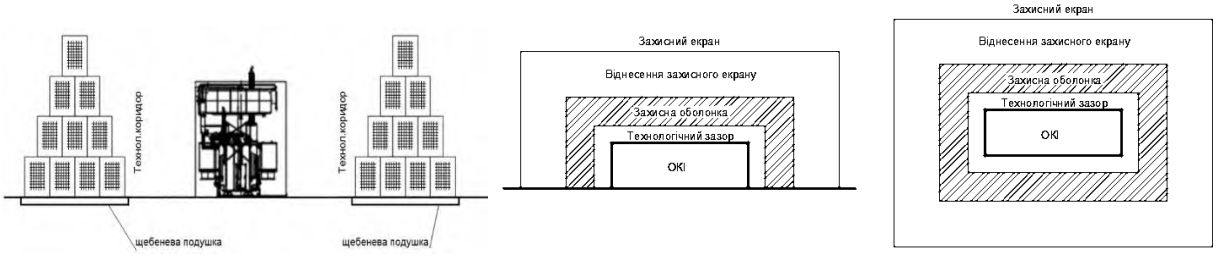
Розрахункові терміни експлуатації систем інженерного захисту становлять:
для 1-го рівня – не менший ніж 5 років;
для 2-го рівня – не нижче нормативного терміну експлуатації елемента об'єкта;
для 3-го рівня – не нижче ніж 100 років.

Згідно з вимогами Концепції "Країна-Фортеця" СІЗ повинні відповідати таким критеріям: ресурсодоступність та швидкість виготовлення і монтажу; простота виконання;

високий рівень живучості та ремонтопридатності елементів при ураженнях, їхня взаємозамінність; відсутність або мінімізація технологічних зупинок основного функціоналу ОКІ при улаштуванні СІЗ; гнучкість у застосуванні, модульність, уніфікація та типізація, можливість влаштування СІЗ із різних елементів; максимізація СІЗ при мінімізації витрат ресурсів; можливість демонтажу, для СІЗ першого рівня.

Конструктивні рішення СІЗ 1 і 2 рівня для різних типів критичних елементів (КЕ) мають відповідати "Типовим рішенням з інженерного захисту критичних елементів об'єктів критичної інфраструктури України від ураження засобами повітряного нападу противника", які також схвалені Постановою Кабінету Міністрів України № 471 [7]. Конструкції та виконання СІЗ 1 рівня із габіонів повинні відповідати вимогам у "Рекомендаціях щодо вибору та встановлення елементів габіонних споруд для реалізації типових рішень з інженерного захисту критичних елементів об'єктів критичної інфраструктури України від ураження засобами повітряного нападу противника", затвердженим заступником начальника Генерального штабу Збройних Сил України 15.11.2023.

Перший рівень захисту рекомендується застосовувати для існуючих ОКІ (рис. 4 *а*). СІЗ 2 рівня за компонуванням повинні виконуватися окремо розташованими (які виконуються на існуючих або нових ділянках для поодиноких КЕ ОКІ) або інтегрованими. Окремо розташовані СІЗ 2 рівня за конструктивом виконують суцільними одношаровими або двошаровими типу "шелтер" (рис. 4 *б*), частково або повністю заглибленими, обвалованими ґрунтом. Узагальнено схеми СІЗ 1 і 2 рівня показано на рис. 4, а варіанти улаштування СІЗ 3 рівня на рис. 5.



а *б*

Рис. 4. Схеми інженерного захисту елементів ОКІ:
а – 1 рівня із застосуванням габіонів;
б – 2 рівня із захисною оболонкою та предетонаційним екраном

Для існуючих будівель та споруд для забезпечення 2 рівня СІЗ зазвичай застосовують один або декілька із наступних заходів: підсилення перекриттів та покриттів шляхом підведення додаткових рам та листів з металу і деревини, підсилення колон та стін каркасів; заповнення просвітів захисними елементами; встановлення виносних та/або окремо розташованих предетонаційних екранів; улаштування спеціальних внутрішніх споруд, що захищають КЕ від падіння решток горизонтальних конструкцій будівель, технологічного обладнання чи ураження уламками (осколками) засобів повітряного нападу противника; у разі необхідності, збільшення товщини основних захисних конструкцій, обшивка металевими листами, в тому числі з використанням бронелистів.

На рис. 5 наведено основні можливі схеми СІЗ 3 рівня: *а* – з повним заглибленням (в такому виконанні досягається найбільший рівень захисту); *б* – з частковим заглибленням (в такому варіанті досягається баланс вартості і строків виконання); *в* – на поверхні (найбільш дешевий варіант, який рекомендується для застосування у випадках неможливості заглиблення через різноманітні фактори, в тому числі, і інженерно-геологічні умови майданчику будівництва).

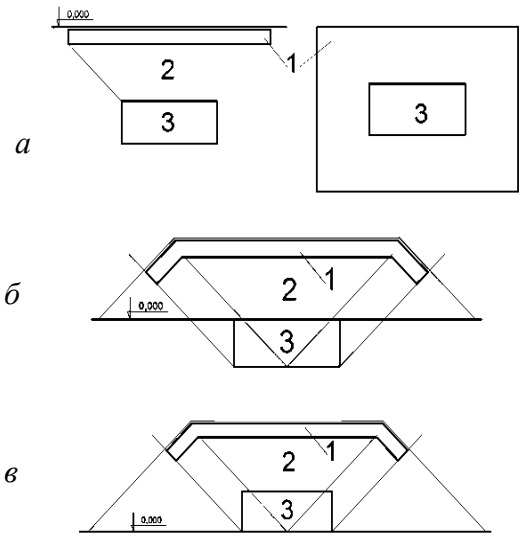


Рис. 5. Варіанти рішень інженерного захисту елементів ОКІ:
а – з повним заглибленням; *б* – частковим заглибленням;
1 – тюфяк; 2 – розподільча товща ґрунту; 3 – остов захисної споруди ОКІ

СІЗ 3 рівня повинні виконуватися у варіантах: повністю інтегровані у контур плями забудови існуючих або нових споруд; частково інтегровані у контур плями забудови існуючих або нових споруд; окремо розташовані. СІЗ 3 рівня, які захищають від дії прямих влучань ЗПН противника (рис. 5), як правило, складаються із 3-х компонентів (зверху донизу): тюфяк, який виконує роль затримуючої плити та призначений для зупинки механічного проникнення БЧ і, відповідно, віддалення місця його можливого розриву при фугасній дії; розподільча товща, яка має амортизувати вибухову хвилю при вибуху заряду на тюфяку; несучий шар – каркас заглибленої конструкції, який має витримувати як власну вагу з нормальним тиском ґрунту, так і варіанти тиску від ВУХ в землі: вертикальної або бічної. Додатково по тюфяку рекомендується влаштовувати 3 або більше шари бутового каміння розміром 300-500 мм. На рис. 6 показано перспективний зовнішній вигляд СІЗ 3 рівня об’єкту енергетичної критичної інфраструктури.

Рис. 6. Візуалізація СІЗ 3 рівня

Зведені СІЗ вже показали значні захисні властивості. В тому числі, масове спорудження СІЗ для захисту об'єктів енергетики дозволило пройти Україні зиму 2024-2025 років практично без блекаутів. СІЗ 1 рівня, в основному габіонні, забезпечили прийнятний рівень захисту за малий час і кошти. Зібрана часткова статистика показала відносну ефективність збудованих СІЗ 1 рівня. БпЛА рф мають більшу точність, ніж ракети, що значно знижує ефективність СІЗ 1 рівня, але їхня руйнівна дія більш локальна. У багатьох випадках знищення КЕ ОКІ, захищеного СІЗ 1 рівня, при прямому влучанні дозволяло зберегти сусідні КЕ, так як СІЗ затримували поширення уламків та ВУХ (рис. 7 та рис. 8).

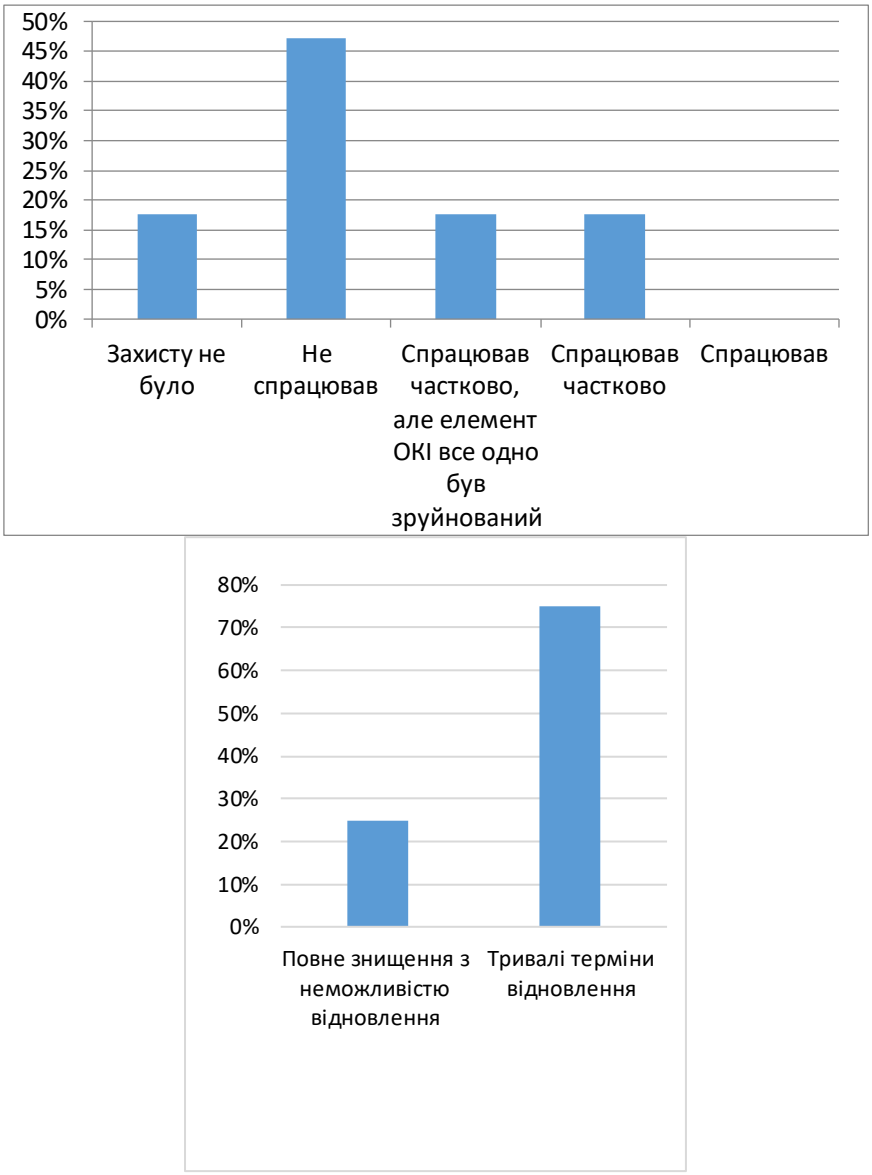
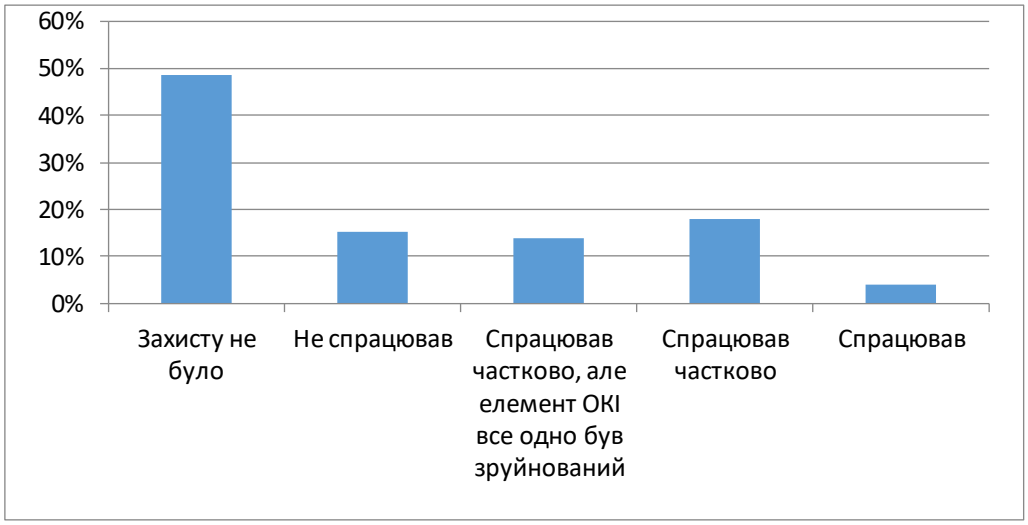


Рис. 7. Ефективність СІЗ 1 рівня супроти влучань БпЛА (2022-2023); наслідки ушкоджень КЕ ОКІ від влучань БпЛА (з захистом і без нього), 2024 р.

СІЗ 2 рівня показали високий рівень захищеності та забезпечили збереження елементів ОКІ під час сотень прямих влучань БпЛА (рис. 8).



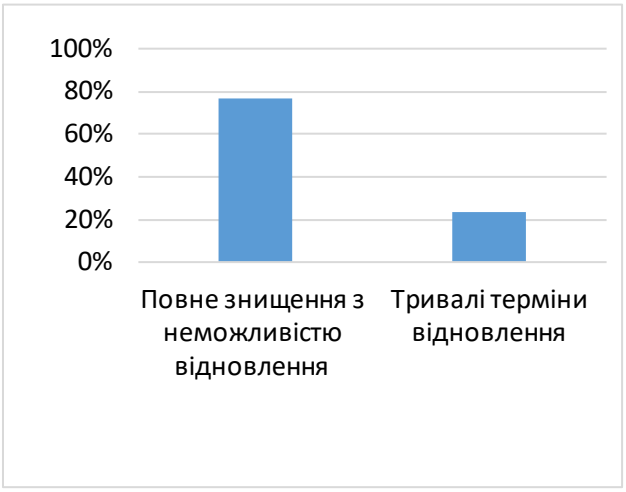


Рис. 8. Ефективність СІЗ 2 рівня супроти влучань ракет (2022-2023); наслідки ушкоджень КЕ ОКІ від влучань ракет (з захистом і без нього), 2024 р.

Статистика щодо ефективності споруд 2-го рівня ще перебуває в процесі збору. Водночас, за приватною інформацією, понад 60 прямих влучань БпЛА у споруди 2-го рівня, виконані повністю згідно з проєктом, жодного разу не призвели до руйнування трансформаторів (рис. 9).

Рис. 9. Приклади побудованих СІЗ 2 рівня

Натомість прямі (і навіть непрямі) влучання БпЛА в споруди 2-го рівня, які були запроєктовані або виконані з порушеннями (кількість поки що невідома), призводили до знищення обладнання КЕ.

На основі Концепції "Країна-Фортеця" на місцевому рівні також була розроблена концепція захисту міста Київ [7].

Висновки

Досвід широкого впровадження Концепції "Країна-Фортеця" для енергетичної критичної інфраструктури показав її високу ефективність. Кількість знищених КЕ на ОКІ значно зменшилась, навіть при нарощуванні ворогом кількості та якості ЗПН, що застосовуються під час повітряних атак. Напрямами подальшого розвитку Концепції "Країна-Фортеця" є: розширення номенклатури ОКІ різних галузей – цивільного, промислового та військового призначення; удосконалення вимог до СІЗ у зв'язку з розвитком ЗПН та тактики їхнього застосування (зокрема нові БЧ збільшеної потужності, термобаричні, дуплетні, касетні, з додатковими уражувальними елементами, ударними ядрами, кумулятивами, вдосконаленими підривачами, що ускладнює розмінування збитих і нерозірваних БЧ; підвищення точності ударів; зростання кількості атак; проведення повторних атак із високою точністю ураження; збільшення кількості атак на цивільні об'єкти тощо); розвиток положень проєктування та методик розрахунку СІЗ на дію ЗПН; впровадження нових класів СІЗ, захищених просторів у житлових і громадських будинках; підсилення існуючих будівель із нульовою живучістю; застосування первинних швидкомонтованих укриттів, розрахованих на дію факторів ЗПН; оснащення будинків і споруд засобами першочергового укріплення та ремонту.

Додатково слід впроваджувати програми широкого навчання населення домедичної допомоги, саморятування та розбирання завалів за типом програми "Білі шоломи" [8].

Список літератури

1. Михайловський Д. В. Еволюція фортифікаційних і захисних споруд. *Будівельні конструкції, теорія і практика.* 2025. № 16. С. 183-211. URL: https://doi.org/10.32347/2522-4182.16.2025.183-211.
2. Коваль М. В., Коваль В. В., Білик А.С., Коцюруба В. І., Кубраков О. М. Основи інженерного захисту об'єктів критичної інфраструктури енергетичної галузі України від засобів повітряного нападу противника : монографія / за ред. А.С. Білика. Київ : ГШ ЗСУ, 2023. 180 с.

3. Kotsiuruba V., Bilyk A., Bzot V., Dzeverin I. Захист об'єктів критичної інфраструктури України від прямих влучань ракет за допомогою підземного розташування. *Ядерна та радіаційна безпека*. 2023. № 2 (98). С. 69-79.
4. Михайловський Д. В., Білик А. С., Скляров І. О. Розрахунок конструкцій будівель і споруд на дії основних факторів ураження засобів повітряного нападу : монографія. Київ : Каравела, 2024. 92 с.
5. Mykhailovskyi D. V., Skliarov I. O., Khomik M. M., Vavilova N. V., Skliarova T. S. Analysis of methods for calculating the penetrating effect of the main types of missiles and fragmentation damage to the structures of protective constructions. *Strength of materials and theory of structures: scientific and technical collection*. 2024. Iss. 113. P. 171-182. URL: https://doi.org/10.32347/2410-2547.2024.113.171-182.
6. Mykhailovskyi D., Skliarov I., Komar O. Analysis of calculation methods for explosion shock wave parameters in the design of protective structures. *Strength of materials and theory of structures: scientific and technical collection*. 2025. Iss. 114. P. 173-182. URL: https://doi.org/10.32347/2410-2547.2025.114.173-182.
7. Постанова Кабінету Міністрів України "Деякі питання інженерного захисту критичної інфраструктури" від 26 квітня 2024 р. № 471.
8. Рішення Київської міської ради від 07.05.2024 № 8/231-606ПР. URL: https://kmr.gov.ua/sites/default/files/606_8.pdf.

УДК 355.45:351.86:327.8 DOI: 10.63978/3083-6476.2025.2.2.03

Коваль Володимир Валерійович
кандидат військових наук,
старший науковий співробітник
Громадська організація "Центр воєнної стратегії і технологій"
Київ, Україна
e-mail: vladimerkoval69@gmail.com
ORCID: 0000-0002-6209-6779

Семененко Олег Михайлович
доктор військових наук, професор
заступник начальника Центрального науково-дослідного інституту Збройних Сил України з наукової роботи
Київ, Україна
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

Кінь Олександр Віталійович
кандидат технічних наук
Дипломатична академія України імені Геннадія Удовенка
Київ, Україна
e-mail: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

КОГНІТИВНІ ОПЕРАЦІЇ ТА ВІЙНИ В СУЧАСНОМУ БЕЗПЕКОВОМУ СЕРЕДОВИЩІ: ПЕРЕДУМОВИ, ДИНАМІКА, НАСЛІДКИ

Анотація. *Сучасне безпекове середовище вже не обмежується фізичним простором бойових дій; воно включає інформаційний, медійний, цифровий і соціальний виміри, у яких розгортаються багатовимірні когнітивні війни з цілою низкою когнітивних операцій, спрямованих на підрив національної єдності, дискредитацію інститутів держави, розмиття уявлення про правду, нав'язування суспільству наративів поразки, зневіри або капітуляції. Найновіші тенденції 2024-2025 років свідчать про еволюцію інструментарію когнітивних операцій. Саме тому вивчення передумов, динаміки та наслідків когнітивних операцій, а також розробка теоретичних і прикладних моделей захисту від них є критично необхідними, бо це відкриває простір для міждисциплінарних досліджень на стику безпекових студій, психології, нейронаук, соціології, інформаційних технологій та військової стратегії. Отже, метою статті є комплексне дослідження природи та механізмів когнітивних операцій і війн у сучасному безпековому середовищі на прикладі когнітивного протистояння між росією та Україною, а також аналіз їх ніх передумов і динаміки розвитку, оцінка можливих наслідків для національної та міжнародної безпеки з урахуванням сучасних викликів і загроз. Основними результатами дослідження є: аналіз термінології за напрямом когнітивних операцій та когнітивних війн; розкриття особливостей основних когнітивних операцій росії проти України; визначення основних характеристик триваючого когнітивного протистояння між росією та Україною; проведення аналітичного узагальнення щодо когнітивних операцій, які реалізувала або реалізовує Україна проти росії, а також проведення оцінювання їхнього ступеня дієвості та наслідків очікуваних результатів. Матеріали статті будуть корисними фахівцям у сфері національної безпеки, стратегічних комунікацій, військової справи, аналітикам, спеціалістам міжнародних відносин та науковцям із галузі політичних, психологічних та військових наук.*

Ключові слова: *виклики і загрози в когнітивному просторі, інформаційна агресія, когнітивні операції, когнітивна війна, когнітивне протистояння, гібридна війна, російсько-українська війна, стратегічна дестабілізація, асиметричні дії, інформаційно-психологічний вплив, національна безпека.*

Volodymyr Koval
PhD in Military Science,
Senior Researcher
Non-Governmental Organization
"Center for Military Strategy and Technologies"
Kyiv, Ukraine
e-mail: vladimerkoval69@gmail.com
ORCID: 0000-0002-6209-6779

Oleh Semenenko
Doctor of Military Sciences,
Professor Deputy Head of the Central Scientific Research
Institute of the Armed Forces of Ukraine for Scientific Work
Kyiv, Ukraine
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

Oleksandr Kin
PhD in Engineering, Associate Professor,
Senior Research Fellow
Diplomatic Academy of Ukraine named after Hennadii Udovenko
Kyiv, Ukraine
e-mail: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

COGNITIVE OPERATIONS AND WARFARE IN THE CONTEMPORARY SECURITY LANDSCAPE: DRIVERS, DYNAMICS, AND IMPLICATIONS

Abstract*. The modern security environment is no longer limited to the physical space of combat; it includes information, media, digital and social dimensions, in which multidimensional cognitive wars are unfolding with a whole range of cognitive operations aimed at undermining national unity, discrediting state institutions, blurring the idea of truth, imposing narratives of defeat, despair or surrender on society. The latest trends of 2024–2025 indicate the evolution of the cognitive operations toolkit. That is why the study of the prerequisites, dynamics and consequences of cognitive operations, as well as the development of theoretical and applied models of protection against them are critically necessary, because this opens up space for interdisciplinary research at the intersection of security studies, psychology, neuroscience, sociology, information technology and military strategy. Thus, the purpose of the article is a comprehensive study of the nature and mechanisms of cognitive operations and wars in the modern security environment using the example of the cognitive confrontation between Russia and Ukraine, as well as an analysis of their prerequisites and dynamics of development, an assessment of possible consequences for national and international security, taking into account modern challenges and threats. The main results of the study are: an analysis of terminology in the field of cognitive operations and cognitive wars; disclosure of the features of the main cognitive operations of Russia against Ukraine; identification of the main characteristics of the ongoing cognitive confrontation between Russia and Ukraine; conducting an analytical generalization on the cognitive operations that Ukraine has implemented or is implementing against Russia, as well as an assessment of their degree of effectiveness and the consequences of the expected results. The materials of the article will be useful to specialists in the field of*

national security, strategic communications, military affairs, analysts, specialists in international relations and scholars in the field of political, psychological and military sciences.

Keywords: *challenges and threats in the cognitive space, information aggression, cognitive operations, cognitive war, cognitive confrontation, hybrid war, Russian-Ukrainian war, strategic destabilization, asymmetric actions, information and psychological influence, national security.*

Вступ

Постановка проблеми. У контексті триваючої російсько-української війни питання когнітивних операцій на середину 2025 року набуває виняткової ваги для національної безпеки України. Росія системно веде гібридну агресію, де когнітивні впливи у вигляді маніпуляції свідомістю, інформаційно-психологічного тиску, формування вигідної картини реальності в свідомості як українського населення, так і міжнародної спільноти є одним з ключових інструментів досягнення воєнно-політичних цілей [1-4].

Сучасне безпекове середовище вже не обмежується фізичним простором бойових дій; воно включає інформаційний, медійний, цифровий і соціальний виміри, у яких розгортаються багатовимірні когнітивні війни та окремі операції. Ці операції спрямовані на підрив національної єдності, дискредитацію інститутів держави, розмиття уявлення про правду, нав'язування суспільству наративів поразки, зневіри або капітуляції [1-21]. Найновіші тенденції 2024-2025 років свідчать про еволюцію інструментарію когнітивних операцій, а саме: використання штучного інтелекту для створення фейків і "deep fake"; масове застосування бот-мереж; вплив через таргетовану рекламу та ігрові платформи; координація інформаційних вкидів із бойовими діями. Особливо небезпечними є сценарії, коли інформаційно-психологічні атаки синхронізуються з ударами по критичній інфраструктурі або з дипломатичними кампаніями тиску. Водночас, попри значну увагу до теми інформаційної безпеки, в Україні досі відсутня цілісна система розуміння й протидії саме когнітивним війнам, таким як війнам за сприйняття, свідомість, волю до спротиву. Такі війни не завершуються з припиненням вогню і мають тривалий ефект на суспільну свідомість, політичну стабільність і стратегічну суб'єктність держави.

Саме тому вивчення передумов, динаміки та наслідків когнітивних операцій, а також розробка теоретичних і прикладних моделей захисту від них є критично необхідними, бо це відкриває простір для міждисциплінарних досліджень на стику безпекових студій, психології, нейронаук, соціології, інформаційних технологій та військової стратегії.

Станом на середину 2025 року актуальним є запит на формування національної концепції когнітивної безпеки, розбудову спеціалізованих спроможностей у Силах оборони, посилення ролі освіти та стійкості суспільства до деструктивного впливу ворожих когнітивних кампаній. Дослідження цієї тематики має стати пріоритетом для науковців, військових аналітиків та стратегічних комунікаторів. Таким чином, подальше наукове опрацювання феномену когнітивних операцій є не лише теоретично значущим, а й практично необхідним для забезпечення стратегічної стійкості та перемоги України у війні нового типу – війні за свідомість, наратив і майбутнє.

Аналіз останніх досліджень і публікацій. Сучасні гібридні конфлікти, зокрема російсько-українська війна, засвідчили зростаюче значення впливу на свідомість, сприйняття та волю як цивільного населення, так і військового керівництва [1-9]. В умовах інформаційного перенасичення та психологічного тиску терміни "когнітивні операції", "когнітивна війна" та "інформаційно-психологічний вплив" дедалі частіше використовуються у військовій, безпековій та науковій риториці. Однак відсутність уніфікованого термінологічного апарату ускладнює формування єдиної доктринальної позиції та нормативного регулювання дій у сфері когнітивної безпеки. У зв'язку з цим проведено аналіз ключових термінів, що використовуються у вітчизняному та зарубіжному дискурсі, для виявлення спільних та відмінних характеристик, визначення прогалин

і суперечностей у поточному розумінні та формулюваннях. У табл. 1 наведено результати аналізу основних понять, що стосуються когнітивного домену сучасної війни [1-21].

Таблиця 1

Аналіз термінології за напрямом когнітивних операцій та когнітивних війн

Термін	Автор	Визначення
Когнітивізм	Ульрік Найссер (Ulric Neisser), 1967	Психологічний напрям, який досліджує внутрішні ментальні процеси (сприйняття, пам'ять, мислення, мова), що лежать в основі поведінки. Пізнання розглядається як активне оброблення інформації
Когнітивна атака	Rand Corporation (Блейс Кук), 2019	Цілеспрямоване інформаційне або психологічне втручання, спрямоване на спотворення або руйнування здатності суб'єкта (особи чи групи) до раціонального мислення та прийняття рішень
Когнітивна атака	Caleb Carr, 2020	Використання медіа, соціальних мереж або дезінформації для маніпуляції уявленнями, емоціями та поведінкою цільової аудиторії задля досягнення стратегічних цілей
Когнітивні операції	NATO, AJP-3.10.1, 2021	Координація заходів, спрямованих на вплив на сприйняття, емоції, процеси ухвалення рішень і поведінку противника, союзників, нейтральних сторін або власного населення в межах інформаційних кампаній
Когнітивна операція	Doctrine for Joint Cognitive Operations (США, 2023)	Планована діяльність, що має на меті змінити або посилити когнітивні установки цільової аудиторії у спосіб, що відповідає стратегічним цілям операції
Когнітивні операції	US Joint Doctrine Note 3-13, 2018	Операції, які цілеспрямовано впливають на когнітивні функції цільових суб'єктів, використовуючи інформаційні, психологічні та кіберзасоби для досягнення оперативних або стратегічних ефектів
Когнітивна війна	Французьке Міноборони (DGRIS), 2020	Нова форма війни, у якій ціллю є людський розум як поле бою. Метою є вплив на пізнавальні процеси індивіда та суспільства через інформаційні, технологічні та психологічні засоби
Когнітивна війна	NATO Innovation Hub, 2021	Стратегія конфлікту, в якій атакуються знання, переконання, сприйняття та ухвалення рішень, з метою контролю або зміни поведінки цільової аудиторії без фізичного знищення
Когнітивна війна	NATO Innovation Hub, 2021	Сукупність дій, спрямованих на вплив на процеси мислення, сприйняття та ухвалення рішень супротивника шляхом маніпулювання інформацією та емоціями
Інформаційно-психологічний вплив	Закон України "Про основи національного спротиву", 2021	Спрямований вплив на свідомість, підсвідомість, емоції, поведінку особи чи групи шляхом поширення спеціально обробленої інформації
Когнітивне маніпулювання	P.W. Singer, Emerson Brooking (LikeWar, 2018)	Прихований або напівприхований вплив на мислення та рішення особи, що створює ілюзію власного вибору, часто через соцмережі, дезінформацію та психологічні техніки

Продовження табл. 1

Термін	Автор	Визначення
Інформаційна агресія	Національна безпекова стратегія України, 2020	Систематичне використання інформаційних засобів з метою дестабілізації державних інституцій, формування паніки, ворожості чи недовіри у суспільстві
Когнітивне середовище	NATO MCDC Project (Multinational Capability Development Campaign), 2020	Сфера, у якій відбувається взаємодія і обробка інформації індивідом або групою, що впливає на прийняття рішень
Когнітивна вразливість	RAND Corporation, 2019	Стан, коли індивід або суспільство схильні до впливу внаслідок нестачі інформації, емоційного напруження або зниженого критичного мислення
Масове когнітивне зараження	R. Hassan (The Age of Disconnection, 2020)	Поширення ідей, наративів або фейків у суспільстві, що впливають на колективну свідомість і змінюють суспільну поведінку, схожу на ефект вірусу
Інформаційна перевага	Joint Publication 3-13 (США, 2012)	Стан, за якого сторона має здатність ефективніше за супротивника збирати, використовувати, розповсюджувати та захищати інформацію
Когнітивна оборона	EU Hybrid COE (Centre of Excellence for Countering Hybrid Threats), 2021	Комплекс заходів, спрямованих на підвищення стійкості суспільства до когнітивного впливу, дезінформації та маніпуляцій

Проведений аналіз дозволяє узагальнити та систематизувати ключові поняття у сфері когнітивних операцій і когнітивних війн, виявити відмінності у їхньому трактуванні в національних і міжнародних джерелах, а також визначити терміни, що потребують уточнення та уніфікації для ефективного використання у нормативно-правовій та доктринальній базі України.

Метою статті є комплексне дослідження природи та механізмів когнітивних операцій і війн у сучасному безпековому середовищі на прикладі когнітивного протистояння між росією та Україною, а також аналіз їхніх передумов і динаміки розвитку, оцінка можливих наслідків для національної та міжнародної безпеки з урахуванням сучасних викликів і загроз.

Виклад основного матеріалу

Розглянемо питання аналізу передумов проведення когнітивних операцій росії, а також формування адекватної системи захисту від когнітивних операцій росії для України. До основних сучасних передумов ведення когнітивних операцій проти росії Україною можна віднести:

стратегічні передумови. Росія системно використовує когнітивну агресію як зброю, ігноруючи міжнародне право, тому когнітивна війна стала неминучим елементом спротиву. Довгостроковий вплив на російське населення через пропаганду зробив його співучасником війни, а отже – потенційним цільовим об'єктом когнітивних впливів. Нездатність демократичних країн ефективно впливати на російську свідомість відкриває вікно для асиметричних дій з боку України;

технологічні передумови. Широке використання штучного інтелекту та big data у персоніфікованому впливі на аудиторії. Мобільність і децентралізованість каналів впливу (соцмережі, платформи) дозволяє діяти точково, обхідними шляхами та анонімно.

Військові події в онлайн-режимі дозволяють створювати наративи в реальному часі з високим емоційним ефектом;

психологічні та соціальні передумови. Фатальна інерція російського суспільства, що підтримує війну, не дозволяє змінити ситуацію лише фізичними засобами. Розшарування російського населення (бідні регіони, меншини, пригнічені спільноти) є потенційно вразливими точками для когнітивних впливів. Моральна втома та страх перед мобілізацією в рф є джерелом підживлення деструктивних наративів (бунт, дезертирство, зневіра).

Необхідність проведення когнітивних операцій проти росії з боку України викликана рядом факторів як з боку росії, так і з боку України:

по-перше, це агресивна інформаційна політика росії, яка проявляється у постійній дезінформації, історичній ревізіїї та створенні ворожих наративів щодо України як на міжнародній арені, так і всередині самої рф та окупованих територій;

по-друге, когнітивна вразливість українського суспільства як наслідок тривалого постколоніального інформаційного впливу росії, нерівномірного розвитку критичного мислення та емоційної втоми від війни;

по-третє, міжнародне суперництво в наративах, яке обумовлено тим, що Україні потрібно формувати виграшні світові історії про свою боротьбу за свободу, щоб утримувати увагу та підтримку союзників;

по-четверте, мобілізаційна слабкість рф. Росія має численні внутрішні соціальні та когнітивні розломи, які можуть бути використані (національні меншини, економічна втома, цинізм тощо);

по-п’яте, еволюція війни до когнітивного виміру, яка визначається новими театрами бойових дій, що охоплюють не лише фізичний простір, але й простір свідомості (психосфера, соціальні медіа, інтерпретація реальності).

Необхідність формування в Україні системи захисту від когнітивних операцій росії та потужного когнітивного впливу в триваючій когнітивній війні обумовлюється рядом факторів, які визначальним чином впливають на кінцевий результат когнітивного російсько-українського протистояння:

- постійна гібридна атака рф на інформаційний простір України (через соціальні мережі, “зливи”, конспірологію, пропаганду “зради”, підрив віри в командування та керівництво);
- недостатня медіаграмотність населення та низький рівень інформаційної гігієни;
- недовіра до інституцій, поширення цинізму, втома від війни – всі ці ознаки посилюють ефективність атак противника;
- інституційна слабкість України у когнітивній сфері, а саме відсутність спеціалізованого командного центру когнітивних операцій та єдиного наративного ядра на національному рівні.

Україна як держава, що постійно зазнає інформаційного та психологічного тиску з боку рф, має вибудувати потужну систему когнітивної безпеки. У табл. 2 розкрито основні сучасні компоненти системи когнітивної безпеки.

Таблиця 2

Основні компоненти системи когнітивної безпеки

Компонент	Зміст
Моніторинг і аналітика	Постійне виявлення когнітивних впливів: наративів, фреймів, емоційних хвиль
Сили когнітивного спротиву	Підрозділи або структури (в ЗСУ, СБУ, НГУ, МВС), здатні діяти активно
Стратегічні комунікації	Превентивна побудова власного наративу, здатного витісняти російський

Продовження табл. 2

Компонент	Зміст
Кібер- та AI-рішення	Автоматичне виявлення дезінформації, deepfake, бот-мереж
Освітній фронт	Системне навчання стійкості до впливу в освіті, армії, бізнесі, політиці
Міжнародна інтеграція	Залучення НАТО/ЄС до створення “щитів когнітивного захисту” (Cognitive Shields)

Нижче наведено узагальнений аналіз ключових аспектів когнітивного протистояння між російською федерацією та Україною, що активно розгорнулося після 2010 року. У табл. 3 представлено основні етапи реалізації когнітивних операцій рф проти України, їхній короткий зміст, характерні інструменти впливу, а також оцінка наслідків для національної безпеки та суспільно-політичної стабільності держави.

Аналіз основних етапів когнітивних операцій російської федерації проти України засвідчує системний, багаторівневий і довготривалий характер інформаційно-психологічного впливу, спрямованого на підрив національної ідентичності, дестабілізацію політичної системи та деморалізацію суспільства. Зміст операцій демонструє поєднання пропагандистських, інформаційно-деструктивних та гібридних технологій із використанням внутрішніх соціальних, економічних і політичних вразливостей України. Водночас причини програшу окремих операцій з боку рф свідчать про підвищення стійкості українського суспільства, зростання ролі незалежних медіа, активізацію міжнародної підтримки та розвиток національних механізмів протидії когнітивним загрозам.

Таблиця 3

Основні когнітивні операції росії проти України:
етапи, зміст, наслідки, причини програшу

Етап	Когнітивні операції рф	Зміст операцій / інструменти	Основні наслідки для України	Причини програшу України
До 2014 року (2004-2013)	Створення прокремлівського дискурсу “братніх народів”	- проросійські медіа в Україні (Інтер, 112, NewsOne); - промоція “русского мира”, “спільної історії”; - агентурна мережа в політичному та культурному середовищі	- формування вразливого інформаційного середовища; - часткове викривлення національної ідентичності населення на півдні та сході України	- відсутність доктрини інфо/когнітивної безпеки; - неспроможність створити потужні національні наративи
2014 рік (Крим та Донбас)	Операція з дезорієнтації – “Нас там нет”. Легітимізація агресії через “захист російськомовних”	- масовані кампанії через ТБ, соцмережі, ботнети; - теза про “державний переворот у Києві”; - деморалізація українських військ у Криму через родинні та ідентичні зв’язки	- пасивність міжнародної спільноти; - втрата Криму без збройного спротиву; - початок конфлікту на Донбасі	- повна відсутність протидії у сфері інформаційної безпеки; - нереактивність стратегічних комунікацій України

Продовження табл. 3

Етап	Когнітивні операції рф	Зміст операцій / інструменти	Основні наслідки для України	Причини програшу України
2014-2021	Формування деструктивної реальності (гібридна війна)	- “Мирний план” рф з одночасною війною; - роздвоєння наративу: “Україна – країна, що воює сама з собою”; - операції впливу на Захід: “втома від України”, “українська корупція”	- затягування міжнародної підтримки; - деморалізація українського населення; - утвердження тези про невирішеність конфлікту	- брак фахових команд в урядових органах; - слабка координація органів інформаційної протидії; - недовіра суспільства до влади
Січень-лютий 2022 року	Операція залякування та розгубленості перед повномасштабним вторгненням	- прогнозоване, але багатоканальне нав’язування ідеї “швидкої поразки ЗСУ”; - пропаганда “Україна не встоїть більше 72 годин”; - дезінформація через псевдоджерела та фейкові зливи	- паніка у частині населення; - евакуація іноземних дипломатів; - початкове недооцінювання вторгнення	- недостатнє роз’яснення суспільству реальних планів рф; - брак системної роботи з внутрішніми наративами
2022-2024	Операції втоми, деморалізації, розколу	- масовані ІПСО: “війна без сенсу”, “Запад бросил”, “ЗСУ не здатні звільнити Крим”; - токсичні інформаційні кампанії в соцмережах; - культивування скандалів і недовіри в тилу	- часткове зниження довіри до влади; - сплески паніки у прифронтових регіонах; - поява рухів пацифістського або капітулянтського спрямування	- занадто повільне реформування системи стратегічних комунікацій; - недостатній моніторинг TikTok/Telegram-сегментів; - брак наративного лідерства
2024-2025 (станом на 24.02.2025)	Операція “розчарування” та “багатоголосся”	- тотальне використання діпфейків, AI-генерованих фейків, псевдоаналітики; - підрив довіри до волонтерів, до мобілізаційних процесів, до військового керівництва; - кібер-атаки з елементами когнітивної маніпуляції	- зростання суспільної апатії; - часткова делегітимізація державного меседжингу; - утворення ворожих “інфо-громад” усередині країни	- відсутність єдиного центру стратегічних комунікацій; - нерозбудована національна платформа антипропаганди - відставання у когнітивних технологіях на базі штучного інтелекту

Спочатку розглянемо період перед 2014 роком та визначимо основні аспекти того, чому Україна програла когнітивну війну росії у 2014 році:

Україна до 2014 року не мала сформованої інформаційної політики, не конструювала і не поширювала власні ідеологічні рамки, тобто існували ознаки системної відсутності наративної доктринальної бази щодо когнітивного протистояння з росією;

значна слабкість державних інституцій і медіа, відсутність стратегічної комунікації, панування проросійських медіа, інерція мислення після СРСР;

потужна суспільна дезорієнтація – брак довіри до держави, поширення "нейтральних", "антидержавних", "антиєвропейських" меседжів;

росія заздалегідь розгорнула системну когнітивну атаку через агентуру, телеканали, соціальні мережі та культурні проєкти, тобто професійність когнітивних дій росії проти України наростала в геометричній прогресії на відміну від застійного стану в Україні.

До основних причин програшу когнітивної війни росії станом на початок 2014 року можна віднести: інформаційна капітуляція всередині Криму та Донбасу; втрату контролю України над телеефіром та інфраструктурою зв'язку; відсутність жодного плану стратегічної комунікації, тобто як рф діяла швидко та централізовано; відсутність когнітивної доктрини та розуміння війни нового типу; сприйняття війни тодішніми органами влади як "медійну кризу", а не війну за свідомість; дискредитацію держави після Майдану, що посилювалося російськими наративами про "нацистський переворот"; рф встигла інфільтрувати агентуру впливу в медіа, політику та церкви, що дозволило реалізувати швидкий "когнітивний бліцкриг".

Головні характеристики когнітивної війни станом на 24.02.2022:

рф розпочала повномасштабну когнітивну атаку разом із воєнною агресією через залякування, інформаційний терор, внутрішній розкол, потужні операції впливу на союзників України;

Україна демонструє потужну стратегічну комунікацію через сильні фігури (Зеленський, Залужний, дипломатичні меседжі), медійні проєкти, зростання ролі нових медіа, але продовжує існувати внутрішня загроза через зневіру, фаталізм, негативну селекцію новин, загальну втому, які ворог активно використовує.

Стан когнітивного протистояння станом на літо 2025 року

Україна і росія ведуть виснажливу когнітивну війну. Росія активно працює на розкладання тилу, внутрішньої мобілізаційної енергії, підрив довіри до командування та створення відчуття "марності спротиву". Україна поступово розгортає більш скоординовану когнітивну оборону та наступ через культурні продукти, публічну дипломатію, міжнародну присутність і протидію в медіа.

Утвердження нової ідентичності – ключовий фронт, бо це є боротьба за зміст і майбутнє України у свідомості як громадян, так і світу. Більше операцій перенесено у віртуально-соціальний простір (Telegram, TikTok, YouTube, боти, deep fake, маніпулятивні фото, меми), які сьогодні є елементами бою за свідомість.

До основних причин відставання від росії у когнітивній війні станом на 2025 рік (не йдеться про поразку у фізичній війні, а саме боротьба у когнітивному вимірі за розум, стійкість, сприйняття, правду) можна віднести наступне:

перенасичення негативом, зневіра, втома суспільства;

ворог грамотно експлуатує виснаження, втрати, скандали, корупцію, конфлікти;

поширюються меседжі: "все марно", "Захід зрадив", "Україна програла", "час домовлятися";

недостатня державна стратегічна комунікація, запізніла реакція, мовчання або бюрократичні фрази;

відсутність єдиного наративу перемоги, надії та стійкості;

провал у роботі з іноземною аудиторією, бо рф повернула собі ініціативу в багатьох країнах Глобального Півдня;

західні ЗМІ знову почали грати у “дві правди” та “обидві сторони винні”;

Україна не веде когнітивну війну всередині росії системно, бо немає чіткої програми розпаду російської свідомості та можливостей впливу на свідомість росіян та інших націй на території росії, бо це “табу” для росії – це найважливіший інструмент впливу як всередині росії, так і поза її межами;

сьогодні постійно втрачається ініціатива, бо навіть російські втрати не трансформуються у розкол чи паніку;

малоефективне використання можливостей ШІ та великих даних, хоча рф уже застосовує генеративні моделі для поширення deepfake, новин і маніпуляцій, не жаліючи на це ресурсів, адже свідомість є найціннішим пріоритетом у війні.

У табл. 4 розкрито основні характеристики триваючого когнітивного протистояння між росією та Україною.

Таблиця 4

Основні характеристики триваючого когнітивного протистояння між росією та Україною

Характеристика	росія	Україна
Головна мета	Деморалізація, дезінтеграція, хаос	Консолідація, мобілізація, підтримка
Інструменти	Пропаганда, боти, ЗМІ, страх, конспірологія	Стратком, соцмережі, дипломатія, культура
Цільова аудиторія	Українське суспільство, союзники України	Українці, західна аудиторія
Стан системи	Скоординована, централізована	Розвивається, все ще частково реактивна

Україна увійшла у фазу когнітивної війни пізно і з величезним “історичним боргом”. Війна проти росії – не лише за територію, а й за реальність, смисли, ідеї та ідентичності. Сьогодні це не просто оборона, а побудова нового когнітивного щита і меча. Перемога України залежить не лише від ракет і дронів, але й від сили слова, образу, наративу. Тому головним викликом є не лише протистояти, а й системно наступати, формуючи майбутнє в головах мільйонів. Україна, попри героїчну стійкість, сьогодні ще не створила інституціалізованої когнітивної доктрини, і тому втратила ініціативу у війні за розум – як всередині країни, так і у світі.

Когнітивна перемога – це не лише відбиття ворожої брехні, а і нав’язування власного бачення реальності, побудованого на правді, волі, моральній силі. Україна може і має це зробити, але для цього потрібна когнітивна мобілізація всього суспільства.

Проведемо аналітичне узагальнення когнітивних операцій, які реалізувала або реалізовує Україна проти росії (табл. 5), а також дамо оцінку їхнього ступеня дієвості та очікуваних результатів.

Таблиця 5

Аналітичне узагальнення щодо когнітивних операцій, які реалізувала або реалізовує Україна проти росії, а також оцінка їхнього ступеня дієвості та очікуваних результатів

Параметр	Опис
1.	*Операції з конструювання української національної ідентичності у протиставленні російській*
Ціль	Формування та посилення української політичної нації, відокремлення від “русского міра”, розвінчання колоніальних наративів
Інструменти	Освітня реформа, декомунізація, дерусифікація, мовна політика, проєкти на кшталт “Історія без брехні”, книги, фільми
Дієвість	Середня – висока. Особливо помітна після 2022 року, проте вразлива у прифронтових та тимчасово окупованих регіонах.

Продовження табл. 5

Параметр	Опис
Очікувані результати	Формування сталого культурного та інформаційного бар'єра проти впливу рф, укріплення єдності нації
2. Контрнаративи у міжнародному інформаційному просторі	
Ціль	Розвінчати фейки рф на міжнародній арені, зберегти підтримку Заходу, показати Україну як жертву та цивілізованого актора
Інструменти	Комунікація в ООН, виступи президента, англомовні медіа, українські експерти та дипломати в західних ЗМІ
Дієвість	Висока. Успішне формування глобального образу України як держави-жертви та борця за свободу
Очікувані результати	Продовження міжнародної підтримки, санкційного тиску на рф, постачання зброї
3. Викриття російських фейків та маніпуляцій в інформаційному просторі	
Ціль	Нейтралізація впливу ІПСО рф, зменшення деструктивного впливу на населення України та партнерів
Інструменти	Центр протидії дезінформації, Telegram-канали ("СБУ", "Спростуй брехню"), OSINT-розслідування
Дієвість	Середня. Є зрушення, але брак єдиної стратегії, системності, потужності розкриття у режимі 24/7
Очікувані результати	Зменшення ефективності операцій рф на внутрішньому та міжнародному рівнях
4. Когнітивна мобілізація через образ героїзму та стійкості	
Ціль	Моральна мобілізація населення, військових, створення образу незламності
Інструменти	Культура героїв (Азовсталь, Буча, Маріуполь), медіапроєкти, фільми, пісні, фото
Дієвість	Висока, особливо на початку повномасштабного вторгнення. Частково згасає через втому, руйнування, втрати
Очікувані результати	Збереження стійкості на фронті, підтримка тилу, зниження паніки
5. Цифрові ініціативи як інструмент когнітивної переваги	
Ціль	Показати перевагу України як цифрової держави над архаїчною росією
Інструменти	"Дія", цифрова держава, використання ШІ, відео в стилі SMM, звернення Зеленського, платформи United24
Дієвість	Середня – висока. Позитивне сприйняття за кордоном, формування іміджу прогресивної нації
Очікувані результати	Зміцнення міжнародного іміджу, залучення ІТ-фахівців, донатів, інвестицій
6. Військово-когнітивні операції (через дрони, відео, меми, психологічний вплив)	
Ціль	Деморалізація противника, створення страху в російському суспільстві, приниження армії рф
Інструменти	Відео ударів FPV-дронів, публікації про втрати, меми про "бавовну", висміювання "кадирівців"
Дієвість	Висока на тактичному рівні, слабша на стратегічному (через ефект заміщення втрат російською пропагандою)
Очікувані результати	Зниження бойового духу супротивника, зростання протестного потенціалу

Україна проводить когнітивні операції, що охоплюють як внутрішній, так і зовнішній простір. Їхня сила полягає в морально-психологічній мобілізації, цифровій відкритості, гнучкості та вмілому використанні сучасних комунікаційних форматів. Проте в Україні сьогодні існує ряд обмежень щодо їх успішної реалізації, а саме: відсутність єдиного стратегічного центру когнітивних операцій; нестача ресурсів на інформаційний

фронт; слабка синхронізація із військово-політичними цілями; дефіцит досліджень з питань когнітивної безпеки.

Для досягнення максимального ефекту необхідно реалізувати низку важливих заходів, а саме: централізація управління інформаційними операціями (ІО); розширення аналітичного сегменту; інтеграція психологічних, культурних та технологічних компонентів у цілісну когнітивну стратегію війни. У табл. 6 розкрито основні складові успішної реалізації когнітивних операцій, а на рис. 1 наведено результати експертного опитування щодо оцінювання ступеня їхньої важливості відносно досягнення позитивного кінцевого результату.

Таблиця 6

Основні складові успішної реалізації когнітивних операцій

№	Складова когнітивної операції	Опис	Важливість (0-1)
1	Стратегічна мета і концепція впливу	Чітке формулювання цілей, логіка когнітивного вторгнення або захисту	0,15
2	Аналіз цільової аудиторії	Детальне вивчення когнітивних вразливостей, моделей мислення, історичних наративів	0,12
3	Контентна платформа (наративи та меседжі)	Створення і поширення меседжів, адаптованих до аудиторії	0,13
4	Інфраструктура поширення (медіа, соціальні мережі)	Інструменти розгортання впливу (ЗМІ, блогери, соцмережі, ІІ, платформи)	0,12
5	Технологічна підтримка (ІТ/ІПСО/ІІ)	Аналітика соцмереж, Big Data, застосування бот-мереж, генерація фейків	0,10
6	Інформаційна перевага/доступ до каналів	Контроль чи перевага у впливових комунікаційних середовищах	0,08
7	Синхронізація з політичними/військовими діями	Узгодженість когнітивного впливу з іншими елементами державної чи воєнної кампанії	0,10
8	Оцінка ефективності (зворотній зв’язок)	Моніторинг результатів, корекція наративів, адаптація операції	0,08
9	Захист власного інформаційного середовища	Виявлення та нейтралізація ворожих когнітивних впливів, робота з уразливістю населення	0,12

Наведені результати оцінювання відображають особливості як наступальних, так і оборонних компонентів когнітивних операцій. Тобто за визначеними у табл. 6 складовими можна оцінити або планувати подібні операції, виявляючи слабкі ланки чи пріоритети для інвестицій. Найвищу вагу мають мета, аудиторія та контент, бо вони визначають саму суть когнітивної операції. Захист від контрнаративів оцінено нижче, оскільки він є реактивною, хоч і важливою складовою. Оцінка ефективності часто недооцінена в багатьох країнах, проте без неї неможливо гнучко адаптуватися, тому її слід розвивати. Серед основних складових успішної реалізації когнітивної операції є критично необхідні, без яких проведення операції є або неможливим, або гарантовано неефективним. Нижче подано поділ усіх складових на незамінні (обов’язкові), важливі та допоміжні елементи.

Критично необхідні складові (без них операція неможлива):

- наявність чіткої мети та цільової аудиторії. Без розуміння того, кого саме потрібно переконати, деморалізувати або мобілізувати, когнітивна операція втрачає сенс. Приклад: рф успішно сегментувала аудиторії в Україні у 2014 році, включаючи військових, проросійських мешканців та нейтральних, і працювала окремо з кожною групою;

- системність інформаційного впливу. Виявляється у спрямованому, безперервному та багатоетапному характері впливу через різні канали. Приклад: рф роками розвивала мережу ЗМІ, блогерів та експертів для системного впливу, на відміну від України, яка діяла ситуативно;

- операційна координація між усіма інструментами впливу (влада, ЗМІ, спецслужби, аналітики). Для успішності когнітивних операцій критично важлива інтеграція всіх ланок – від аналітики до тактичних медіарішень. Без цього ефекти нівелюються або можуть суперечити одне одному.

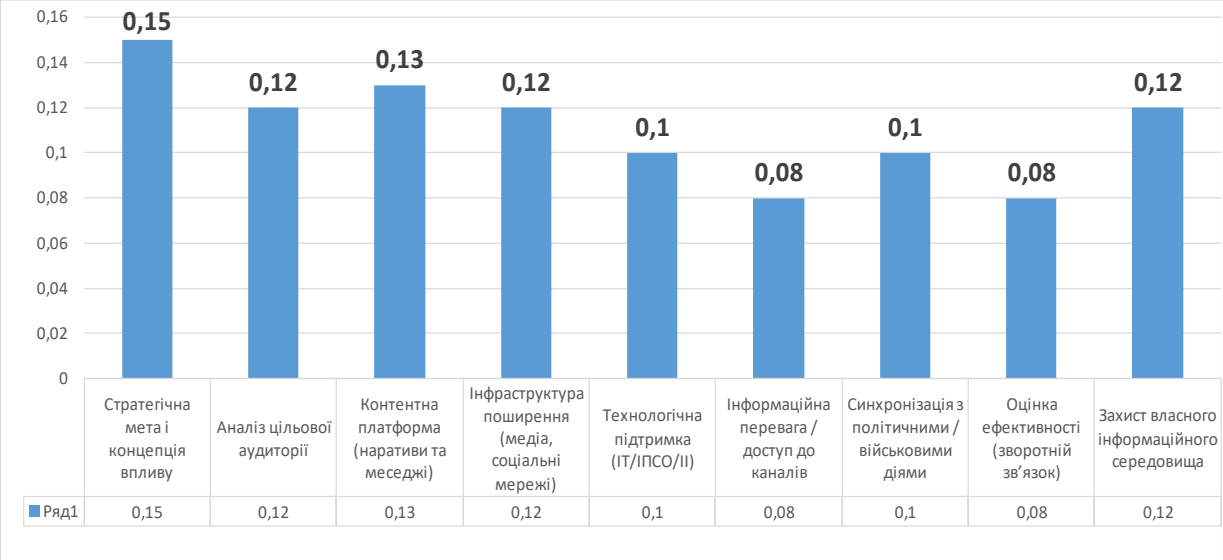


Рис. 1. Результати експертного оцінювання ступеня важливості основних складових успішної реалізації когнітивних операцій

Важливі складові (без них можливо, але значно знижується ефективність):

- контроль або проникнення в інформаційне середовище противника, що проявляється через можливість впливати не лише на власну аудиторію, а й на аудиторію ворога. Приклад: обмежений вплив українських меседжів на російське населення через жорстку цензуру в рф;

- експертне та фактологічне забезпечення (наративи, тези, меседжі), а саме створення довготривалих концептів, які працюють проти ворожих наративів. Україна часто програє через слабке стратегічне меседжування, що сприяє домінуванню емоційного, ситуативного контенту.

Допоміжні складові (підсилюють, але не є критичними):

- технічна та цифрова перевага (ботмережі, генерація контенту, BigData-аналітика). Технології посилюють вплив, але не замінюють ідеї та мету;

- психолого-культурне проникнення в логіку мислення аудиторії противника. Важливо для довгострокового впливу (через гумор, мову, кодові слова). Приклад: українські меми або проєкти типу "єППО", "Бавовна" мають ефект, але без мети вони розчиняються;

- здатність адаптувати операцію до змін ситуації (гнучкість). Можливість змінювати хід дій під нову обстановку, що робить кампанію живою. РФ уміє гнучко змінювати меседжі (від "нас там нема" до "ми відвоюємо святу Русь").

Критично важливими складовими, без яких когнітивну операцію неможливо реалізувати, є: наявність мети та цільової аудиторії; системність дій; операційна координація між усіма ланками впливу. Без цих трьох компонентів будь-яка операція залишиться фрагментарною, незрозумілою, неефективною або навіть контрпродуктивною.

Україна має серйозно інституціоналізувати саме ці три речі, щоб перейти від ситуативної комунікації до системної когнітивної боротьби.

Успішна реалізація когнітивної операції передбачає не лише досягнення інформаційної або психологічної переваги, а й глибоке перетворення способу мислення, прийняття рішень та поведінкових моделей цільової аудиторії. Очікувані наслідки операції можна класифікувати за рівнями впливу:

1. Стратегічний рівень

а) Підрив волі до спротиву у противника – формування у ворожого суспільства переконання у неминучості поразки, безглуздості війни, недовіри до власного керівництва.

б) Деморалізація політичного та військового керівництва – примушення до помилкових рішень або бездіяльності через дезінформацію, ілюзії чи хибне сприйняття ситуації.

в) Формування підтримки на міжнародному рівні – переконання ключових зовнішніх акторів у правоті власної позиції, делегітимізація позицій ворога.

2. Оперативний рівень

а) Руйнування внутрішньої єдності противника – створення недовіри між армією, суспільством та політиками; підтримка сепаратизму або внутрішнього розколу.

б) Зниження боєздатності військ через інформаційне перевантаження та дезорієнтацію – поширення хибної інформації, що унеможливлює ефективне командування та реагування.

3. Тактичний / суспільно-психологічний рівень

а) Формування необхідних емоційних станів у противника – паніка, розгубленість, депресія, втома, агресія, апатія, байдужість.

б) Маніпуляція масовою свідомістю – нав'язування власних наративів, зміна оцінки подій (наприклад: "нас ніхто не підтримує", "уряд нас зрадив", "ворог не такий вже й небезпечний").

в) Стимулювання масової підтримки власних дій серед нейтральної або противної аудиторії шляхом використання культурних, релігійних, гуманітарних або етичних аргументів для впливу на громадську думку.

4. Поведінкові наслідки (кінцева мета)

а) Зміна або руйнування моделей поведінки противника.

б) Змусити противника діяти у спосіб, вигідний оператору операції.

в) Створення нових стійких переконань, які змінюють сприйняття війни, цілей або засобів її ведення.

Основними ефектами для власної аудиторії є: консолідація суспільства; підвищення бойового духу; легітимація власної політики; мобілізація ресурсів.

Для комплексного розуміння характеру та спрямованості когнітивних операцій доцільно проаналізувати їхні передбачувані результати, інтенсивність впливу та кінцеві цілі, що переслідує агресор. У табл. 7 подано систематизовану інформацію щодо основних очікуваних наслідків таких операцій, визначено рівень їхнього впливу на ключові сфери життєдіяльності держави та суспільства, а також окреслено кінцеві стратегічні завдання, досягнення яких прагне ініціатор операції.

Таблиця 7

Основні очікувані наслідки когнітивних операцій України

Очікуваний наслідок	Рівень впливу	Ціль
Деморалізація противника	Стратегічний	Послаблення волі до боротьби
Порушення управління та прийняття рішень	Оперативний	Зниження ефективності дій супротивника
Формування підтримки серед міжнародної аудиторії	Стратегічний	Отримання переваги в геополітичному середовищі

Продовження табл. 7

Очікуваний наслідок	Рівень впливу	Ціль
Руйнування єдності в суспільстві противника	Оперативний	Створення внутрішньої нестабільності
Нав'язування власних наративів (переінтерпретація реальності)	Тактичний / психологічний	Зміна сприйняття та оцінки подій
Формування очікуваної поведінки противника	Поведінковий	Примус до дій, вигідних ініціатору операції
Підвищення бойового духу власного суспільства	Підсилювальний	Зміцнення власної внутрішньої стійкості

Програш України у когнітивній війні з росією як у стратегічному, так і в тактичному вимірах, несе системну загрозу національній безпеці, стійкості суспільства, легітимності влади, а також ефективності оборони й мобілізації. Наслідки такого програшу варто розглядати в часовій перспективі, а саме:

1. Короткострокова перспектива (1–2 роки).

Внутрішні наслідки (ризики): поглиблення внутрішнього розколу в суспільстві; ескалація недовіри до інститутів державної влади, ЗС України, командування та волонтерських ініціатив; активізація проросійських наративів через дезінформацію, маніпуляції фактами та "втому від війни"; зниження мотивації до мобілізації та спротиву через втрату віри у доцільність спротиву; емоційне виснаження, дефетизм, відмова служити та міграція населення.

Зовнішньополітичні наслідки (ризики): послаблення підтримки України в західному медіа-просторі через недопрацювання в міжнародних когнітивних операціях; вплив російських наративів на політичні рішення урядів країн-партнерів; посилення інформаційного впливу рф через стабільне просування тез про "втому Заходу", "недемократичну Україну", "неминучість компромісу" та "безперспективність наступу".

2. Середньострокова перспектива (3–4 роки).

До основних наслідків середньострокового періоду належать:

- розмиття національної ідентичності через деукраїнізацію культурного простору, тобто молодь дедалі частіше обирає нейтральну або проросійську позицію (через соцмережі, вплив російської мови/контенту);
- деморалізація суспільства шляхом зростання апатії, пасивності, політичного нігілізму та втрата ціннісної цілісності (люди не розуміють, за що боротись);
- руйнування мобілізаційного потенціалу, а саме: система оборони не зможе відновлювати свої ресурси; деградація відношення до служби та нарощування ідеї "армія не для мене", яка стане мейнстрімом;
- параліч стратегічного мислення керівництва держави, яке перестає формувати ініціативу, віддає перевагу реактивним діям;
- брак когнітивної переваги на рівні стратегічного планування.

3. Довгострокова перспектива (5+ років)

До основних наслідків довгострокового періоду належать:

- капітуляція у "м'якій" формі (когнітивно-цивілізаційна), що проявляється у поступовій втраті суб'єктності України та можливій згоді на мир на умовах рф (через внутрішній тиск населення, вплив зовнішніх сил);
- консервація корупційної та неефективної державності, бо без перемоги в когнітивній війні неможливо побудувати ефективні інституції, адже їхня легітимність постійно підривається зовнішньо та внутрішньо;

- іституційна дестабілізація, яка проявляється через регулярні внутрішньополітичні кризи, зміни урядів, вуличні протести під впливом інформаційно-психологічних операцій рф;

- зменшення шансів на інтеграцію до ЄС і НАТО через те, що захід не сприйматиме Україну як стабільного партнера з високим рівнем резильєнтності;

- повзуча реінтеграція з росією, яка обумовлюється впливом рф через "миротворчі" організації, проросійські медіа, "зелену" економіку, енергетику, релігійні інституції тощо.

Програш України в когнітивній війні з росією – це не просто поразка в інформаційній сфері, а загроза втрати державності в новому, гібридному вигляді. Замість танків – наративи, замість ракет – сенси, замість десанту – алгоритми впливу на свідомість. Без системного перегляду підходів до когнітивної безпеки Україна ризикує програти війну, навіть за наявності можливостей виграти її на полі бою.

Висновки

Отже, когнітивна війна сьогодні є одним із ключових вимірів сучасного безпекового середовища, де битва за свідомість, уявлення і волю населення стає не менш важливою, ніж традиційні бойові дії. Російсько-українська війна (з 2014 року) демонструє, що успіх чи поразка в когнітивному просторі визначає не лише імідж держави на міжнародній арені, а й безпосередню здатність країни захищати свою територіальну цілісність та національну ідентичність. Когнітивна війна – це війна за свідомість, де інформація, наративи та смисли стають головними бойовими інструментами. Перемога у цій війні є ключовою умовою для досягнення загальної перемоги України у гібридному конфлікті з росією. Тільки системний, скоординований, інноваційний підхід до когнітивної безпеки здатен зламати перевагу ворога і забезпечити стійкість українського суспільства та держави в умовах сучасних викликів.

Матеріали дослідження можуть бути використані як аналітична основа для удосконалення нормативно-правової бази та стратегічних документів у сфері національної безпеки, підготовки навчально-методичних матеріалів для сил безпеки та оборони, а також розробки комплексних програм протидії когнітивним загрозам.

Подальші дослідження можуть включати: поглиблений аналіз інструментарію когнітивних операцій у кіберпросторі; оцінку ефективності національних механізмів стійкості; вивчення міжнародного досвіду протидії когнітивним загрозам; розробку рекомендацій щодо інтеграції сучасних технологій, зокрема штучного інтелекту, у системи захисту від когнітивних впливів.

Список літератури

1. Горбулін В. Гібридна війна як ключовий інструмент російської геостратегії реваншу. URL: www.niss.gov.ua/public/File/2015_book/012315_Gorbulyn.pdf.
2. Семененко О., Горбатюк В., Тарасов О., Столінець С., Мусієнко В., Прохорський С. Система когнітивного впливу Російської Федерації на Україну та аудиторії інших держав: безпековий вимір. *Соціальний розвиток і безпека.* 2025. № 15 (1). С. 26–43. URL: https://doi.org/10.33445/sds.2025.15.1.4.
3. Maksymenko S.D., Derkach L.M. Understanding modern cognitive war in the global dimension, its genesis in the Ukrainian context: review and directions for future research. *Obrana a Strategie.* 2023. № 23 (1). P. 126–148. URL: https://doi.org/10.3849/1802-7199.23.2023.01.126-148.
4. Taranenko A. Cognitive security as a dimension of Russia-Ukraine war. *Politology Bulletin (National University of Kyiv-Mohyla Academy).* 2024. № 92. P. 371–382. URL: https://doi.org/10.17721/2415-881x.2024.92.371-382.
5. Назар М.М., Зінченко О.В. До питання психологічної структури фейків під час російсько-української війни. *Віртуальний освітній простір: психологічні проблеми* : зб. тез доп. XII міжнар.

наук.-практ. конф., Інститут психології імені Г. С. Костюка НАПН України, м. Київ, 2024. URL: https://lib.iitta.gov.ua/id/eprint/742707/.
6. Krainikova T., Prokopenko S. Waves of disinformation in the hybrid Russian-Ukrainian war. *Current Issues of Mass Communication*. 2023. № 33. URL: https://cimc.knu.ua/.
7. Danyliuk I., Bohucharova O. The Russia-Ukraine war in Western media: a psycholinguistic modelling of the "hybrid" phase. *East European Journal of Psycholinguistics*. 2023. № 10 (2). URL: https://doi.org/10.29038/eejpl.2023.10.2.dan.
8. Bugayova N., Stepanenko K. A primer on Russian cognitive warfare. Foreign Policy (adapted). Aug. 1 2025. URL: https://foreignpolicy.com.
9. Mejova Y., Capozzi A., Monti C., De Francisci Morales G. Narratives of War: Ukrainian Memetic Warfare on Twitter. Sep 2023. URL: https://arxiv.org/abs/2309.08363.
10. Makhortykh M., Baghumyan A., Vziatysheva V., Sydorova M., Kuznetsova E. LLMs as information warriors? Auditing how LLM-powered chatbots tackle disinformation about Russia's war in Ukraine.
11. Gouliev Z. Propaganda and Information Dissemination in the Russo-Ukrainian War: NLP of Russian and Western Twitter Narratives.
12. Wang L., Wang R. Cyber warfare: a study of Zelenskyy's social media political performance strategies and effects. *Frontiers in Psychology*. 2024. URL: https://doi.org/10.3389/fpsyg.2024.1478639.
13. Cigar N. The Russian Military's Biological Warfare Disinformation Campaign and the Russo-Ukrainian War. *The Journal of Slavic Military Studies*. 2024. № 36 (4). P. 361–409. https://doi.org/10.1080/13518046.2023.2305511.
14. Wikipedia-записи про гібридну війну, соцмережі та інформаційні операції: Russian hybrid warfare in Europe, Ukrainian information war against Russia, Social media in the Russo-Ukrainian War.
15. Neisser U. Cognitive Psychology. New York: Appleton-Century-Crofts, 1967.
16. US Department of Defense. Joint Doctrine Note 3-13: Operations in the Information Environment. Washington, DC: Joint Chiefs of Staff, 2018.
17. Carr C. Cognitive attacks: how disinformation targets the brain. *Journal of Information Warfare*. 2020. № 19 (1). P. 45–58.
18. Direction Générale des Relations Internationales et de la Stratégie (DGRIS). La guerre cognitive: La nouvelle menace stratégique. Ministère des Armées, République Française, 2020.
19. RAND Corporation. (Cook, B. et al.). Cognitive Vulnerabilities and Information Warfare. Santa Monica, CA: RAND, 2019.
20. NATO. Allied Joint Publication AJP-3.10.1: Allied Joint Doctrine for Psychological Operations. NATO Standardization Office, 2021.
21. NATO Innovation Hub. Cognitive Warfare: The Battle for Your Brain. Norfolk, VA: NATO ACT, 2021.

УДК 355.40 DOI: 10.63978/3083-6476.2025.2.2.04

Семенюк Юрій Володимирович
кандидат політичних наук
начальник кафедри
Національний університет оборони України
Київ, Україна
e-mail: snik71083@gmail.com
ORCID: 0000-0002-9415-4427

ТРАНСФОРМАЦІЯ МІЖНАРОДНИХ ВІДНОСИН ТА РОЗВІДУВАЛЬНА ДІЯЛЬНІСТЬ

Анотація. *Розглянуто трансформацію міжнародних відносин як чинник впливу на розвідувальну діяльність. Наведено, що трансформація міжнародних відносин – це глибока зміна у системі взаємодій між державами, міжнародними організаціями та іншими суб'єктами на глобальному рівні. Показано, що існуюча система міжнародних відносин і безпековий простір, не витримавши гібридних викликів і загроз XXI століття, переживають фундаментальну трансформацію. Це, в свою чергу, призвело до формування нової глобальної архітектури безпекового простору і середовища міжнародних відносин. В умовах сучасних глобальних викликів і загроз міжнародній і національній безпеці відбулася трансформація геополітичного простору, яка виявила низку політичних, безпекових, економічних та гуманітарних проблем, які неможливо адекватно оцінити й подолати виключно на рівні окремо взятої держави. Їхнє вирішення лежить у міжнародній політичній площині та у сформованому державами-глобалізаторами міжнародному просторі безпеки.*

Ключові слова: *трансформація, міжнародні відносини, безпековий простір, глобалізація, вплив, розвідувальна діяльність.*

Semeniuk Yurii
PhD of Political Sciences
head of the department
National University of Defense of Ukraine
Kyiv, Ukraine
e-mail: snik71083@gmail.com
ORCID: 0000-0002-9415-4427

TRANSFORMATION OF INTERNATIONAL RELATIONS AND INTELLIGENCE OPERATIONS

Abstract. *The article examines the transformation of international relations as a factor influencing intelligence activities. It argues that the transformation of international relations is a profound change in the system of interactions between states, international organizations, and other actors at the global level. It is shown that the existing system of international relations and security space, unable to withstand the hybrid challenges and threats of the 21st century, is undergoing a fundamental transformation. This, in turn, has led to the formation of a new global architecture of security space and the environment of international relations. In the context of contemporary global challenges and threats to international and national security, a transformation of the geopolitical space has taken place, revealing a number of political, security, economic, and humanitarian problems that cannot be adequately assessed and overcome solely at the level of individual states. Their solution lies in the international political sphere and in the international security space formed by globalizing states. The 21st century has seen the restoration of a great power, imperial type of geopolitical consciousness, which, based on the experience of the*

historical past, offers the ideal of state development in the form of the creation of "great empires" and mechanisms for their domination over 'medium' and "small" states. This is primarily characteristic of the Russian Federation and the People's Republic of China, which are trying in various ways to implement the idea of a "great power renaissance". Russia's unprovoked large-scale invasion of Ukraine confirmed that the era of interstate competition and conflict is not a thing of the past, but has instead become a defining feature of the current era. Researchers and experts in intelligence, taking into account the "revolutionary changes" in the security environment, in the nature of threats and peace, as well as changes in the nature of warfare, emphasizing the changing nature of information, the speed of technological change, and the variability of expectations not only of consumers of intelligence information but also of society, have begun to talk about the need for a "revolution in intelligence".

Keywords: *transformation, international relations, security space, globalization, influence, intelligence activities.*

Вступ

Постановка проблеми. Трансформація міжнародних відносин – це глибока зміна у системі взаємодій між державами, міжнародними організаціями та іншими суб'єктами на глобальному рівні. Вона охоплює переосмислення традиційних підходів, появу нових акторів та викликів, а також перерозподіл впливу у світі. Активні геостратегічні діючі актори активізують діяльність за межами своїх національних кордонів з метою зміни геополітичної ситуації у напрямі побудови нового світоустрою. Тому турбулентність і напруга в глобальній політиці та економіці продовжують наростати. Існуюча система міжнародних відносин і безпековий простір, не витримавши гібридних викликів і загроз XXI століття, нині переживають фундаментальну трансформацію. Це, в свою чергу, призвело до формування нової глобальної архітектури безпекового простору і середовища міжнародних відносин.

Аналіз останніх досліджень і публікацій. Проблемі трансформації міжнародних відносин та її впливу на економіку, політику і інформаційний простір присвячені наукові праці як зарубіжних, так і вітчизняних дослідників [1-9], однак питання впливу на розвідувальну діяльність залишаються недостатньо дослідженими.

Мета статті – розглянути трансформацію міжнародних відносин як чинник впливу на розвідувальну діяльність.

Виклад основного матеріалу

В умовах сучасних глобальних викликів і загроз міжнародній і національній безпеці відбулася трансформація геополітичного простору, яка виявила низку політичних, безпекових, економічних та гуманітарних проблем, які неможливо адекватно оцінити й подолати виключно на рівні окремо взятої держави [3]. Їхнє вирішення лежить у міжнародній політичній площині та у сформованому державами-глобалізаторами міжнародному просторі безпеки [4].

Реальністю XXI ст. стала реставрація великодержавного, імперського типу геополітичної свідомості, який, опираючись на досвід історичного минулого, пропонує ідеал державного розвитку у вигляді створення "великих імперій" та механізмів їхнього домінування над "середніми" та "малими" державами, а також недержавними політичними силами [5]. В першу чергу це властиво рф та КНР, які в умовах XXI ст. у різний спосіб намагаються практично реалізувати задум "великодержавного ренесансу" [6]. При цьому слід враховувати, що в постмодерних умовах великодержавницька геополітична свідомість зазнала змін: її орієнтація на максимально можливе територіальне домінування приховується інформаційним шумом щодо необхідності конструювання "великих політичних просторів", здатних створити кращі умови задля задоволення соціально-економічних, політичних, культурних та інших потреб покірних народів і націй (останнім не забороняється мати власну "декоративну" державність, межі якої мають

регулюватися новітньою метрополією) [7]. Неспровоковане широкомасштабне вторгнення росії в Україну підтвердило, що ера міждержавного змагання та конфліктів не відійшла в минуле, а стала визначальною характеристикою нинішньої епохи [8].

Показово, що з початком XXI ст. дослідники та експерти з розвідувальної діяльності, взявши до уваги "революційні зміни" в безпековому середовищі, у природі загроз та миру, як і зміни в характері воєн, наголосивши на мінливості характеру інформації, швидкості технологічних змін, варіативність очікувань не лише споживачів розвідувальної інформації, але й суспільства, заговорили про необхідність "революції у розвідці" [9].

Зокрема, у Національній розвідувальній стратегії США, опублікованій у серпні 2023 року, визначено шість основних напрямів розвитку Розвідувального співтовариства (РС) США, а саме:

– посилення ролі розвідки у зв'язку із загостренням стратегічної конкуренції між США, Китаєм та росією. Означено, що лише КНР має і наміри, і спроможності конкурувати зі США, а рф є джерелом постійної загрози регіональній безпеці в Євразії, а також дестабілізаційним чинником глобального рівня. У контексті стратегічної конкуренції основним завданням РС США є забезпечення лідерства США у сфері технологій та інновацій, насамперед через розвідку з відкритих джерел, роботу з біг-дата, штучний інтелект (ШІ) і поглиблену аналітику. Для цього РС США має активізувати співпрацю із союзницькими та партнерськими розвідками, а також із громадським і приватним сектором;

– пошук, професійний розвиток та утримання на службі талановитих співробітників РС США. Найбільш цінними є технічно підготовлені та обдаровані кадри, які через організаційно-бюрократичні та інші обмеження або не можуть працевлаштуватися в розвідці, або звільняються після нетривалого періоду служби. Щоб пришвидшити прийом на роботу, планується модернізувати систему відбору та працевлаштування співробітників РС США, а щоб підвищити рівень професійного розвитку, вважається доцільним і надалі практикувати спільні місії для представників різних розвідувальних органів, які братимуть у них участь на ротаційній основі;

– розробка інтероперабельних та інноваційних рішень для формування нових спроможностей РС США. Це передбачає створення уніфікованих підрозділів, які відповідають за закупівлю необхідного майна та обладнання; запровадження централізованої автоматизованої системи постановки запитів на закупівлю та єдиної системи укладення контрактів на виконання робіт. Успіх забезпечується формуванням корпоративної культури, спрямованої на пошук нових інструментів, процесів та стандартів, що допомагають виконувати трудомісткі завдання завдяки продуктивній взаємодії людини з машиною (штучним інтелектом). Принцип датацентричності передбачає підвищення доступності та стандартизації розвідувальної інформації, а також спроможностей пошуку і добування конкретних даних із наявних обсягів інформації, що потребує інтеграції науково-дослідних, технічних, аналітичних і добувних підрозділів РС США;

– розширення, диверсифікація та посилення партнерства у сфері розвідки. Створення мережі союзників і партнерів підвищує операційні та аналітичні спроможності РС США. Важливо активізувати обмін розвідувальною інформацією на регіональному та локальному рівнях, а також удосконалити процедури обміну інформацією з недержавними та субнаціональними установами, оскільки їхня роль суттєво зросла, особливо у сфері захисту критичної інфраструктури від кіберзагроз;

– підвищення рівня експертизи щодо транснаціональних викликів, таких як кліматичні зміни, контрабанда наркотиків, фінансова криза, порушення ланцюгів поставок, корупція, невідомі хвороби, проривні технології. РС США планує залучати

кращих експертів із високим рівнем обізнаності у відповідних сферах для формування пропозицій щодо стратегічних рішень керівництвом держави;

– забезпечення стійкості функціонування РС США. Це передбачає модернізацію та розширення розвідувальної інфраструктури, що підвищує спроможності раннього виявлення та попередження найбільш небезпечних загроз, таких як пандемії, масовані кібератаки, кліматичні зміни й терористичні акти. Водночас розвідувальна інфраструктура має забезпечувати не лише стійке функціонування розвідки, а й можливість завдання ударів у відповідь та швидкого відновлення в разі нападу.

У контексті цифровізації розвідувальної діяльності заслуговує на увагу прийнята в липні 2023 року Дата-стратегія РС США на 2023-2025 роки, яка висвітлює основні напрями політики цифровізації РС США.

Основні напрями реалізації Дата-стратегії РС США:

– застосування принципу E2E (віч-на-віч) у дата-менеджменті, що передбачає детальне планування, розробку та реалізацію єдиних процедур збору, обробки, розподілу та використання інформації. Для цього буде впроваджено єдиний формат розвідувальних даних (тегів чи міток) для подальшої обробки за допомогою ШІ та стандарти генерування, обміну, розподілу, доведення та захисту інформації;

– забезпечення інтероперабельності (взаємосумісності) даних для своєчасного доведення їх до потрібного споживача. Передбачає зміну парадигми управління розвідкою з системно-центричної на датацентричну. Якщо раніше основним завданням було створення інформаційної архітектури (комп'ютери, сервери, мережі тощо), то нині фокус управління спрямовано на процедури збору, аналізу та розподілу інформації із використанням ШІ. Датацентричний підхід має поліпшити якість розвідувальної інформації, поглибити її інтеграцію, підвищити точність інтерпретації та інтероперабельність. Застосування ШІ має скоротити час збору й обробки необхідної інформації з тижнів/днів до годин/хвилин;

– розвиток партнерства у сфері цифрових інновацій, що передбачає активну співпрацю РС США з іноземними розвідками, цивільними установами та академічними колами для кращого розуміння інформаційних технологій і реагування на зміни в їхньому розвитку. Варто наголосити на тому, що до цього часу співпраця РС США з приватним сектором та науковцями не мала такого важливого значення з огляду на стрімкість цифрової революції, насамперед у сфері ШІ;

– підвищення дата-грамотності співробітників розвідки. Перехід до датацентричної моделі розвитку РС США неможливий без зміни системи освіти, курсової та професійної підготовки співробітників розвідки в контексті усвідомлення того, що робота з даними – це основа успішного виконання будь-якої місії (завдання). Дата-грамотність визнається однією з ключових професійних компетентностей як пересічних виконавців, так і старших керівників розвідки.

Висновки

Таким чином, незважаючи на те, що сутність розвідувальної діяльності впродовж багатьох років залишалася майже незмінною, унаслідок суттєвих змін у розвитку оперативної обстановки та впровадження технологічних інновацій її організація, процеси та матеріальні ресурси постійно еволюціонують. Саме завдяки прогресивним військовим технологіям стало можливим добувати значні обсяги даних, швидко та точно обробляти їх і надавати оперативну розвідувальну інформацію військовому керівництву. Ця інформація відіграє вирішальну роль у виробленні прогнозних оцінок щодо подальших кроків і можливостей противника, а також для визначення потенційних загроз. Крім того, технологічний прогрес стає головним чинником не лише зміни конфігурації світового порядку, а й стратегій військових операцій.

Список літератури

1. Zbigniew Brzezinski. The Grand Chessboard. American Primacy and Its Geostrategic Imperatives. *Basic Books*. 2016. P. 39–41.
2. Shin Joung Yeo. Geopolitics of search: Google versus China? *Media, Culture & Society*. 2016. Vol. 38 (4). P. 1045–1057.
3. Гурковський В., Колесник В., Бажора О. Трансформація міжнародних відносин: виклики та загрози світовій безпеці. *Публічне урядування*. 2020. № 4 (24). С. 74–93.
4. Поліщук І. Глобалізація як провідна тенденція розвитку сучасних міжнародних відносин. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2023. № 1 (15). С. 195–203.
5. Павленко Д. Г., Семенюк Ю. В., Лисецький Ю. М. Міждержавні протистояння. Нові реалії. *Держава і право. Збірник наукових праць. Серія: Політичні науки.* 2021. № 89. С. 249–257.
6. Семенюк Ю. В., Лисецький Ю. М. Геополітичний трикутник. *Держава і право.* 2024. Вип. 95. С. 223–232.
7. Гридасова Г. Трансформація акторів міжнародних відносин: держава та транснаціональні медійні корпорації. *Наукові записки*. 2018. № 3 (71). С. 369–376.
8. Ткачук А. П. Трансформація міжнародних відносин в умовах збройної агресії Російської Федерації проти України. *Наука і оборона*. 2023. № 1. С. 27–32.
9. Семенюк Ю. В., Мокляк С. П., Лисецький Ю. М. Розвідувальна діяльність і міжнародні відносини. Нові реалії та підходи : монографія / за заг. ред. Ю. М. Лисецького. Київ : ЛАТ&К, 2021. 160 с.

УДК 351.011:001.89 DOI: 10.63978/3083-6476.2025.2.2.05

Хлонь Сергій Євгенович
кандидат історичних наук
заступник командира
Військова частина А4983

Ковальчук Андрій Іванович
доктор філософії в галузі географії
старший офіцер відділу дослідження
розвитку Сил підтримки
Військова частина А4983
ORCID: 0000-0001-6448-4727

НЕОБХІДНІСТЬ УТВОРЕННЯ НАУКОВОЇ УСТАНОВИ СИЛ ПІДТРИМКИ ЗБРОЙНИХ СИЛ УКРАЇНИ В КОНТЕКСТІ СУЧАСНИХ ВОЄННИХ ВИКЛИКІВ

Анотація. *У статті обґрунтовано необхідність утворення наукової установи Сил підтримки Збройних Сил України з огляду на динамічні зміни в способах ведення бойових дій та застосування противником нових зразків озброєння та військової техніки. Метою майбутньої наукової установи є забезпечення якісного виконання пошукових, теоретичних та експериментальних досліджень у сферах інженерної, ХБРЯ захисту, геопросторової, гідрометеорологічної та кінологічної підтримки. Аналізується поточна обмеженість наукового потенціалу існуючих наукових підрозділів установ, що провадять свою діяльність в інтересах Сил підтримки Збройних Сил України та підкреслюється, що створення нового наукового центру в системі наукових установ Міністерства оборони України сприятиме швидкій нейтралізації загроз, що виникають перед українськими військами. Досвід країн-членів НАТО також розглядається для підтвердження важливості розвитку цих напрямків підтримки.*

Ключові слова: *наукова установа Сил підтримки Збройних Сил України, інженерна підтримка, ХБРЯ захист, геопросторова підтримка, гідрометеорологічна підтримка, кінологічна підтримка, виклики сучасності на полі бою.*

Sergii Khlon
PhD of Historical Sciences
Deputy commander Military unit A4983

Andrii Kovalchuk
PhD of Geographic Sciences
Senior officer of the department for research and development of Support Forces
Military unit A4983
ORCID: 0000-0001-6448-4727

ESTABLISHING A RESEARCH INSTITUTION FOR THE SUPPORT FORCES OF UKRAINE'S ARMED FORCES IN RESPONSE TO MODERN MILITARY CHALLENGES

Abstract. *The article provides a comprehensive justification for the urgent necessity of establishing a state scientific institution for the Support Forces of the Armed Forces of Ukraine. This need is dictated by the profound and*

dynamic changes in the methods of warfare, as observed in modern armed conflicts, and the enemy's rapid deployment of new, technologically advanced weapons and military equipment. These factors create persistent challenges for the Armed Forces of Ukraine, necessitating a structured and agile response.

The primary objective of this new scientific institution is to ensure the high-quality execution of a wide range of exploratory, theoretical, and experimental research. This research is designed to cover critical support areas that are paramount for the combat readiness of the Support Forces. These areas include:

Engineering support, encompassing the development of innovative fortification techniques, mine-laying and breaching technologies, and methods for overcoming various obstacles, as well as Chemical, Biological, Radiological, and Nuclear (CBRN) defense, which involves enhancing detection, monitoring, and personnel protection systems to counter evolving threats. It will also conduct research, focused on Geospatial support, focused on the creation of high-precision geospatial data, the refinement of digital mapping technologies, and the effective use of Global Navigation Satellite Systems (GNSS) and Unmanned Aerial Vehicles (UAVs) for data collection and navigational purposes, as well as Hydrometeorological support, aimed at improving systems and technical means for providing accurate meteorological forecasts and assessing their impact on weapon system effectiveness. The institution will also conduct research on the topic of canine support, dedicated to developing doctrinal documents and modernizing training methods to enhance the operational efficiency of canine units in combat scenarios.

The article analyzes the current limitations of the scientific potential within existing units and institutions, highlighting that their insufficient specialization and capacity hindering a swift response to modern threats. The establishment of a new, dedicated scientific institution is therefore argued to be crucial for consolidating scientific efforts and enabling the rapid neutralization of emerging challenges. The research also draws upon the experience of NATO member countries to underscore the strategic importance of these support functions. This alignment with international standards is vital for ensuring the interoperability and future cooperation of Ukrainian forces with allied partners.

Keywords: *scientific institution for the Support Forces of the Armed Forces of Ukraine, engineering support, CBRN defense, geospatial support, hydrometeorological support, canine support, modern battlefield challenges.*

Вступ

Постановка проблеми. Сучасні воєнні конфлікти, особливо повномасштабна російсько-українська війна, характеризуються безпрецедентною динамікою змін у прийомах і способах ведення бойових дій, а також постійним випробуванням та застосуванням противником нових зразків озброєння та військової техніки (ОВТ) безпосередньо на полі бою. Асиметрична війна, в поєднанні із застосуванням усіх доступних ресурсів рф та її сателітів, це мало досліджене явище в сучасному світі. Дієві методи та засоби протидії гібридним агресіям мають бути розроблені враховуючи перебіг російсько-української війни. Використання досвіду повномасштабних бойових дій, збір та узагальнення такого досвіду, визначення нагальних потреб у науковій і науково-технічній продукції, – це питання, які є вагомою складовою для підтримання та розвитку спроможностей Сил оборони України. Для вирішення цих задач фаховий та своєчасний оперативний науковий супровід та розробка контрзаходів стануть вагомим позитивним внеском для забезпечення ефективності дій Сил оборони України. Існуюча структура наукових підрозділів установ, що провадять свою діяльність в інтересах Сил підтримки Збройних Сил України, має незначну штатну чисельність та повне наукове завантаження персоналу, що не дозволяє забезпечити виконання всього спектру наукових завдань за напрямками Сил підтримки Збройних Сил України, особливо на оперативному та тактичному рівнях. Це створює критичну прогалину у здатності швидко реагувати на нові виклики та загрози. Обмеженість ресурсів як людських, так і матеріальних, вимагає чіткого визначення реальної потреби у науковій та науково-технічній продукції. В умовах війни на виснаження, в якій опинилась наша держава, критично важливим є максимально ефективне провадження наукової і науково-технічної діяльності.

Аналіз останніх досліджень і публікацій. Успіхи на полі бою сьогодні у значній мірі залежать від можливостей випереджати противника в технологічному розвитку та швидкості впровадження інновацій у ланцюгу “наука (розробка) – виробництво – застосування”.

Водночас, комплексний підхід до наукового забезпечення застосування саме Сил підтримки Збройних Сил України та координація відповідних досліджень залишаються недостатньо вивченим. Аналіз стану функціонування системи розвитку спроможностей за напрямками військ (Сил), а зокрема, за напрямками Сил підтримки [1; 7; 13] Збройних Сил України, показує ряд проблемних питань, що потребують проведення комплексу скоординованих фундаментальних та прикладних досліджень. Діючі наукові та науково-дослідні установи Міністерства оборони України, що здійснюють свою діяльність в інтересах Сил підтримки Збройних Сил України, не спроможні охопити весь спектр наукових завдань за цими напрямками, зокрема на оперативному та тактичному рівнях.

Існуючий міжнародний досвід як міжнародних партнерів України [4; 5; 8], так і противника [2; 3; 6; 9; 10; 11; 12] по створенню наукових установ, демонструє їхню ключову роль у забезпеченні технологічної переваги та інноваційному розвитку оборонної сфери. Яскравим прикладом такої синергії є діяльність таких установ за напрямками підтримки у Сполучених Штатах Америки та в рамках НАТО.

Агентство перспективних оборонних досліджень (DARPA) є незалежним науково-дослідним та дослідно-конструкторським органом у складі Міністерства оборони США [4]. Його місія полягає у співпраці з новаторами як в урядових структурах, так і поза ними для розробки передових технологій. Ця модель дозволяє швидко реагувати на актуальні потреби оборони та створювати проривні рішення.

Ще одним ключовим інститутом є Науково-дослідний та дослідно-конструкторський центр Інженерних військ армії США (ERDC) [5], який виступає провідним центром досліджень та розробок для Інженерного корпусу армії США. ERDC є невід'ємною частиною Офісу помічника міністра оборони з питань досліджень та інженерії, що підкреслює його стратегічне значення. Заступник міністра оборони з питань досліджень та інженерії (USD (R&E)) відповідає за синхронізацію зусиль у сфері науки і технологій по всьому Міністерству оборони та родах військ. ERDC допомагає у вирішенні складних проблем цивільного та військового будівництва, геопросторових наук, водних ресурсів та екологічних наук. Його діяльність зосереджена на п'яти основних напрямках, зокрема на військовій інженерії, яка надає військовослужбовцям інноваційні технології для захисту сил та маневру, а також на дослідженнях, що стосуються військових об'єктів, цивільного будівництва, геопросторової інженерії та проєктованих стійких систем [5].

На рівні НАТО інноваційний процес підтримується через таку ініціативу, як акселератор оборонних інновацій для Північної Атлантики (DIANA) [8]. Цей незалежний інноваційний фонд, заснований у 2022 році, має на меті підтримку компаній, що працюють у сфері "глибоких технологій", які роблять внесок в обороноздатність. Інноваційний акселератор DIANA охоплює проєкти у сферах штучного інтелекту, великих даних, квантових технологій, біотехнологій, гіперзвуку та космосу, що відображає основні технологічні пріоритети Альянсу в умовах сучасних загроз [8].

Противник також провадить діяльність з формування наукових установ. Прикладом є наукові роти [12]. Концепція наукових рот в рф передбачає створення штатних підрозділів російської армії для проведення наукових досліджень та розробок в інтересах оборони. Ці формування підпорядковуються органам військового управління. Служба в них проходить за призовом, але в межах наукової діяльності, що, за офіційною позицією міністерства оборони рф [12], дозволяє ефективно використовувати потенціал призовників. Кожна рота має свій конкретний профіль, визначений міністерством оборони, та закріплена за профільним підприємством оборонно-промислового комплексу. Перша така рота була створена у 2013 році, і на сьогодні їхня кількість у складі збройних сил рф досягла 12. Їхнє основне завдання – виконання прикладних досліджень у високотехнологічних напрямках, таких як кібербезпека, криптографія, безпілотні системи, штучний інтелект та моделювання бойових операцій. Ключовим елементом реалізації цієї моделі є Військовий інноваційний технополіс "ЕРА", що функціонує під егідою міністерства оборони рф [6; 9]. Він

позиціонується як науковий кластер, який об'єднує військові, наукові та виробничі структури з метою пошуку, розвитку та впровадження проривних технологій. В "ЕРА" діють спільні лабораторії, де молоді вчені та оператори наукових рот працюють під керівництвом досвідчених фахівців. Ця модель дозволяє поєднувати військову службу з науково-дослідною роботою, з подальшим працевлаштуванням в оборонно-промисловому комплексі. Таким чином, ця система позиціонується як ефективна модель взаємодії наукових, освітніх та виробничих організацій [12].

Враховуючи міжнародний досвід провідних інституцій, таких як DARPA, ERDC та DIANA, створення наукової установи Сил підтримки Збройних Сил України є критично важливим для забезпечення технологічної переваги та адаптації до сучасних воєнних викликів. Наукова установа Сил підтримки Збройних Сил України відіграватиме ключову роль у консолідації зусиль, спрямованих на інноваційний розвиток у сферах військової інженерії, ХБРЯз, геопросторової та гідрометеорологічної підтримки. Її діяльність дозволить не лише швидко реагувати на застосування противником нових зразків озброєння та військової техніки, а й систематизувати бойовий досвід, створюючи новітні доктринальні документи та забезпечуючи наукове супроводження розробки та впровадження ОВТ за номенклатурою Сил підтримки. Таким чином, вона стане фундаментом для довгострокового технологічного розвитку та інтеграції українських військових стандартів у міжнародну систему безпеки за напрямками Сил підтримки Збройних Сил України.

Пріоритетними дослідженнями наукової установи Сил підтримки Збройних Сил України є:

1. Подолання системи інженерних загороджень під час прориву глибокоешелонованої оборони, аналізуючи історичний досвід наступальних операцій.
2. Влаштування інженерних загороджень.
3. Підтримка подолання водних перешкод; подолання перешкод на суходолі. Підтримка пересування військ (Сил).
4. Оцінювання ХБРЯ обстановки. Управління ризиками ХБРЯ загроз.
5. Посилення захисту військ (Сил) із застосування аерозолів.
6. Вогневе ураження противника із застосуванням вогнеметної зброї.

Метою статті є обґрунтування необхідності та визначення основних функцій і завдань наукової установи Сил підтримки Збройних Сил України, роль та місце в системі наукових та науково-дослідних установ Міністерства оборони України, що сприятиме підвищенню обороноздатності України шляхом якісного наукового забезпечення розвитку Збройних Сил України та швидкої нейтралізації загроз, що виникають перед нашими військами за напрямками Сил підтримки Збройних Сил України.

Виклад основного матеріалу

Утворення наукової установи Сил підтримки Збройних Сил України є важливим кроком у підвищенні обороноздатності країни та матиме на меті наукове забезпечення розвитку Сил підтримки Збройних Сил України за ключовими напрямками, що відповідають сучасним викликам.

Інженерна підтримка є однією з фундаментальних складових системи об'єднаної підтримки військ (сил). Наукова установа проводитиме дослідження, які охоплюватимуть широкий спектр питань: від обладнання переправ і влаштування інженерних загороджень до маскування військ та розмінування місцевості. Важливість цього напряму підтверджується наявністю численних стандартів НАТО (STANAG 2010, 2017, 2021, 2036, 2143, 2221, 2282, 2369, 2370, 2394, 2929, 2989, 2991), що вказує на його пріоритетність у військовій справі.

Хімічний, біологічний, радіологічний та ядерний захист (ХБРЯз) також перебуває в фокусі уваги. У рамках цього напряму центр обґрунтовуватиме шляхи вдосконалення методів оцінювання РХБ-обстановки, досліджуватиме способи застосування підрозділів аерозольного маскування та вогнеметних підрозділів, а також аналізуватиме їхній внесок у загальну вогневу підтримку.

Геопросторова підтримка має вирішальне значення для успішного ведення бойових дій. Центр займатиметься розробкою адаптивних картографічних рішень, удосконаленням методів цифрового картографування, технологій друку та навігаційної підтримки військ. Окрему увагу буде приділено використанню глобальних навігаційних супутникових систем (GNSS) для високоточного визначення позицій та застосуванню БПЛА для збору геодезичної інформації.

Гідрометеорологічна підтримка є критично важливою для планування операцій. Дослідження будуть спрямовані на вдосконалення системи та технічних засобів забезпечення гідрометеорологічною інформацією, а також на розробку методів прогнозу небезпечних явищ погоди та оцінки їх впливу на ефективність застосування зброї. Приклад НАТО, яке має Комбінований метеорологічний та океанографічний підрозділ (CMU) і надає METOC-послуги для командування, підкреслює визнану важливість цього виду підтримки серед союзників.

Кінологічна підтримка є ще одним напрямом, який буде розвиватися у центрі. Дослідники займатимуться розробкою доктринальних документів, засад функціонування та розвитку кінологічної освіти, а також впровадженням нових технологій для підвищення ефективності кінологічних розрахунків як у бойових умовах, рятувально-пошукових роботах, так і у ході реабілітації ветеранів.

Необхідність створення наукової установи Сил підтримки Збройних Сил України та переваги від її діяльності випливають з потреби відповіді на сучасні воєнні виклики. Наукова установа забезпечить швидкий пошук рішень з нейтралізації загроз за напрямками підтримки, проводячи стислі у часі науково-прикладні дослідження для оперативної реакції на динамічні зміни способів ведення бойових дій.

Важливою перевагою стане комплексність досліджень, оскільки наукова установа Сил підтримки Збройних Сил України буде здатна виконувати весь спектр наукових завдань – від пошукових до експериментальних. Це дозволить забезпечити повний цикл розробок.

Створення наукової установи Сил підтримки Збройних Сил України також сприятиме раціональному розподілу наукових завдань. Це вирішить проблему повного наукового завантаження та незначної штатної чисельності в інших наукових установах Міністерства оборони України та Збройних Сил України.

Крім того, діяльність наукової установи Сил підтримки Збройних Сил України забезпечить синхронізацію з досвідом НАТО, оскільки пріоритетні напрямки його роботи відповідають підходам, що застосовуються країнами-членами Альянсу. Це є критично важливим для інтеграції та взаємосумісності.

Наукова установа Сил підтримки Збройних Сил України також займатиметься розробкою доктринальних документів, здійснюючи наукове супроводження для їхнього створення на всіх рівнях — від стратегічного до тактичного.

Вона забезпечить впровадження досвіду та наукове супроводження всього життєвого циклу ОВТ за напрямками підтримки. Це включає аналіз і узагальнення бойового досвіду, обґрунтування оперативно-стратегічних та тактико-технічних вимог до ОВТ за номенклатурою Сил підтримки Збройних Сил України, а також експериментальні дослідження новітніх зразків.

Щодо удосконалення системи управління, наукова установа Сил підтримки Збройних Сил України обґрунтовуватиме структуру управління Сил підтримки,

функціональний розподіл завдань між органами військового управління, а також вимоги до пунктів управління та засобів зв'язку.

Фінансово-економічне обґрунтування реалізації проєкту передбачає його здійснення в межах видатків Міністерства оборони та не потребує додаткових видатків з державного бюджету.

Високу ефективність функціонування показали досягнення військової частини, котра є прообразом майбутньої наукової установи. Протягом поточного року невеликою кількістю дослідників було виконано низку ключових завдань, зокрема:

1. Створено рекомендації (методичні рекомендації) з питань:
   - протидії мінним тралам та особливості улаштування інженерних загороджень в урбанізованій місцевості;
   - улаштування інженерних загороджень інженерними підрозділами;
   - перспективних способів подолання інженерних загороджень противника та забезпечення живучості й мобільності груп розгородження;
   - проведення оперативно-тактичних розрахунків за напрямком ХБРЯ захисту;
   - захисту особового складу від хімічної зброї та небезпечних хімічних речовин.
2. Укладено посібник (методичний посібник) по:
   - складанню метеорологічних бюлетенів за стандартом НАТО METOC в інтересах артилерії;
   - кінологічній підтримці.
3. Розроблено:
   - вимоги до сучасних аерофотознімальних комплексів, спеціального ПЗ для створення цифрових моделей місцевості;
   - методику оцінювання вартості діяльності за напрямком геопросторової підтримки;
   - інструкцію з виконання лазерного сканування та обробки отриманих даних;
   - навчально-методичні програми за напрямками: патрульно-розшукові собаки; штурмові собаки.

Ці досягнення свідчать про наявний потенціал та кваліфікацію персоналу, що є міцною основою для розширення та поглиблення наукових досліджень у межах новоствореної наукової установи. Утворення наукової установи Сил підтримки Збройних Сил України є важливим кроком у підвищенні обороноздатності країни, та матиме на меті наукове забезпечення розвитку Сил підтримки Збройних Сил України за ключовими напрямками, що відповідають сучасним викликам.

Утворення наукової установи є відповіддю на сучасні воєнні виклики. Воно забезпечить швидку нейтралізацію загроз, проводячи стислі у часі науково-прикладні дослідження для реагування на зміни способів ведення бойових дій.

Важливою перевагою стане комплексність досліджень, оскільки майбутня наукова установа буде здатна виконувати весь спектр наукових завдань – від пошукових до експериментальних. Це дозволить забезпечити повний цикл розробок.

Висновки

Утворення наукової установи Сил підтримки Збройних Сил України є критично важливим та своєчасним рішенням для підвищення обороноздатності України. Цей крок дозволить:

забезпечити якісне та оперативне наукове супроводження розвитку Сил підтримки Збройних Сил України за всіма ключовими напрямками (інженерна, РХБЗ, геопросторова, гідрометеорологічна та кінологічна підтримка);

сприяти пришвидшенню нейтралізації загроз, що виникають перед українськими військами в умовах динамічної війни та застосування противником новітніх ОВТ;

оптимізувати розподіл наукових завдань та ресурсів між науковими установами Міністерства оборони України, усуваючи існуючі обмеження щодо штатної чисельності та наукового завантаження.

інтегрувати передовий досвід та стандарти країн-членів НАТО у діяльність Збройних Сил України, що підвищить взаємосумісність та ефективність міжнародної співпраці.

Реалізація цього проєкту, що базується на вже наявних досягненнях та кваліфікації існуючої військової частини, котра є прообразом майбутньої наукової установи Сил підтримки Збройних Сил України, забезпечить необхідну науково-дослідну платформу для інноваційного розвитку та адаптації українських Збройних Сил України за напрямками Сил підтримки Збройних Сил України до сучасних та майбутніх викликів.

Список літератури

1. AJP-3.8: NATO Doctrine for CBRN Defence. (б.д.).
2. Bendett S., Gilli A., Gilli F., Kofman M., Michail D. *Advanced military technology in Russia*. Chatham House. 2021. URL: https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-23-advanced-military-technology-in-russia-bendett-et-al.pdf.
3. Connolly R., Boulegue M. *Russia's State Armaments Programme, 2018-2027*. Chatham House. 2018. URL: https://www.chathamhouse.org/sites/default/files/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf.
4. DARPA. (б.д.). *About*. URL: https://www.darpa.mil/about.
5. ERDC. (б.д.). *US Army Engineer Research and Development Center*. URL: https://www.erdc.usace.army.mil/.
6. Gur. (б.д.). *Federal State Autonomous Institution Military Innovative Technopolis Era*. URL: https://war-sanctions.gur.gov.ua/uav/companies/14304.
7. Heise G. Climate Change and Impact on Military Operations. EUROMIL. 2019. URL: https://euromil.org/wp-content/uploads/2019/09/191024_Presentation_LtCol_Heise_Climate-Change-and-Impact-on-Military-Operations_GMACCC_excerpt.pdf.
8. NATO. (б.д.). *The Defence Innovation Accelerator for the North Atlantic (DIANA)*. URL: https://www.nato.int/cps/en/natohq/202240.htm.
9. OECD.AI. (б.д.). *Russia Discusses Military AI Enhancement at ERA Technopolis*. URL: https://oecd.ai/en/incidents/2025-01-31-8b81.
10. Open Sanctions. (б.д.). *Federal State Autonomous Institution Military Innovative Technopolis Era*. URL: https://www.opensanctions.org/entities/NK-eKB8AdJWFuGApx2mvY7akJ/.
11. Ponomareva L. V. (б.д.). *Problems of modernization in Russia*. URL: https://serious-science.org/problems-of-modernization-in-russia-4359.
12. Russian Ministry of Defence. (б.д.). *Scientific companies*. URL: https://mil.ru/service/recrut/conscription/scientific-companies.
13. U.S. Department of the Army. (2014). ATP 3-34.80: Engineer reconnaissance. URL: https://irp.fas.org/doddir/army/atp3-34-80.pdf.

UDK 355.40 DOI: 10.63978/3083-6476.2025.2.2.06

Oleh Zolotukhin
PhD in Engineering, Associate Professor of Department
Dean of Computer Science Faculty,
Head of Artificial Intelligence Department
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
e-mail: oleg.zolotukhin@nure.ua
ORCID: 0000-0002-0152-7600

Valentin Filatov
Doctor of Engineering Science, Professor
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
e-mail: valentin.filatov@nure.ua
ORCID: 0000-0002-3718-2077

Maryna Kudryavtseva
PhD in Engineering, Associate Professor of Department
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
e-mail: maryna.kudryavtseva@nure.ua
ORCID: 0000-0003-0524-5528

Serhiy Shaptala
Non-Governmental Organization "Center for Military Strategy and Technologies"
Kyiv, Ukraine
e-mail: smokliak@ukr.net
ORCID: 0000-0002-0348-4050

USING ARTIFICIAL INTELLIGENCE METHODS IN TASKS OF DECENTRALIZED CONTROL OF A GROUP OF UNMANNED AERIAL VEHICLES

Abstract. *For solving tasks dangerous to humans, a group of unmanned aerial vehicles (UAVs) has advantages over a single device. The greatest result is the implementation of decentralized control of a group of UAVs. The work considers the problem of decentralized control of a group of UAVs for the effective solution of strategically important tasks in conditions of uncontrolled situations using swarm intelligence methods. The work presents a structural diagram and implements a method of decentralized control of a group of UAVs. Practical results – modeling the behavior of drones in a group.*

Keywords: *agent, artificial intelligence, decentralized management, Python programming language, unmanned aerial vehicle.*

Золотухін Олег Вікторович
кандидат технічних наук, доцент
декан факультету комп'ютерних наук,
завідувач кафедрою штучного інтелекту
Харківський національний університет радіоелектроніки
Харків, Україна
e-mail: oleg.zolotukhin@nure.ua
ORCID: 0000-0002-0152-7600

Філатов Валентин Олександрович
доктор технічних наук, професор
Харківський національний університет радіоелектроніки
Харків, Україна
e-mail: valentin.filatov@nure.ua
ORCID: 0000-0002-3718-2077

Кудрявцева Марина Сергіївна
кандидат технічних наук, доцент
Харківський національний університет радіоелектроніки
Харків, Україна
e-mail: maryna.kudryavtseva@nure.ua
ORCID: 0000-0003-0524-5528

Шаптала Сергій Олександрович
Громадська організація "Центр воєнної стратегії і технологій"
Київ, Україна
e-mail: smokliak@ukr.net
ORCID: 0000-0002-0348-4050

ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАДАЧАХ ДЕЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ГРУПОЮ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Анотація. *Для вирішення небезпечних для людини задач група безпілотних літальних апаратів (БПЛА) має переваги щодо поодинокого квадрокоптеру. Однак найбільшу цінність представляє можливість децентралізованого управління групою БПЛА, коли єдиний центр управління пристроями або оператор відсутні. Таке рішення дозволяє вирішувати стратегічно важливі завдання у різних сферах: військовій, логістичній, побутовій, рятувальній, моніторингу місцевості. В даній роботі розглядається задача децентралізованного управління групою безпілотних літальних апаратів для ефективного вирішення завдань в умовах неконтрольованих ситуацій з використанням методів штучного інтелекту, а саме колективного розуму та ройового інтелекту. Метою роботи є дослідження ройових методів, методів децентралізованого управління групою БПЛА, адаптивних алгоритмів для ефективного вирішення завдань в умовах неконтрольованих ситуацій. У роботі представлено структурну схему і реалізовано метод децентралізованого управління групою БПЛА. У рамках практичних результатів проведено моделювання поведінки дронів у групі. Представлені результати роботи полягають в забезпеченні контролю над групою БПЛА, необхідність групового управління обумовлена тим, що багато задач виконуються швидше, точніше та з меншими ресурсними витратами. Зростанню актуальності використання децентралізованого управління для вирішення практичних завдань сприяє здешевлення елементної бази з одночасним*

зменшенням її розмірних характеристик, що робить можливим використання великих груп БПЛА. Також підвищенню ефективності використання децентралізованих методів сприяє зростання складності завдань, покладених на БПЛА, збільшення частки невизначеності в умовах виконання місії, а також зростання рівня довіри до систем управління групами пристроїв. Зазначені фактори сприяють необхідності оперативного прийняття рішення і максимізації самостійності дій БПЛА.

Ключові слова: *агент, безпілотний літальний апарат, децентралізоване управління, мова програмування Python, штучний інтелект.*

Introduction

Modern military conflicts demonstrate a transition to a new paradigm of warfare, where information technology and automated systems play a key role. Artificial intelligence (AI) is one of the leading tools that can significantly change the nature and course of military operations. With the ability to analyze large amounts of data in real time, make predictions, and autonomously perform tasks, AI provides an advantage in high-tech conflicts.

Artificial intelligence encompasses a set of technologies that enable the performance of tasks that traditionally require human intelligence: pattern recognition, natural language processing, decision-making and learning from experience. The current development of AI is based on such areas as: machine learning, deep learning, neural networks, computer vision, natural language processing (NLP), and robotics.

In the civilian sector, these technologies are already widely used in medicine, transportation, industry, financial systems, and education. The military sector is largely adopting these developments, adapting them to solve specific tasks: from detecting enemy objects to controlling autonomous systems.

Information advantage in modern wars is no less important than the numerical advantage of troops. AI allows for effective processing of data from various sources: satellite images, radio intelligence signals, data from unmanned aerial vehicles and sensor systems. Autonomous systems are one of the most promising areas of application of AI. Unmanned aerial vehicles (UAVs), which perform reconnaissance, target strikes and communications have gained the greatest popularity. Intelligent algorithms allow such autonomous devices to independently navigate in space, avoid obstacles and work in groups (swarm methods).

Drones and unmanned aerial vehicles are modern software and hardware devices that have become an integral aspect of modern society and are expanding into various industries, which allows them to solve a number of complex or dangerous tasks for humans. For example, in the domestic sphere – these are the tasks of the “Smart Home”, in the commercial sphere – these are the tasks of delivery and logistics, in the scientific or applied sphere – research into the chemical and biological composition of organisms, as well as in the military, police and rescue spheres. The use of drones in cities for solving local monitoring tasks is also very useful.

Let’s consider the basic definitions [1, p. 3-5].

A drone is any mobile unmanned transport vehicle, i.e. without a pilot on board, pre-programmed to perform a specific task in the air, on land or under water. Thus, the term “drone” refers not only to the modern recreational quadcopter, but also to sea (for example, a submarine) or land-based autonomous vehicles, as well as to remotely controlled vehicles. When using drones for aerial missions, this term is mainly used by mass media to refer to a simple aircraft. They are mainly available as ready-made solutions [1, p. 3-5].

An unmanned aerial vehicle is a vehicle that flies without a pilot, either remotely and fully controlled from another location (ground, another aircraft, space) or programmed and fully autonomous. This refers to large unmanned aerial vehicles with autopilots, which have found widespread use in the civil and defense sectors [1, p. 3-5].

The use of both terms depends on the characteristics of the aircraft, as well as the scope of application.

An unmanned aerial vehicle complex is a set of several devices that include the unmanned aerial vehicle itself, as well as the equipment necessary for its operation: a ground control station, an antenna system, and catapults.

This paper considers the devices of unmanned aerial vehicles (agents or boids).

Advantages of using unmanned aerial vehicles are [2, p. 140-145]:

speed – the necessary information on unmanned aerial vehicles can be provided to the client faster using special cameras and data channels, rather than using traditional shooting methods, which can sometimes be slow;

economy – data is obtained faster than with the help of conventional collection methods, so various missions can be performed in a shorter period of time, thus, the cost is lower than when using other devices;

safety – UAV operators do not need to be in territory that may be dangerous for various reasons;

high level of accuracy – an unmanned aerial vehicle can receive high-speed data. This is due to the duplication of information received during the flight – the more rewrites, the more accurately the recorded information;

to carry out a mission or task, there is no need to involve a qualified pilot, since they are unmanned, and all systems are designed in such way that human intervention in the work is minimized;

An unmanned aerial vehicle is capable of flying and collecting information in rain, fog, foggy weather, and high temperatures.

According to the principle of controlling groups of agents (UAVs), centralized and decentralized systems can be considered.

Centralized management of all elements of the group is carried out from a single coordination center, the policy clearly delimits types of activities or operations.

Decentralized management implies the absence of a single control center for the formation of coordination teams for each of the group elements.

The work explores methods of swarm intelligence, methods of decentralized control of a group of unmanned aerial vehicles in uncontrolled situations.

Swarm intelligence is the collective behavior of individuals (agents) in a system that is self-organizing without a defined control center, that is, in a decentralized group [3, p. 6-12]. One of the fundamental rules of swarm intelligence is the fact that it requires a fairly large number of agents capable of interacting with each other and the environment.

A single agent follows simple rules that are inherent in it (either by physical laws or genetics). Despite the absence of a command center that would indicate what each of the fighters should do, their random interactions lead to the fact that the general behavior of the group becomes clearly intelligent. At the same time, each specific fighter does not necessarily behave intelligently. Such behaviors are demonstrated, for example, by ants, bees, termites, wolves, water droplets, the human immune system, bats, etc.

To achieve a specific goal set by a group of unmanned aerial vehicles in the case of centralized control each drone can perform a certain sequence of actions known in advance.

In the case of decentralized control, which is more flexible, this sequence must be found by the control system of a group of agents in the process of achieving the goal, while the actions of a group of unmanned aerial vehicles must be coordinated in some way.

Statement of the problem.

Thus, the aim of the work is implementation of method of decentralized control of a group of unmanned aerial vehicles. This task consists in implementing the control system by agents of the sequence of actions of all group members when solving the task.

To achieve this goal in work:

a study of swarming methods and algorithms was conducted, and the bee method was selected for the implementation of a UAV group control system;

a structural scheme for decentralized management of the UAV group is presented;

the implementation of a method for decentralized control of a group of unmanned aerial vehicles was presented;

a practical implementation is presented.

Analysis of recent research and publications.

The biggest advantage of unmanned aerial vehicles is the ability to perform tasks that may be dangerous or impossible for humans to execute. In this sense, the use of UAVs is more suitable for performing tasks of photo or video monitoring, data reconnaissance, and combat operations.

The disadvantages of UAVs include limited payload and flight time. As for the use of UAVs, the problem may be the presence of various obstacles, accidental or intentional. But these disadvantages can be solved by using a group of vehicles. There are certain problems with this approach, namely the coordination and interaction of certain UAV units in a group and the distance of communication with the remote control.

The actuality of this work consists in providing control over the UAV group, specifically, the UAV group has certain advantages over a single UAV:

1) increased awareness of the environment for communication within the group;
2) interchangeability of UAVs due to the replacement citation;
3) increased reliability;
4) speed of task completion;
5) the ability to collectively perform more complex tasks.

When performing the assigned tasks, the UAV group may encounter certain obstacles that must be overcome by the entire group or to reduce the number of disabled UAVs. After completing the task, it is necessary (if required by the task) to return to the starting point of departure [4, p. 1256-1260].

Since the tasks are performed by a group of UAVs, it is necessary to use a mechanism for transmitting data about threats between certain UAV units. This is necessary in order to reduce the chance of each UAV in the group colliding with a threat.

Moreover, if one of the UAVs in the group loses contact with the operator controlling it (or the entire group), it is necessary for this unit to be able to continue the execution of the task set thanks to another UAV in the group that has contact with the operator. That is, if the UAV loses contact with the operator, by default, it will return to the operator's side until contact is restored. In the context of completing the task, this is incorrect behavior, since it is necessary to be in the UAV group, avoid threats, and achieve the task. For this reason, the neighboring UAV, which has not lost contact with the operator, will provide him with information about new commands or threats, which the "lost" UAV will execute according to its initial task [4, p. 1256-1260].

The need for group management is due to the fact that many tasks are performed faster, more accurately, and with less resource costs.

Let's consider the choice and justification of the UAV behavior model.

The technology of UAV behavior can be based on the general theory of technical systems control [5, p. 40-45; 6, p. 22-30]. Behavior can be considered as a special case of the general theory of optimal control of objects. In such formulation, the UAV appears as an abstract discrete control system, which based on its actions and the reaction to these actions of the environment chooses the optimal strategy of behavior.

In many real-world situations, the choice of options has to be made under conditions of a priori uncertainty, when based on the available data, it is not possible to specify in advance which of the possible options should be chosen to ensure the achievement of a given goal. In this case, achieving a given goal is possible only on the basis of the application of an adaptive approach [7, p. 50-55], the meaning of which is to use current information obtained as a result of individual selection actions, which allows to compensate for the lack of information and implement the optimal management strategy for the class of systems.

Let us consider the general formulation of the adaptive selection problem, presented in Fig. 1.

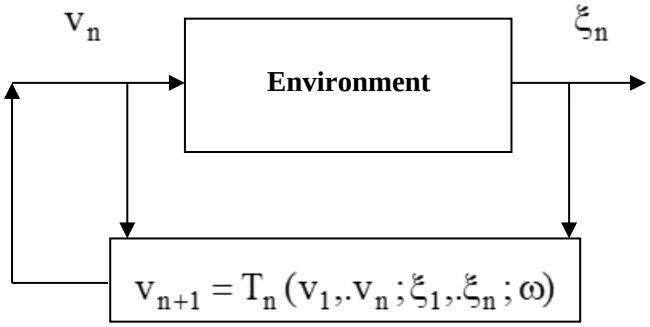


Fig. 1. Scheme of adaptive selection of options
Source: developed by the authors based on data from [7, p. 50-55].

The meaning of the approach is as follows: at each of the successive moments in time $t_n (n = 1,2\ldots)$ you must choose an option v_n from a finite set of possible options V.

As a result of the choice made, the system loses ξ_n is a random variable – elementary result function ω, and depend on v_n and, possibly, the states of the system. A sequence of options is implemented $\{v_n\}$ should be such that the set goal, which is formulated in terms of the limit values of current average losses, is achieved.

The presence of a priori uncertainty, which consists in the lack of accurate information about the losses of the system and its characteristics, leads to the fact that the formation of a sequence of options $\{v_n\}$, which ensures the achievement of the target condition of the problem being solved, should be carried out in accordance with the adaptive approach. In this case, the choice of the next option v_{n+1} is carried out based on the sequence of losses obtained at the current time $\xi_1, \xi_2, \ldots, \xi_n$, the corresponding implemented sequence of options $v_1, v_2, \ldots, v_n$. This means that v_{n+1} is a function of $v_1, v_2, \ldots, v_n$, $\xi_1, \xi_2, \ldots, \xi_n$ and maybe from time to time n and elementary result ω. Thus

$$v_{n+1} = T_n(v_1, v_2, \ldots, v_n; \xi_1, \xi_2, \ldots, \xi_n; \omega), n = 1,2, \ldots , \quad (1)$$

where ξ_n depending on the task a scalar or a vector.

Function T_n we will call the option selection rule v_{n+1}. This function can be either deterministic or random. Sequence $\{T_n\}$ selection rules determines the strategy for selecting options or the management strategy [8, p. 60-65; 9, p. 310-315].

Let's consider existing systems of centralized and decentralized management of groups of autonomous intellectual objects.

At work [10, p. 74-80] the task of automating the work of a group of quadcopters in a location where drones take off, land, and fly along a given trajectory is considered. Quadcopters under the control of an operator can perform tasks of various complexity, such as filming materials for a film or a search operation, but the greatest value is the possibility of automating the task performed, when only one operator is needed to monitor the clear execution of the work, a watchman, i.e. a centralized control system is considered. It is possible to automate the process of cargo delivery, spot scanning, as well as shipping and handling operations.

The work provides a review of group management, in particular group management methods and strategies used in practice. Based on the analysis of group management, the method of quadcopter system design is selected.

Work [11, p. 403-408] is devoted to a topical problem of mathematical modeling and control theory: the task of decentralized control by multi-agent system consisting of agents

modeling autonomous robots, with the aim of providing a fixed group of agents with a system that has a given geometric shape.

For an even distribution of agents in the mission zone, maintaining stable communication among the group, and preventing collisions, a certain geometric structure of the system must be maintained during the mission (a certain position relative to each other or relative to the center of mass of the group, which creates certain geometric figures).

To solve this problem, the following approaches are used:

1) to set the desired distance between pairs of agents and apply graph stiffness theory [12, p. 215-217; 13, p. 88-94];

2) to set the desired position of the agent with respect to its neighbors and vectors and to create rules of consensus (averaging) [14, p. 989-995; 15, p. 1860-1863; 16, p. 171-176];

3) at every moment, it is necessary to transmit information to the agents about the structure and direction of the request form, on the basis of which each agent can configure the request person and follow him [17, p. 2011-2014].

When developing algorithms based on one of the three approaches described above, as a rule, serious difficulties arise in processing the following citations:

1) the departure of one or several agents with the subsequent loss of the ability to transmit information, especially the leader agent;

2) interruption of communication with an agent who, on the way to the target point, found himself in the zone of information exchange with other agents;

3) communication problems with the coordination center (in cases where it is envisaged to continuously or periodically transmit information important for management from this center to agents).

At work [18, p. 1468-1473] a mathematical model is presented that describes a group of workers, and a fully decentralized control rule and algorithm are developed that allow for effective control of a group of agents while preserving the geometric shape of the system (certain mutual distances relative to each other) under the conditions of complete autonomy of the agent and the possibility of obtaining information only from its closest neighbors. In this case, the rule of thumb is to avoid the occurrence of the described extraneous citations.

An original decentralized management rule is proposed, which combines some principles of consensus (average), as well as elements of the approach using virtual leaders.

New elements for the field are used: criteria for the formation of a pattern corresponding to a given geometric structure with the necessary accuracy are formulated, based on the concepts of geometric structure of a pattern and virtual leaders introduced in this work, taking into account the complexity of various constraints. A distinctive feature of the generated control rules is that the set of virtual leaders is individual for each agent, the agent can independently coordinate virtual leaders and their preferences with the original generated rules, which allows choosing a place in the geometric structure of the formation dynamically without a fixed binding of the agent to a particular position in the geometric structure of the formation.

Thus, the analysis of research and publications demonstrates the relevance of using decentralized management of a group of agents.

Purpose of the article.

The purpose of the work is to study swarm methods, methods of decentralized control of a group of UAVs, adaptive algorithms for effective task solving in uncontrolled situations.

Presentation of the main material

Various swarm intelligence methods can be used to formalize UAV group flights: the particle swarm method, ant and bee algorithms [19, p. 1215-1220; 20, p. 1943-1946; 21, p. 12-18].

Despite their sufficient efficiency, particle swarm and ant swarm algorithms have some drawbacks. Due to the large number of parameters that can be adjusted, the considered methods

are quite sensitive to their choice and require careful tuning. The influence of such settings has an ambiguous effect on the efficiency of the algorithm and requires research when solving each specific problem.

The process of selecting settings does not have sufficient theoretical justification and in most cases is reduced to "fitting" the values. It is also necessary to have a fairly large amount of relevant information about the associated problem in order to select the values of the parameters responsible for local and global convergence. The strength of these methods is their high efficiency when successfully selecting the parameters to be adjusted, as well as the simplicity of program implementation.

In connection with the noted shortcomings of the particle swarm and ant swarm algorithms, let us consider the bee swarm method, which is less sensitive to parameters, but has a more complex logic of operation.

An artificial bee colony operate an algorithm similar to the extraction of nectar by honey bees. Instead of a field of flowers, let's consider a solution domain. Instead of nectar, let's use the criteria of an optimization problem, the objective function [22, p. 460-465].

At each iteration of the algorithm, regions with the best value of the objective function are selected and called "best". From the remaining regions, those considered "promising" are also selected. It is possible to set a certain minimum distance between two neighboring regions. In this case, if overlap occurs, the region with the worst value of the objective function is rejected. Another region is selected instead. The data of the area is remembered and during the next iteration, a certain number of bees are sent to it.

Algorithmic work can be divided into two stages [22, p. 460-465]:

1. Initialization:
   - upon initialization, initial positions are generated for n agents;
   - in the simplest case, the random sampling method is used.
2. Local search:
   - after forming lists of the best and most promising areas, "worker bees" are sent to their vicinity;
   - in some variants of the algorithm, the number of bees sent depends on the quality of the region from the point of view of the objective function. This dependence can be linear or determined by more complex rules;
   - in this case, a fixed number of bees is sent to each area, depending on the class to which the area belongs;
   - for each iteration, the "scouts beers" are sent to new areas.

   With the given algorithm, several parameters are created:
   1) the number of scouts;
   2) a number of the best and most perspective;
   3) a radius of the local scouting;
   4) the number of bees for each area class,
   5) minimum possible distance between neighboring areas.

The quality of the obtained solutions depends significantly on the choice of these parameters. In addition, the speed of the algorithm also depends on this choice.

There are countless modifications of this algorithm. They improve the quality of the results and the speed of it's work. This is mainly due to the reduction of dependence on the selected parameters.

The structural scheme of decentralized management of a group of UAVs based on the bee swarm method is shown in Fig. 2. The group of UAVs is represented in the form of a swarm of bees.

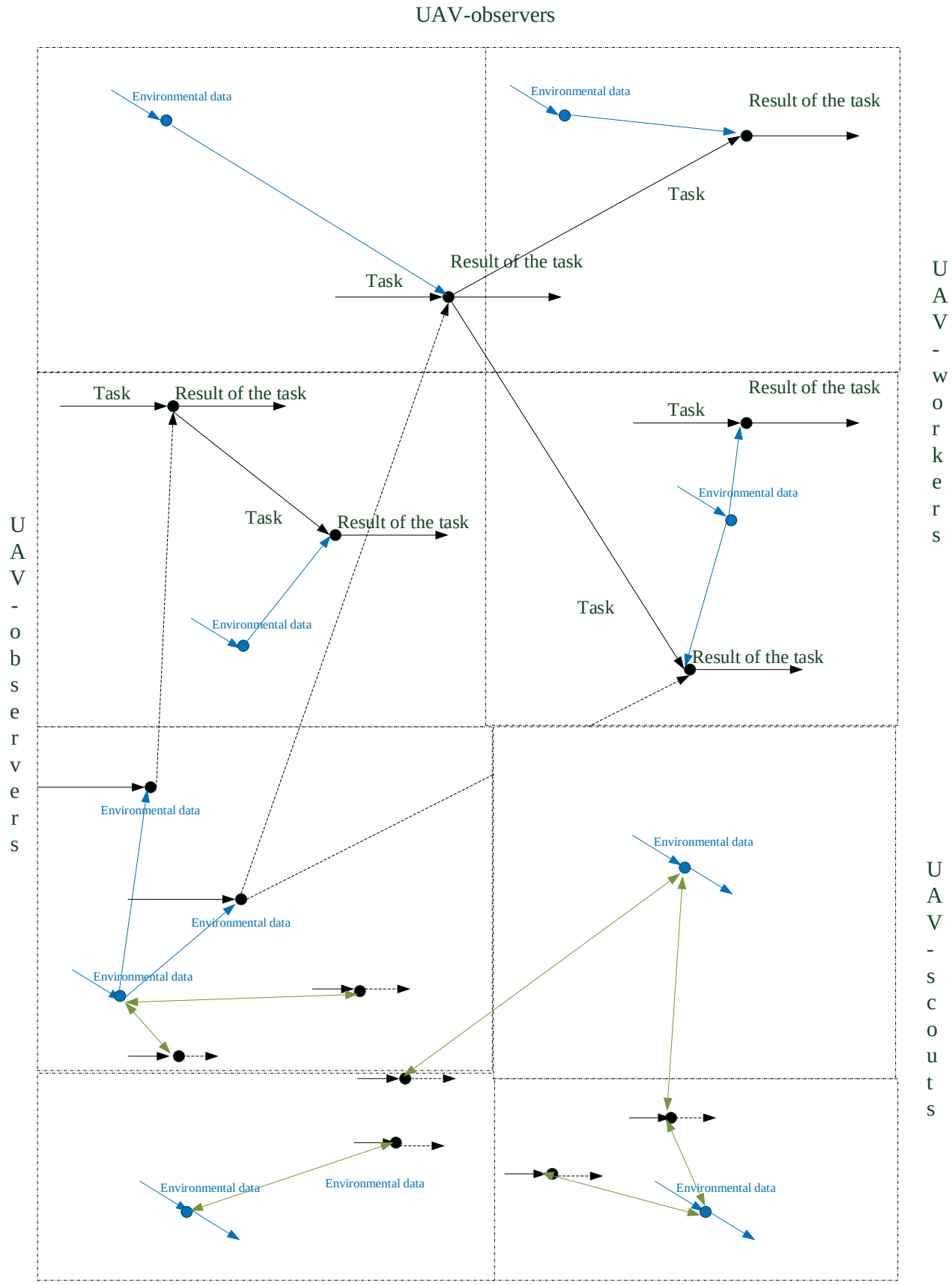


Fig. 2. Structural scheme of decentralized management of the UAV group
Source: developed by the authors

There are 3 groups of UAV-bees represented on the map:

UAV-scouts (first to conduct areas exploration, collect data on the environment);

UAV-observers (explore larger areas in the search area than the scouts);

UAV-workers (directly perform the assigned task, for example, armed or unarmed drones).

UAV-scouts collect data about the environment and transmit it to UAV-observers and UAV-workers for safe task performance.

UAV-observers also collect data about the environment, but they are exploring large areas in a search pattern (squares), compared to scouts and transmit the data to UAV-workers.

UAV-workers are considered the most valuable and strategically important devices that directly perform the task to achieve the goal. They use the received data about the environment and receive input for the task, which is performed decentralized, for example, from the cloud. The result of the task is similarly corrected.

Let's consider the main stages of implementing the adaptive bee algorithm.

1. Algorithm initialization. At the initialization stage, it is necessary to find or set several starting points and calculate the value of the objective function at them.

The group of UAVs, or bee swarms, is a vector of uniformly distributed random variables X, $X \epsilon D_x$.

The task is to find the point x_{nom} in the middle of the plane of Dx in the n-dimensional space

$$x_{nom} = \arg\max_{x \epsilon Dx} \text{dist}\,(x, \partial D_x), \quad (2)$$

Let's consider three types of UAVs:

s_j – UAV-scouts;

w_k – UAV-workers;

q_l – UAV-observers (explore larger areas in the search area than the scouts).

A swarm of UAVs represents the multitude

$$SW_{UAV} = \{s_j \cup w_k \cup q_l\}, j = 1, S; k = 1, W; l = 1, Q, \quad (3)$$

All particles act individually, following the general principle of the best personal and best joint position. The essence of the algorithm lies in the repeated undirected random search method (the process of UAV dispatch) in limited areas of the search path, called sections [22, p. 460-465].

For each type of UAV the parameter r(0;1] is set, which corresponds to the size of the investigated area. For UAVs, this parameter takes the following values:

$r_{sj} = 1$ – UAV-scouts are exploring the whole environment;

$r_{wk} = 0.1$ or 10% – from the initial size of the search area for UAV-observers;

$r_{ql} = 0.05$, or 5% for UAV-workers.

At the initialization stage it is necessary to find or set several starting points for the location of the UAV X_i in the area D_x, such that $X_i = \text{random}(Dx)$, for example, $X_1(x_1,y_1,\ldots,z_n)$, $X_2(x_2,y_2,\ldots,z_n)$, $X_3(x_3,y_3,\ldots,z_n)$ (see Fig. 3) and calculate the value of the objective function $\text{dist}(x, \partial D_x)$ in them.

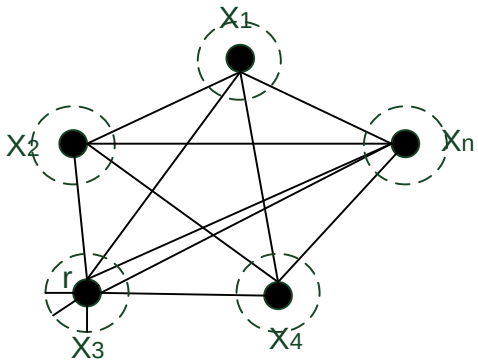


Fig. 3. UAV locations and their surroundings
Source: developed by the authors based on data from [22, p. 460-465].

2. Local search.

Depending on the objective function $\mathrm{dist}(x, \partial D_x)$, in the area D_x are selected areas:

b − the best ones, corresponding to the largest values of the objective function;

g − the good ones, that correspond closest to the best values of the objective function.

Then UAV-workers are sent to the b areas.

$$p_w = \frac{W}{b}, \tag{4}$$

UAV-observers are sent to the areas g.

$$p_q = \frac{Q}{g}, \tag{5}$$

The general recommendation for choosing the number of plots and bees is as follows. Each of the best plots should have more bees than the good plots, and the area should be smaller [22, p. 460-465].

It is important to note that the UAV-workers are not sent exactly to the place where the UAV-scouts and UAV-observers have found perspective and best places, but in their vicinity. In addition, the vicinity which defines the area where the UAV can be sent, can be reduced as the iteration number increases, so that the step-by-step solution approaches the "end" of the extreme. But if the cloud is reduced too quickly, then the writing can "get stuck" in local extremes [22, p. 460-465].

The size of the search area can be set both statically and dynamically, depending on the number of iterations. When implementing a dynamically changing search area, the convergence speed of the algorithm increases, but there is a possibility of the algorithm getting stuck in a local extremum. In this case, the global optimum may not be found. Based on this, when implementing this algorithm, fixed values were chosen for these parameters [22, p. 460-465].

After the UAV group explores the found areas, the areas are again sorted in descending order of the objective function among the UAVs participating in the search process, then a further selection of the best and most efficient areas is carried out and a new UAV dispatch is carried out. These steps are repeated until the stopping criterion is satisfied – achieving the set goal of the UAV group.

There can be several stopping criteria. For example, if the value of the objective function at the global extremum is known, then the algorithm can be repeated until the function reaches some value close to the desired one. If the value of the function at the extremum is unknown, then the algorithm steps can be repeated until the solution found does not improve after a sufficiently large number of iterations.

In the Fig.4 the graphs of the convergence of the bee swarm method depending on different sets of adjustable parameters are given. The abscissa axis shows the iterations, the ordinate axis shows the value of the objective function. From these graphs it is clear that the choice of algorithm parameters is not a critical factor in solving the optimization problem.

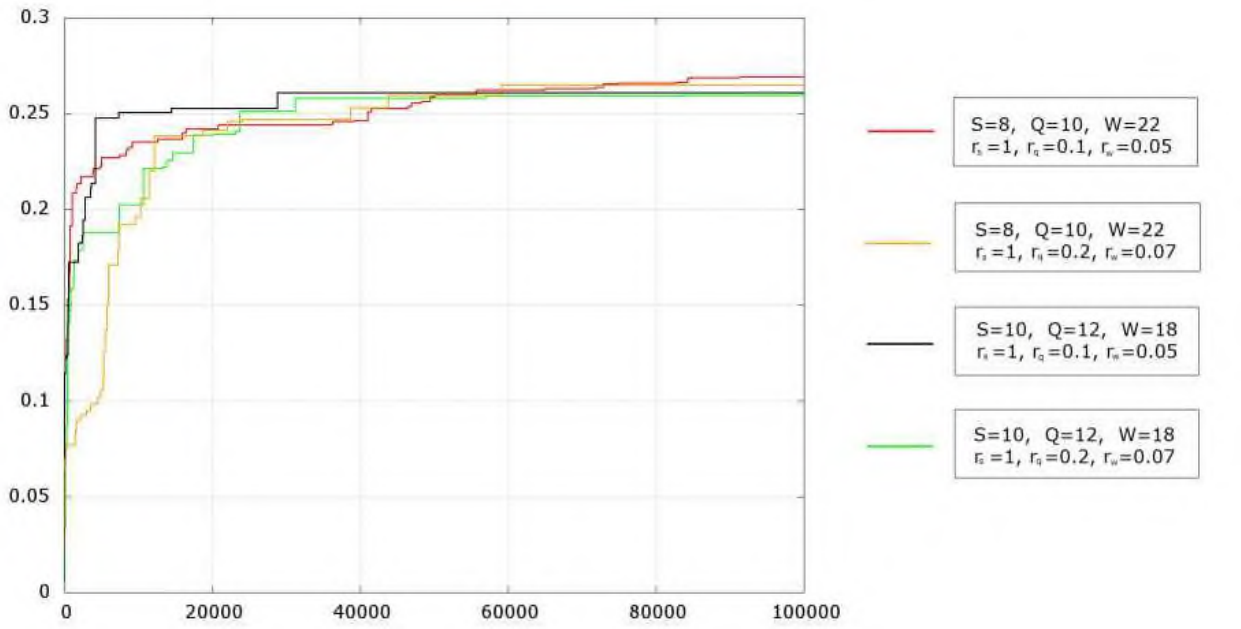


Fig. 4. The work of the swarm algorithm with different parameter sets
Source: developed by the authors

Thus, the task of ensuring the reliability of the technical devices of the UAV group against failures, which must be written at the stage of system design is considered. This is due to the incompleteness of the relevant information about possible external processes that may arise (the appearance of an obstacle for the UAV). The bee swarm method considered in the work, despite the rather complicated logic of the work and the process of organizing the calculation, in comparison with other methods, shows its effectiveness.

The main difficulties in using other search methods of this group are the selection of adjustable parameters. There is no universal set of parameters and it is not always possible to select different combinations of settings in order to choose the best one for each new task [23, p. 83-86].

In the work a modification of the bee swarm method is proposed, which simplifies the logic of its work and program implementation. This modification has shown its effectiveness and versatility. The considered method depends to a lesser extent on the quality of parameter settings.

Thus, if we consider all the criteria in the complex, from the point of view of the best solution to the task, limited time and computational resources, the absence of the possibility of fine-tuning the parameters of the algorithms, the absence of information about the associated task, then using the bee swarm method is the best for solving the problem of controlling a group of UAVs with decentralized control.

In Fig. 5 (a, b, c, d, e, f) you can see how the UAV agents gradually accumulate around one best solution.

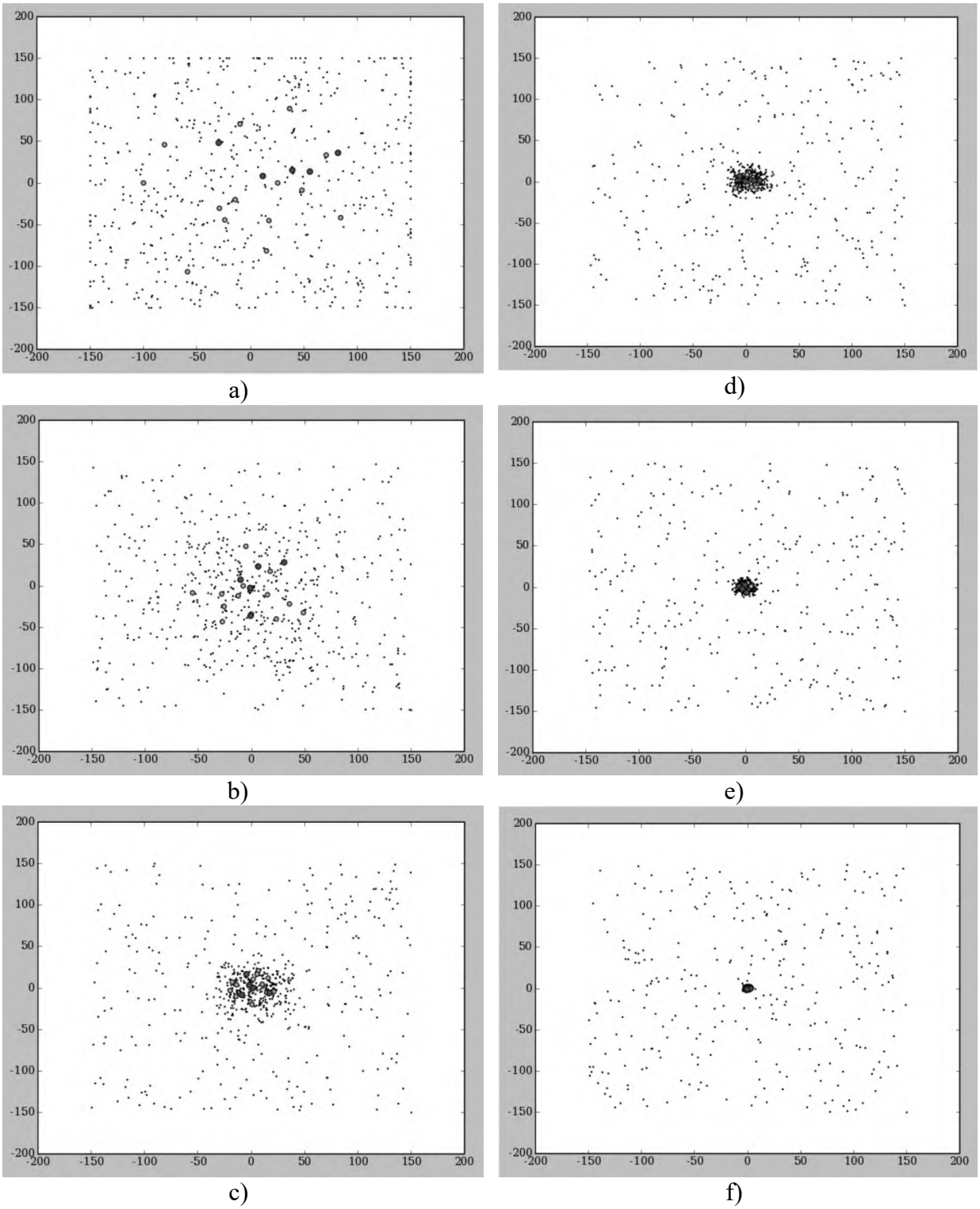


Fig. 5. Gradual accumulation of UAV agents around a single best solution
Source: developed by the authors

In this figure the red dots are the UAV bees that found the best solutions, the yellow dots are the are the chosen solutions and the black dots are other UAV bees, including the UAV-scouts that are randomly selected.

Conclusions

Thus, the main advantage of using the decentralized system proposed in this work is the absence of a single agent management center, since it can potentially be destroyed.

To implement an agent-based UAV control system, reliable and unconditional task performance and achievement of the set goal are provided. During the task performance, various obstacles may arise, both accidental and intentional, therefore it is necessary to use protective conditions for unmanned aerial vehicles. One such condition for increasing the reliability of task performance is the organization of UAVs into groups. Another option is to use special UAV-scouts and UAV-observers, who will constantly collect data about the environment and transmit it to UAV-workers for successful task completion, maintaining the integrity of the devices, and returning to the original point of departure.

In such scenarios, drones are often used as mobile sensors, which are used to collect data, which is then processed in a cloud service.

But, considering the technologies for creating autonomous drones, both armed and unarmed, the ethical and legal aspects of the use of artificial intelligence when used in combat situations become relevant. One of the most important challenges is the issue of responsibility for the actions of autonomous systems. International humanitarian law does not contain clear provisions on the use of combat drones. Therefore, in international community there is a need to regulate the activities of agent-based artificial intelligence technologies, creation of a regulatory framework that will regulate the limits of their application.

Ethical issues also include the problem of making decisions about the use of force by autonomous devices. Developers emphasize the need for “human control”, when the final decision to defeat the target remains with a person.

Humanity is rapidly approaching the point when autonomous systems can begin to act against humanity, and human intervention in this system will become difficult or even almost impossible.

References

1. Austin R. Unmanned Aircraft Systems: UAVs Design, Development and Deployment. Chichester : Wiley, 2010. 372 p.
2. Valavanis K. P., Vachtsevanos G. J. Handbook of Unmanned Aerial Vehicles. Dordrecht : Springer, 2015. 3020 p.
3. Bonabeau E., Dorigo M., Theraulaz G. Swarm Intelligence: From Natural to Artificial Systems. New York : Oxford University Press, 1999. 320 p.
4. Bekmezci I., Sahingoz O., Temel Ş. Flying ad-hoc networks (FANETs): A survey. *Ad Hoc Networks*. 2013. Vol. 11. № 3. P. 1254–1270. URL: https://doi.org/10.1016/j.adhoc.2012.12.004.
5. Lewis F., Vrabie D., Syrmos V. Optimal Control. Chichester : Wiley, 2012. 552 p.
6. Anderson BDO, Moore JB Optimal Control: Linear Quadratic Methods. Mineola : Dover, 2007. 352 p.
7. Åström K., Wittenmark B. Adaptive Control. 2nd ed. Mineola : Dover, 2013. 576 p.
8. Sutton R. S., Barto A. G. Reinforcement Learning: An Introduction. 2nd ed. Cambridge, MA : MIT Press, 2018. 552 p.
9. Bertsekas D. P. Dynamic Programming and Optimal Control. Belmont, MA. *Athena Scientific*. 2017. Vol. 1-2. 1366 p.
10. Michael N., Fink J., Kumar V. Cooperative manipulation and transportation with aerial robots. *Autonomous Robots*. 2008. Vol. 30. № 1. P. 73–86. URL: https://doi.org/10.1007/s10514-010-9201-3.
11. Olfati-Saber R. Flocking for multi-agent dynamic systems: Algorithms and theory. *IEEE Transactions on Automatic Control.* 2006. Vol. 51. № 3. P. 401–420. URL: https://doi.org/10.1109/TAC.2005.864190.
12. Hendrickx JM, Tsitsiklis JN Convergence of type-symmetric and cut-balanced consensus seeking systems. *IEEE Transactions on Automatic Control*. 2013. Vol. 58. № 1. P. 214–218.
13. Ren W., Beard R. Distributed Consensus in Multi-vehicle Cooperative Control: Theory and Applications. London : Springer, 2008. 316 p.
14. Jadbabaie A., Lin J., Morse A. Coordination of groups of mobile autonomous agents using nearest neighbor rules. *IEEE Transactions on Automatic Control*. 2003. Vol. 48. № 6. P. 988–1001.

15. Ren W., Beard R., Atkins E. A survey of consensus problems in multi-agent coordination. *Proceedings of the American Control Conference*. 2005. P. 1859–1864.
16. Moreau L. Stability of multiagent systems with time-dependent communication links. *IEEE Transactions on Automatic Control*. 2005. Vol. 50. № 2. P. 169–182.
17. Tanner H., Jadbabaie A., Pappas G. Stable flocking of mobile agents. Part I: Fixed topology. *Proceedings of the 42nd IEEE Conference on Decision and Control*. 2003. P. 2010–2015. URL: https://doi.org/10.1109/CDC.2003.1272910.
18. Fax J. A., Murray R. M. Information flow and cooperative control of vehicle formations. *IEEE Transactions on Automatic Control*. 2004. Vol. 49. № 9. P. 1465–1476.
19. Dimarogonas D. V., Kyriakopoulos K. J. Connectedness preserving distributed swarm aggregation for multiple kinematic robots. *IEEE Transactions on Robotics*. 2008. Vol. 24. № 5. P. 1213–1223.
20. Kennedy J., Eberhart R. Particle swarm optimization. *Proceedings of IEEE International Conference on Neural Networks*. 1995. P. 1942–1948.
21. Dorigo M., Stützle T. Ant Colony Optimization. Cambridge, MA : MIT Press, 2004. 328 p.
22. Karaboga D., Basturk B. A powerful and efficient algorithm for numerical function optimization: Artificial bee colony (ABC) algorithm. *Journal of Global Optimization*. 2007. Vol. 39. № 3. P. 459–471. URL: https://doi.org/10.1007/s10898-007-9149-x.
23. Filatov V., Yerokhin A., Zolotukhin O., Kudryavtseva M. The Information Space Model in the Tasks of Distributed Mobile Objects Managing. *Information Extraction and Processing*. 2019. № 47 (123). P. 80-86. URL: https://doi.org/10.15407/vidbir2019.47.080.

УДК 006:355.45 DOI: 10.63978/3083-6476.2025.2.2.07

Крет Микола Анатолійович
начальник науково-дослідного відділу вивчення та впровадження досвіду наукового центру
Військова академія
Одеса, Україна
e-mail: danmerantanta802@gmail.com
ORCID: 0009-0000-8654-599X

Страшков Максим Андрійович
науковий співробітник науково-дослідного відділу вивчення та впровадження досвіду наукового центру
Військова академія
Одеса, Україна
e-mail: mr_stramax@icloud.com
ORCID: 0009-0001-1438-2295

НЕТИПОВІ РІШЕННЯ СТАНДАРТИЗОВАНИХ ПРОЦЕСІВ. ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПЛАНУВАННЯ БОЙОВИХ ДІЙ ШЛЯХОМ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТА АНАЛІТИЧНИХ СИСТЕМ УПРАВЛІННЯ

Анотація. *У статті проаналізовано впровадження інноваційних інформаційно-аналітичних рішень у стандартизовані процеси бойового управління на прикладі бойового досвіду 13-ї бригади оперативного призначення Національної гвардії України. Автори досліджують трансформацію класичних командно-штабних моделей, зокрема обмеження, успадковані від радянської системи управління: надмірну бюрократизацію, відсутність автоматизації та нестачу гнучких інструментів для оперативного аналізу. Представлено практичні приклади інтеграції цифрових рішень – платформи "Дельта" для ситуаційної обізнаності та Power BI як аналітичного інструменту для обробки великих масивів бойових даних. Окрема увага приділена функціонуванню нових організаційних ролей – ISTAR-підрозділів і Battle Captain, які виконують ключову роль у забезпеченні реального часу реагування, координації та синхронізації бойових дій. Стаття ґрунтується на емпіричних даних, зібраних під час роботи зведеної робочої групи в бойових умовах, що надає дослідженню прикладного характеру. Узагальнено рекомендації щодо масштабування ефективної організаційної моделі в інші підрозділи Сил оборони України. Досвід бригади представлено як приклад інституційної ініціативи, де цифрові технології, аналітика й адаптація цивільного досвіду стають основою модернізації системи бойового управління. Запропоновані підходи можуть стати базою для оновлення нормативних документів та подальшої цифрової трансформації командно-штабних структур.*

Ключові слова: *інформаційно-аналітична система, ситуаційна обізнаність, ISTAR, Battle Captain, Power BI, Дельта, бойове управління, автоматизація, Національна гвардія України, планування бойових дій.*

Mykola Kret
Head of the Research Department for the Study and Implementation of Experience,
Scientific Center of the Military Academy
Odesa, Ukraine
e-mail: danmerantanta802@gmail.com
ORCID: 0009-0000-8654-599X

Maksym Strashkov
Research Officer, Research Department for the Study and Implementation of Experience,
Scientific Center of the Military Academy
Odesa, Ukraine
e-mail: mr_stramax@icloud.com
ORCID: 0009-0001-1438-2295

NON-STANDARD APPROACHES TO STANDARDIZED PROCESSES: ENHANCING COMBAT OPERATIONS PLANNING THROUGH ADVANCED INFORMATION AND ANALYTICAL MANAGEMENT SYSTEMS

Abstract.*This article presents a comprehensive analysis of the implementation of innovative information and analytical solutions within standardized combat management processes, focusing on the real-life combat experience of the 13th Operational Brigade of the National Guard of Ukraine. The authors examine the profound transformation of classical command-and-control models that still bear the influence of the Soviet legacy. Key systemic limitations are highlighted, including excessive bureaucratization, manual planning, the lack of modern process automation, and a deficiency of tools for operational data analysis.*

The study explores practical cases of integrating digital platforms into combat operations: the use of the "Delta" situational awareness system for real-time monitoring and visualization of intelligence data; and the application of Power BI for processing and interpreting large volumes of combat-related information, enabling data-driven decision-making in compressed timeframes.

Special attention is paid to the emergence of new organizational approaches driven by the realities of modern warfare – particularly the introduction of ISTAR units (Intelligence, Surveillance, Target Acquisition and Reconnaissance) and the role of the Battle Captain. These roles play a critical part in synchronizing intelligence, command, and firepower in real time, significantly enhancing the responsiveness to dynamic battlefield conditions.

The article is practical in nature, drawing upon empirical data collected during the deployment of a joint operational group in active combat conditions. This allows the authors to formulate specific recommendations for scaling the successful organizational model across other units within the Ukrainian Defense Forces. The experience of the 13th Brigade is presented as a grassroots institutional initiative, where digital technologies, data analytics, and elements of civilian management lay the foundation for a modern, flexible, and adaptive combat management system.

The proposed approaches hold strong potential for regulatory formalization and further digital transformation of command-and-control structures, which is critically important in the context of protracted armed conflict and the need to strengthen operational capabilities.

Keywords: *information-analytical system, situational awareness, ISTAR, Battle Captain, Power BI, Delta, combat control, automation, National Guard of Ukraine, combat planning.*

Вступ

Постановка проблеми. Всупереч більшості оцінок і прогнозів щодо характеру майбутніх збройних конфліктів, динаміка змін форм і методів застосування військ (сил) у ході російсько-української війни є безпрецедентною. Протидія противнику, що має значну перевагу в ресурсах, кількості озброєння та людському потенціалі, можлива лише за умови системного перехоплення та утримання ініціативи – на тактичному, оперативному й стратегічному рівнях. При цьому ініціатива не є вродженою перевагою однієї зі сторін, а формується внаслідок постійного вдосконалення наявних методів, розробки нових підходів та гнучкого застосування набутих знань і досвіду.

Одним із ключових факторів, що сприяють появі нетипових рішень у стандартизованих військових процесах, стало залучення до формування Сил оборони України фахівців із

цивільним досвідом у сфері ІТ, аналітики, управління проєктами та інших галузей. Це дозволило реалізувати низку ініціатив, які або набули загальновійськового масштабу (наприклад, системи "Кропива", "Дельта"), або залишилися локальними, проте демонструють високу ефективність в умовах конкретного оперативного середовища.

Разом із тим, класичні підходи до бойового управління, успадковані з радянської моделі, виявляють суттєві обмеження в умовах сучасного високодинамічного бою. Зокрема, це стосується громіздких процедур документообігу, низького рівня автоматизації, обмеженої гнучкості реагування та відсутності інструментів оперативного аналізу. У таких умовах виникає об'єктивна потреба у впровадженні нових інформаційно-аналітичних систем, які забезпечують не лише ситуаційну обізнаність у реальному часі, а й можливості глибокого стратегічного аналізу, оцінки тенденцій, візуалізації рішень і синхронізації дій між різними ланками управління.

Актуальність дослідження зумовлена необхідністю систематизації та узагальнення передового досвіду впровадження таких рішень у бойову практику, насамперед на прикладі однієї з бригад Національної гвардії України. Йдеться про практичне поєднання ситуаційних платформ (як-от "Дельта"), аналітичних інструментів (Power BI), нових ролей управління (Battle Captain) та розвідувальних структур (ISTAR) в єдину систему, здатну ефективно функціонувати в умовах сучасного конфлікту.

Аналіз останніх досліджень і публікацій. Питання інформаційно-аналітичної підтримки управління військами, побудови автоматизованих систем ситуаційної обізнаності та впровадження інноваційних методів планування бойових дій не є новими у вітчизняному науковому просторі. Починаючи з початку 2010-х років, у дослідженнях українських військових науковців активно формувалося розуміння необхідності трансформації командно-штабних процедур, цифровізації управлінських процесів і підвищення ролі аналітики в оперативному плануванні.

У цьому контексті заслуговують на особливу увагу роботи Власюка В. [1], Бобилова В. [2], Бабкова Ю. [3], Беспалька О., Маслюка Л. [5], Бондарчука С. [6] та інших дослідників. У своїх публікаціях вони наполегливо розробляли підходи до концептуального обґрунтування вимог до сучасних систем управління, вивчали потенціал імітаційного моделювання, досліджували інформаційну підтримку прийняття рішень у структурах Національної гвардії, аналізували перспективи створення ситуаційних центрів і застосування мережецентричних концепцій у збройних конфліктах нового типу.

Варто підкреслити, що для свого часу – переважно 2016-2021 років – ці праці мали прогресивний, випереджальний характер. У багатьох із них окреслено проблеми, які тоді лише починали визрівати, але після 2022 року стали критичними: надмірна бюрократизація бойового управління, низький рівень автоматизації аналітики, відсутність горизонтальної координації між підрозділами, дефіцит інструментів для динамічного прийняття рішень. Автори не лише виявляли ці слабкі місця, а й пропонували проєктні рішення, описували моделі впровадження, прогнозували очікувану ефективність – саме на базі тодішніх технологічних і організаційних реалій.

Хоча ці роботи за своєю сутністю є переважно теоретичними або модельними, вони виконали важливу функцію – заклали інтелектуальний фундамент для тих змін, які пізніше стали необхідністю. Можна стверджувати, що саме завдяки напрацюванням попередників і ретельному аналізу запропонованих ними рішень з'явилася можливість переосмислити й адаптувати ці підходи до нових викликів – війни великої інтенсивності, багатовимірного фронту, тотального застосування БПЛА, розвідки та кіберзагроз.

Разом із тим, істотним обмеженням проаналізованих праць є їхня приналежність до довоєнної аналітичної парадигми. Пропоновані там підходи орієнтовані на більш передбачувані, симетричні сценарії конфліктів, з чіткими межами відповідальності, стабільними каналами зв'язку та умовно "чистим" інформаційним простором. Більшість

технологічних рішень, що аналізуються в цих роботах, – це або застарілі програмні продукти (локальні БД, десктопні середовища, окремі ГІС-системи), або модулі, які не мають здатності до масштабування, адаптації в бойових умовах та інтеграції з сучасними платформами типу "Дельта".

Крім того, в теоретичних публікаціях 2010-х років відчутна відсутність практичного компоненту – мова йде про прогнозовану ефективність, очікувані результати, концептуальні моделі впровадження, але не про апробовані в реальних бойових умовах системи. Тобто, тоді ще не йшлося про практичну перевірку навантажувальних властивостей, цифрової стійкості, гнучкості при зміні тактичної обстановки, людського фактору, постійної ротації особового складу тощо.

У цьому контексті об'єктом аналізу в межах даного дослідження виступає приклад впровадження елементів інформаційно-аналітичної системи управління XX бригади Національної гвардії України. Йдеться не про експериментальну модель чи концептуальний проєкт, а про діючу організаційну систему, що функціонує безпосередньо в умовах бойових дій та забезпечує повний цикл управлінських процесів: планування, координацію та аналіз обстановки у режимі постійного оперативного чергування.

Зазначені організаційно-технічні рішення не були прямо передбачені в попередніх наукових розробках, однак за своїм характером демонструють зв'язок із теоретичними положеннями, які висвітлювались у проаналізованих публікаціях попередніх років. Зокрема, спостерігається спадкоємність у питанні необхідності підвищення гнучкості управлінських структур, інтеграції аналітики в процес ухвалення рішень та оптимізації інформаційних потоків між рівнями управління.

Таким чином, отриманий досвід не суперечить наявній науковій традиції, а виступає її емпіричним продовженням. Дослідження спрямоване на документування та аналіз впроваджених рішень, що функціонують у бойових умовах і, на відміну від попередніх теоретичних моделей, дозволяють оцінити ефективність інформаційно-аналітичної підтримки управління на практиці.

Метою статті є аналіз практичного досвіду впровадження нетипових організаційно-технічних рішень у межах стандартизованих процесів бойового управління, зокрема – інтеграції інформаційних та аналітичних систем у діяльність XX бригади оперативного призначення НГУ. Дослідження спрямоване на виявлення факторів, що сприяють підвищенню ефективності планування та управління бойовими діями в умовах активних бойових дій, а також на обґрунтування доцільності масштабування подібних підходів у межах інших підрозділів Сил оборони України.

Виклад основного матеріалу

У період з 14 до 21 травня 2025 року зведеною робочою групою (ЗРГ) було здійснено аналіз проблематики, визначеної в бойовому розпорядженні старшого начальника. Робота проводилась комплексно, із залученням різних методів збору та перевірки інформації, зокрема:

– особисте спостереження за організацією бойового управління на командному пункті;

– проведення інтерв'ювання з представниками оперативного складу, відповідальними за планування дій та ведення бойових документів;

– анкетування та опитування фахівців структурних підрозділів, що здійснюють організацію, ведення та інформаційне наповнення інформаційних систем.

Зібрані матеріали дозволили виявити успішні практики у використанні ІСУ в умовах оперативного застосування підрозділів. Окрема увага приділялась оцінці функціональності програмних рішень, організації обміну інформацією в реальному часі, ступеню інтеграції

систем між різними рівнями управління та відповідності практичного застосування вимогам нормативно-правових документів.

Результатом роботи зведеної робочої групи стало чітке розуміння ключової ролі автоматизованих систем у процесах планування, ведення бойових дій і узагальнення їхніх результатів. За оцінками членів ЗРГ та оперативного складу основного командного пункту (ОКП), ефективне функціонування бойового управління стало можливим завдяки інтеграції двох типів інформаційних систем:

- систем візуалізації оперативної обстановки (ситуаційної обізнаності);
- систем збору, обробки, аналізу та структуризації інформації.

Система візуалізації оперативної обстановки (ситуаційної обізнаності)

На рівні бригади основною платформою ситуаційної обізнаності є інформаційна система "Дельта", яка широко апробована і використовується у більшості підрозділів Сил оборони України. Водночас, 13-та бригада оперативного призначення Національної гвардії України реалізувала нові підходи до управління, що дозволили досягти вищого рівня оперативності, узгодженості та точності бойових рішень.

Особливістю тактичного операційного центру (ТОЦ) 13-ї бригади, яка відрізняє його від аналогічних командних пунктів інших бригад, є фактична імплементація підрозділу *ISTAR* та введення посади *Battle Captain*.

ISTAR: структура та функціонування

ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) – це концепція, що об'єднує розвідку, спостереження, виявлення цілей і розвідку в бою. У практиці Збройних Сил НАТО (Канада, Велика Британія), ISTAR – це високоспеціалізований бойовий елемент, відповідальний за отримання, обробку, аналіз і передачу розвідувальної інформації, необхідної для ухвалення рішень на тактичному та оперативному рівнях.

У 13-й бригаді оперативного призначення ISTAR реалізовано на двох рівнях: батальйонному та бригадному ISTAR, який підпорядковується черговому Battle Captain.

Основні функції ISTAR батальйону:

- збір інформації про противника, місцевість та бойову обстановку;
- постійний моніторинг визначених секторів – переважно за допомогою відеосигналу з безпілотних літальних апаратів;
- виявлення, класифікація та пріоритизація цілей для ураження;
- первинна аналітична обробка даних.

Комплектування ISTAR батальйону здійснюється за рахунок наявних розвідувальних підрозділів батальйону, що дозволяє інтегрувати цю функцію в загальну структуру бойового управління.

ISTAR бригади

Цей підрозділ підпорядковується черговому Battle Captain, працює у 12-годинних змінах і виконує аналогічні до батальйону функції, однак на рівні бригадного управління. Основна відповідальність – перевірка коректності нанесення інформації на загальну картину ситуаційної обізнаності (оперативну мапу), а також внесення уточнень і коректив. Фактично ISTAR бригади виступає радником Battle Captain'а з питань бойового управління на визначених напрямках. Комплектування і навчання ISTAR бригади відбувається за рахунок розвідувального батальйону бригади.

Важливим аспектом у вивченні та узагальненні досвіду стало дослідження підготовки ISTAR-фахівців та вимог до кандидатів. Станом на час перебування ЗРГ, всі ISTAR-оператори бригадного і батальйонного рівня були мобілізованими військовослужбовцями без попередньої військової розвідувальної спеціалізації, з різними цивільними професіями. За словами чергового Battle Captain, повний цикл підготовки

ISTAR-фахівця триває орієнтовно 2 тижні та включає обов'язкове стажування на посаді ISTAR батальйону.

Найбільш критичною проблемою в організації підрозділів ISTAR є відсутність штатних посад. Комплектування здійснюється виключно за рахунок особового складу, призначеного на інші функції, зокрема дешифрувальників у розвідувальних підрозділах. Це створює додаткове навантаження на особовий склад і знижує формалізований контроль за підготовкою та ротацією ISTAR-груп.

Досвід 13-ї бригади оперативного призначення НГУ свідчить про ефективність впровадження структур ISTAR у бойове управління, особливо в умовах використання сучасних автоматизованих систем. Для масштабування цієї практики на інші підрозділи Сил оборони України, з метою забезпечення своєчасної, точної, перевіреної розвідувальної інформації для ухвалення оперативних рішень, ведення точного вогню, уникнення втрат серед власних сил і підтримки ситуаційної обізнаності на всіх рівнях управління доцільним є:

– офіційне закріплення ISTAR-структур у штатах бригад;

– розробка стандартизованої програми підготовки ISTAR-фахівців.

Battle Captain – це офіцер тактичного рівня, який відповідає за безперервне управління бойовими діями безпосередньо з основного командного пункту (ОКП) підрозділу. Ця функція реалізується на ротаційній основі, як правило, в 12–годинному режимі чергування, і є ключовим елементом оперативного управління поточною обстановкою на напрямку.

Для чіткого розуміння ролі Battle Captain у сучасній структурі управління, зокрема в межах діяльності командного пункту бригади, слід зазначити: Battle Captain фактично виконує частину функцій оперативного чергового, однак його відповідальність звужена виключно до питань бойової обстановки, оперативного реагування та взаємодії з ISTAR-групою.

Паралельно з Battle Captain на ОКП функціонує оперативний черговий, який відповідає переважно за документообіг, супровід бойових наказів, ведення журналів, адміністративне забезпечення та комунікацію з вищим командуванням. Такий розподіл обов'язків дозволяє максимально ефективно розділити бойову роботу та документообіг, уникнути перевантаження одного офіцера та забезпечити постійний контроль над ситуацією.

Організація робочих місць та технічне забезпечення

З міркувань безпеки, фото і відеофіксація робочих місць Battle Captain, ISTAR-групи та оперативного чергового заборонена, однак спостереження зведеної робочої групи дозволяють окреслити основні характеристики організації цих приміщень.

Робоче місце Battle Captain та ISTAR-групи:

1) Оснащене сучасними цифровими засобами: ноутбуки, планшети, монітори, телевізори великого формату, сенсорні панелі, окремі інформаційні панелі за напрямками.

2) Безперервний захищений зв'язок із підрозділами ISTAR на рівні батальйону.

3) Виключене використання паперових документів: відсутні принтери, роздруківки, журнали – уся інформація обробляється, виводиться та оновлюється в цифровому форматі.

4) Основним джерелом інформації є система ситуаційної обізнаності "Дельта", яка працює у багаторівневому режимі з поділом доступу за напрямками та пріоритетами. Уся техніка (планшети, телевізори, монітори) синхронізована з "Дельтою", забезпечуючи повну оперативну картину поля бою.

Робоче місце оперативного чергового:

1) Має класичну адміністративну організацію, характерну для типових пунктів управління.

2) У приміщенні переважають паперові носії інформації: журнали обліку, стікери, друковані телеграми, шаблони донесень тощо.

3) Постійно присутні помічники чергового, які займаються обробкою поточних донесень, складанням рапортів, оформленням супровідних документів та взаємодією зі штабом.

У процесі трансформації структури бойового управління 13-ї бригади оперативного призначення Національної гвардії України впровадження функції Battle Captain стало критичним кроком до підвищення оперативності, цифровізації та точності управління бойовими діями.

Така модель чітко розділяє бойову, інформаційно–аналітичну та документаційно-адміністративну діяльність, дозволяючи зосередити зусилля на кожному напрямку окремо. Вона є перспективною для розширеного впровадження в інших бригадах Сил Оборони України.

Система збору, обробки, аналізу та структуризації інформації

За аналітичну складову у 13-ій бригаді оперативного призначення Національної гвардії України відповідає інструмент Power BI, запозичений з комерційного сектору та адаптований під аналітичні потреби бригади.

Вибір Power BI як основного інструменту аналітичної обробки та візуалізації даних у підрозділі бригадного рівня був зумовлений насамперед відсутністю функціонально подібних платформ у чинному програмно-технічному забезпеченні Сил оборони та Сил безпеки України.

На сьогодні найбільш розвиненою, масштабованою та широко впровадженою системою ситуаційної обізнаності в Збройних Силах України є платформа “Дельта”. Вона перебуває у стані постійного вдосконалення, активно розвивається як за функціоналом, так і за інтеграційними можливостями. Однак, на поточному етапі свого технічного та архітектурного розвитку, “Дельта” не дозволяє ефективно обробляти й візуалізувати великі обсяги накопичених даних, що є критично важливим для глибокого стратегічного аналізу та прогнозування.

Зокрема, у рамках попередніх спроб, здійснених аналітиками відділення планування бригади, проводилось тестування функціоналу “Дельти” для відображення динаміки вогневих уражень з боку противника та власних сил у розрізі застосування артилерії та безпілотних авіаційних комплексів. Метою була побудова цілісної картини щільності, інтенсивності й напрямків бойового впливу на ділянках фронту протягом тривалого періоду.

Втім, ці спроби виявили системні обмеження платформи “Дельта”, пов’язані з технічною складністю візуалізації значного обсягу історичних подій. Із розширенням часової вибірки – наприклад, понад один місяць – спостерігається різке збільшення кількості елементів, що мають бути одночасно відображені на карті. Це, у свою чергу, спричиняє зниження продуктивності, зависання системи або її тимчасову зупинку.

Зі слів старшого офіцера відділення планування, “Дельта” наразі технічно здатна стабільно працювати лише з інформацією в межах 30-денного періоду. Спроба роботи з більш глибокими аналітичними горизонтами – наприклад, у розрізі кварталів або років – є нереалізованою через перевантаження даними, нестачу ресурсів обробки або недосконаліть механізмів фільтрації на великих масштабах.

У зв’язку з цим виникла об’єктивна потреба в альтернативному рішенні для накопичення, систематизації, аналізу та візуального подання інформації, з можливістю інтеграції великої кількості записів за довготривалий період часу. Саме тому було обрано платформу Power BI, яка забезпечує гнучкість у роботі з великими даними, широкі можливості побудови складних графіків, автоматизованих звітів, фільтрації за будь-якими параметрами та візуалізації змін у динаміці.

Таким чином, застосування Power BI дозволяє закрити аналітичний дефіцит, не дублюючи, а доповнюючи можливості "Дельти", особливо в контексті стратегічного аналізу та узагальнення бойового досвіду на рівні бригади. Power BI – це потужна платформа бізнес-аналітики від корпорації Microsoft, яка дозволяє об'єднувати, обробляти, аналізувати та візуалізувати великі масиви даних із різних джерел в інтерактивній формі. Основною перевагою Power BI є здатність перетворювати необроблені дані на зрозумілу, візуально структуровану інформацію, що слугує базою для ухвалення ефективних управлінських рішень.

Попри його первинне цивільне призначення, Power BI активно впроваджується у державному, оборонному та безпековому секторах багатьох країн-членів НАТО, а його можливості відкривають нові перспективи і для структур Збройних Сил України.

Основні функціональні можливості Power BI:

– збір та об'єднання даних із різноманітних джерел: Excel, бази даних SQL, хмарні платформи, Google Sheets, REST API тощо;

– обробка та очищення даних без необхідності програмування (через Power Query);

– побудова інтерактивних візуалізацій: графіки, діаграми, карти, гістограми, матриці тощо;

– оновлення даних у реальному часі, підтримка динамічних фільтрів і KPI-індикаторів;

– поширення аналітичних звітів через браузер, мобільні додатки або вбудовування у внутрішні портали.

Потенційне застосування Power BI в системі ЗСУ

1. Оперативне управління та ситуаційна обізнаність:
   а) аналітика переміщення підрозділів, ліній зіткнення, зон відповідальності;
   б) оцінка щільності вогню, втрат, логістичних вузлів.
2. Логістика та забезпечення:
   а) контроль за станом запасів (ПММ, БК, ЗІП), облік залишків на складах;
   б) відстеження маршрутів постачання, виявлення "вузьких місць";
   в) аналіз ефективності логістичних операцій.
3. Персонал та навчання:
   а) аналітика обліку особового складу: ротації, втрати, дисциплінарні показники;
   б) моніторинг результатів бойової підготовки;
   в) звіти про відвідуваність, успішність, допуски та сертифікацію військовослужбовців.
4. Медичне забезпечення:
   а) аналіз потреб у медичному евакуаційному транспорті;
   б) візуалізація захворюваності, поранень, потреб у медикаментах;
   в) контроль за розгортанням і завантаженням стабілізаційних пунктів.
5. Кіберзахист та інформаційна безпека:
   а) зведення інцидентів інформаційної безпеки;
   б) виявлення тенденцій у кібератаках та проникненнях;
   в) візуалізація навантаження на IT-інфраструктуру підрозділів.

Перевага	Значення
Інтерактивність	Користувач може самостійно змінювати фільтри, діапазони часу, джерела даних
Візуальна простота	Складні дані подаються у вигляді графіків, що легко сприймаються навіть без аналітичної освіти

Перевага	Значення
Оновлення в реальному часі	Підтримка критичних для бойових рішень оновлень без затримок
Швидке розгортання	Не потребує складної IT-інфраструктури – працює на ПК або в браузері
Безпека даних	Підтримка шифрування, керування доступом, інтеграція з Azure і Microsoft 365

Висновки

Досвід 13-ї бригади оперативного призначення Національної гвардії України є яскравим прикладом інституційної ініціативи та організаційної гнучкості в умовах війни, що триває. На відміну від формального впровадження інструментів "згори", у цій бригаді вдалося реалізувати повноцінну інтеграцію цифрових технологій, нестандартних управлінських підходів та нових організаційних ролей на основі внутрішнього попиту і логіки бойових завдань.

Використання Power BI виникло не з теоретичних міркувань, а як практична відповідь на функціональні обмеження системи "Дельта". Попри свої сильні сторони в оперативному управлінні, "Дельта" не здатна ефективно працювати з великим обсягом історичних даних. Power BI дозволив заповнити цю прогалину, ставши інструментом для поглибленої аналітики, побудови динамічних звітів, візуалізації трендів та історичного аналізу дій противника і власних сил. Замість дублювання функцій, Power BI логічно доповнив "Дельту", перетворивши її з ізольованої платформи ситуаційної обізнаності на частину комплексної аналітичної екосистеми.

Особливу увагу командування бригади приділило залученню та утриманню фахівців із цивільним досвідом у сфері IT та аналітики. Умови служби для таких військовослужбовців адаптовані до особливостей їхньої роботи: створено комфортне, технічно оснащене робоче середовище, максимально наближене до звичного "офісного" формату. Це не лише сприяє утриманню таких фахівців у підрозділі, але й запобігає професійному вигоранню, зберігаючи високу мотивацію на тривалий період. У бригаді не зафіксовано випадків втрати ключових кадрів через дезадаптацію або перевтому.

Упровадження ролі Battle Captain стало інноваційним елементом в організації бойового управління. Цей офіцер не просто є черговим на командному пункті – він виконує функції оперативного координатора бою, має повноваження на тимчасове блокування ризикованих дій, відповідає за синхронізацію дій усіх наявних засобів ураження, розвідки та піхотних підрозділів. Його присутність дозволяє усунути розрив між рівнем оперативного командування та тактичним виконанням. Це практична адаптація концепції Joint Fires Officer з армії США, реалізована у форматі, максимально наближеному до українських реалій.

Додатковою силою у системі управління є впровадження ISTAR-груп – структур, що відповідають за збір, перевірку, обробку та візуалізацію розвідувальної інформації з різних джерел (БПЛА, спостереження, технічні засоби). Існування ISTAR як на рівні батальйону, так і на рівні бригади, дозволяє забезпечити точність, актуальність і оперативність даних для Battle Captain і командування. Це критично важливо в умовах інформаційного перевантаження і постійно змінної бойової обстановки.

Відмова від використання Power BI або "Дельти" для моделювання бойових сценаріїв пояснюється не обмеженнями інструментів, а правильним розумінням їхнього призначення. У бригаді для моделювання використовується варгеймінг – структурований імітаційний метод, який дозволяє програти сценарії дій з урахуванням людського чинника, непередбачуваності та розвідданих. Залучення фізичних макетів, офіцерських суджень і

модераторської оцінки дозволяє досягти набагато реалістичніших і точніших висновків, ніж цифрові симуляції, які не встигають за розвитком засобів ураження та новітніх форм бойових дій.

Бригада створила організаційну модель, яка вже викликає зацікавлення в інших частинах – зокрема, досвід переймають 3-тя штурмова бригада, 93-тя механізована тощо. Такий інтерес демонструє потенціал до масштабування цього підходу в межах усієї системи Сил оборони. Найважливіше – це не окремі інструменти, а спосіб мислення: в основі цієї моделі лежить командирський карт-бланш, довіра до ініціативи офіцерів, делегування повноважень, гнучке планування та швидке ухвалення рішень.

Досвід 13-ї бригади НГУ – це не лише про технології чи інновації. Це приклад того, як оперативна логіка, довіра до фахівців, автономія прийняття рішень та гнучке поєднання цивільних і військових практик можуть якісно змінити бойове управління. Саме на таких ініціативах формується армія нового покоління – спроможна діяти не лише за наказом, а й за сенсом. І саме тому цей досвід заслуговує на подальше вивчення, підтримку та доктринальне закріплення.

Список літератури

1. Власюк В. Інформаційно-аналітичні основи формування концепції обґрунтування вимог до системи управління для підтримання заданого рівня боєздатності військ (сил). *Сучасні інформаційні технології у сфері безпеки та оборони.* 2024. № 51 (3). С. 89-95. URL: https://doi.org/10.33099/2311-7249/2024-51-3-89-95.
2. Бобилов В., Мельник Я., Кравчук А. Підвищення ефективності підтримки прийняття рішень в автоматизованих системах управління військами за рахунок застосування в її роботі засобів імітаційного моделювання бойових дій військ (сил). *Сучасні інформаційні технології у сфері безпеки та оборони.* 2019. № 34 (1). С. 19-22. URL: https://doi.org/10.33099/2311-7249/2019-34-1-19-22.
3. Бабков Ю. П., Горєлишев С. А., Побережний А. А. Комплексний підхід до використання елементів інформаційно-аналітичної системи для підтримки прийняття рішень на застосування угруповань Національної гвардії України. *Збірник наукових праць Національної академії Національної гвардії України.* 2015. № 1 (25). С. 73-82. URL: https://doi.org/10.33405/2409-7470/2015/1/25/139509.
4. Беспалько О. В., Кучеренко Ю. Ф., Власік С. М., Закіров З. З., Ткаченко В. І. Інформаційні війни сучасності та застосування мережецентричних систем управління військового призначення. *Системи озброєння і військова техніка.* 2023. № 74. С. 61-66. URL: https://doi.org/10.30748/soivt.2023.74.09.
5. Маслюк Л., Гавалко В., Колодяжний А., Джигомон С. Інформаційно-аналітична підтримка організації роботи органів військового управління під час планування операції. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 47 (2). С. 75-84. https://doi.org/10.33099/2311-7249/2023-47-2-75-84.
6. Бондарчук С., Васюхно С., Галаган В., Гріненко О. Пропозиції щодо організації інформаційно-аналітичної підтримки ведення проєктів інформатизації. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського.* 2021. № 3 (73). С. 68-73. https://doi.org/10.33099/2304-2745/2021-3-73/68-73.
7. Pavlyshenko D., Pavlyshenko B. Predictive Analytics of Air Alerts in the Russian-Ukrainian War. arXiv preprint. 2024. arXiv:2411.14625. URL: https://doi.org/10.48550/arXiv.2411.14625.
8. Li Y., Lin Z., Wang X., Liu C., Wu L., Zhang F. A real-time battle situation intelligent awareness system based on Meta-learning & RNN. arXiv preprint. 2025. arXiv:2501.13704. URL: https://doi.org/10.48550/arXiv.2501.13704.

УДК:355.48:623.746:351.862(477) DOI: 10.63978/3083-6476.2025.2.2.08

Шаптала Сергій Олександрович
Громадська організація "Центр воєнної стратегії і технологій"
Київ, Україна
e-mail: smokliak@ukr.net
ORCID: 0000-0002-0348-4050

Романенко Євген Олександрович
доктор наук з державного управління, професор, провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
Київ, Україна
e-mail: poboss1978@gmail.com
ORCID: 0000-0003-2285-0543

Гурковський Володимир Ігорович
доктор наук з державного управління, професор, начальник відділу
Центральний науково-дослідний інститут Збройних Сил України
Київ, Україна
e-mail: volodymyr.gurkovskyi@gmail.com
ORCID: 0000-0003-2021-5204

БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ В АСИМЕТРИЧНІЙ ВІЙНІ: ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ТА СТРАТЕГІЧНА РОЛЬ У ПРОТИСТОЯННІ ТЕХНОЛОГІЧНІЙ ЕСКАЛАЦІЇ РОСІЇ

Анотація. *Стаття присвячена дослідженню масштабного застосування безпілотних літальних апаратів (БПЛА) у російсько-українській війні, де дрони стали ключовим елементом асиметричної стратегії України в умовах технологічної ескалації росії, зокрема з появою реактивних Shahed-238 ("Герань-3"). Описано технічні характеристики, класифікацію та тактичне використання ударних, розвідувальних, імітаційних і перехоплювальних БПЛА обома сторонами конфлікту. Зазначено, що рф активно нарощує виробництво дронів-камікадзе типу Shahed і нових моделей, таких як "Бандероль", із використанням іноземних компонентів, зокрема китайських та іранських. Натомість Україна демонструє інноваційність, розробляючи дрони-перехоплювачі, автономні системи виявлення та технології штучного інтелекту, що забезпечують ефективну протидію ворогу.*

Особливу увагу приділено зміні тактики бойових дій: від масованих наступів до точкових ударів малими мобільними групами під прикриттям БПЛА. Українська стратегія спирається на швидку адаптацію, волонтерську мобілізацію та технічну креативність, що дозволяє компенсувати обмеженість ресурсів. Поява реактивних Shahed-238 із високою швидкістю та дальністю польоту створює нові виклики для української ППО, вимагаючи розвитку реактивних перехоплювачів і модернізації оборонних систем.

Стаття підкреслює, що безпілотники кардинально змінили характер війни, створивши "зону ураження" вздовж лінії фронту та змістивши акцент із чисельної переваги на технологічну. Описано, як інтеграція штучного інтелекту та комп'ютерного зору в БПЛА, таких як українські "Ватра" чи російські V2U, формує нову фазу війни, де автономність і точність стають визначальними. Висновки акцентують на тому, що успіх України в асиметричному протистоянні залежить від поєднання інновацій і міжнародної підтримки, що дозволяє нейтралізувати зростаючу загрозу реактивних дронів.

Ключові слова: *безпілотники, БПЛА, асиметрична війна, FPV, Shahed-238, дрони-перехоплювачі, війна технологій, штучний інтелект, інновації, ГУР МОУ.*

Serhiy Shaptala
Non-Governmental Organization
"Center for Military Strategy and Technologies"
Kyiv, Ukraine
e-mail: smokliak@ukr.net
ORCID: 0000-0002-0348-4050

Yevhen Romanenko
Doctor of Science in Public Administration, Professor
Colonel, Leading Researcher,
Central Research Institute
Armed Forces of Ukraine
Kyiv, Ukraine
e-mail: poboss1978@gmail.com
ORCID: 0000-0003-2285-0543

Volodymyr Gurkovsky
Doctor of Science in Public Administration, Professor
Colonel, Head of Department,
Central Research Institute
Armed Forces of Ukraine
Kyiv, Ukraine
e-mail: volodymyr.gurkovskyi@gmail.com
ORCID: 0000-0003-2021-5204

UNMANNED AERIAL VEHICLES IN ASYMMETRIC WARFARE: TECHNICAL CAPABILITIES AND STRATEGIC SIGNIFICANCE IN COUNTERING RUSSIA'S TECHNOLOGICAL ESCALATION

Abstract. *This article investigates the extensive use of unmanned aerial vehicles (UAVs) in the Russia-Ukraine war, where drones have become a pivotal component of Ukraine's asymmetric strategy amid Russia's technological escalation, particularly with the emergence of jet-powered Shahed-238 ("Geran-3") drones. It provides a detailed description of the technical characteristics, classification, and tactical applications of combat, reconnaissance, decoy, and interceptor UAVs employed by both sides of the conflict. The study highlights Russia's ramped-up production of kamikaze drones like Shahed and new models such as "Banderol," incorporating foreign components, notably from China and Iran. In contrast, Ukraine showcases innovation through the development of interceptor drones, autonomous detection systems, and AI-driven technologies to counter the enemy effectively.*

The article emphasizes the shift in battlefield tactics from large-scale offensives to precision strikes by small mobile units supported by UAVs. Ukraine's strategy relies on rapid adaptation, volunteer mobilization, and technical ingenuity to offset resource constraints. The introduction of high-speed, long-range Shahed-238 drones poses new challenges for Ukraine's air defense, necessitating the development of jet-powered interceptors and advanced defense systems.

The study underscores that UAVs have fundamentally transformed the nature of warfare, creating a "kill zone" along the front line and shifting the focus from numerical superiority to technological dominance. It describes how the integration of artificial intelligence and computer vision in UAVs, such as Ukraine's "Vatra" or Russia's V2U, marks a new phase of warfare where autonomy and precision are paramount. The conclusions highlight that

Ukraine's success in this asymmetric conflict hinges on combining innovation, and international support to neutralize the growing threat of jet-powered drones.

Keywords: *drones, UAVs, asymmetric warfare, FPV, Shahed-238, interceptor drones, technological warfare, artificial intelligence, innovation, HUR of Ukraine.*

Вступ

Постановка проблеми. Сучасний конфлікт у небі характеризується масовим застосуванням безпілотників обома сторонами. Рф активно нарощує виробництво БПЛА та щоденно завдає масованих ударів по українських містах, в той час як Україна лідирує у бойовому застосуванні дронів: з території рф атакує стратегічні аеродроми, а на фронті відбиває просування ворога безпілотниками. Обидві сторони віддають перевагу недорогим високоточним рішенням: для України дрони стали дешевою альтернативою ракеті, а рф випускає баражуючі боєприпаси і FPV-"камікадзе" у сотні разів більше, ніж до 2022 року. Така гонка провокує ескалацію та асиметричне протистояння: масові удари дешевими безпілотниками розмивають традиційну перевагу супротивника у живій силі та техніці.

Україна залишається лідером у використанні безпілотників на полі бою. Вона запускала безпілотники з території росії для ударів по стратегічних авіабазах, знищуючи бомбардувальники. Київ також розгорнув дрони для руйнівного ефекту на лінії фронту, запобігаючи російським наступам, та для ударів по життєвоважливій інфраструктурі в глибині російської території. Рф наздогнала і максимізує виробництво та використання безпілотників, але вони роблять це традиційним способом. Українцям вдається не відставати у війні безпілотників, реагуючи асиметрично.

Дрони виявилися недорогою альтернативою високоточній зброї. Зростання у всіх категоріях випущених росією баражуючих боєприпасів та FPV-дронів порівняно з показниками до 2022 року, збільшення на кілька порядків. Держава-агресор активно нарощує виробництво безпілотників, що дозволяє їй щоденно завдавати масованих ударів по українських містах. Це відбувається на тлі просування її військ на полі бою та посилення тиску на Київ з метою змусити його до мирних умов. Про це пише Bloomberg [1].

Кремль спричиняє смертоносні руйнування, зокрема в Києві та Одесі, випускаючи сотні безпілотників щоночі. Лише за одну ніч Україна зафіксувала 315 безпілотників та сім ракет, а попередньої ночі – рекордні 479 БПЛА. Москва неухильно збільшувала кількість атак безпілотниками з початку року, досягнувши в лютому щоденного рекорду у 267 БПЛА. Після початкового відставання від України у розробці дронів після повномасштабного вторгнення 2022 року, країна-агресор послідовно нарощувала масове виробництво іранських БПЛА Shahed та інших типів безпілотних літальних апаратів.

Президент росії володимир путін у квітні наказав виробникам оборонної продукції прискорити випуск безпілотників, оскільки, за його словами, "цієї зброї, як і раніше, не вистачає". Він також закликав Росію "стати одним зі світових технологічних лідерів" у виробництві безпілотників до 2030 року.

Мета Москви – використовувати "стратегію покарання" з недорогими "Шахедами", щоб змусити Київ підкоритися. Хоча Україна збиває більшість із них, ця зброя "перевантажує українську ППО та підриває моральний дух цивільного населення за допомогою постійних нічних атак", – йдеться у звіті Центру стратегічних та міжнародних досліджень.

За оцінками України, рф готується виробляти від 300 до 350 безпілотників дальнього радіусу дії на день і прагне збільшити випуск до 500 одиниць на день. Російські виробники дронів зуміли збільшити виробництво літальних апаратів великої дальності до понад 30 000 цього року (з 15 000 у 2024 році), а також випустити до 2 мільйонів малих

тактичних безпілотників, що використовуються проти танків та артилерії. Українська військова розвідка також звинуватила росію у використанні електроніки здебільше з Китаю, порушуючи санкції [1].

І Україна, і рф прагнуть впроваджувати недорогі високоефективні технології, часто заради навіть незначної переваги на полі бою.

Мета статті: дослідити роль БПЛА у формуванні асиметричної стратегії України в умовах технологічної ескалації росії з особливим акцентом на появу реактивних дронів Shahed-238 (“Герань-3”); надати детальний опис технічних характеристики сучасних БПЛА, включаючи ударні, розвідувальні, імітаційні та перехоплювальні моделі та їхній вплив на тактику бойових дій, обороноздатність і темпи технологічної адаптації; з’ясувати виклики, пов’язані з протидією високошвидкісним реактивним дронам. Окремо розглянуто, чому саме асиметричне використання БПЛА дало змогу Україні стримувати противника в умовах обмежених ресурсів. Також стаття окреслює тенденції, які формують нову логіку ведення війни – через швидкі інженерні рішення, креативність та пошук переваги в небі.

Ця стаття поєднує підходи з кількох суміжних галузей: військової справи, державного управління, національної безпеки. Такий міждисциплінарний підхід дозволяє не лише описати технічні характеристики дронів, а й показати, як вони впливають на тактику бою, оборонне планування та стійкість держави до нових типів загроз.

У процесі підготовки статті використано матеріали з відкритих джерел, зокрема публікації міжнародних медіа (Bloomberg, Reuters), аналітичні огляди ГУР МОУ, Центру стратегічних і міжнародних досілжень, а також технічні описи з профільних військових платформ. Важливу роль відіграли спостереження за практичним застосуванням дронів на фронті – як з боку України, так і країни-агресора.

У статті застосовано описовий і порівняльний підхід. Дрони класифіковано за типами та призначенням (ударні, розвідувальні, імітаційні, перехоплювачі), що дозволило показати різницю у цілях, характеристиках і способах їхнього використання. Особливу увагу приділено технічним параметрам БПЛА, які згадуються у звітах та відкритих технічних описах, зокрема – потужність боєвої частини, дальність дії, способи наведення та стійкість до РЕБ, складнощі перехоплення реактивних Shahed-238 (“Герань-3”). Стаття уникає суб’єктивних оцінок, надаючи перевагу фактичному опису функціональних характеристик, тактичних особливостей і статистичних даних.

Матеріал статті структуровано так, щоб показати, як перманентно змінюється логіка бойових дій під впливом дронових технологій. Демонструється стрімке зростання кількості FPV-“камікадзе” та устаткування дронів потужнішими боєголовками, порівнюючи за цими показниками дані до і після 2022 року. Це дозволяє окреслити технологічний розвиток “бездротової війни” і сформулювати стратегічні висновки на основі кількісних і якісних характеристик БПЛА.

Таким чином, описовий характер статті проявляється в викладі технічних характеристик, класифікації та тактичного застосування БПЛА, а наукова обґрунтованість забезпечується використанням достовірних відкритих джерел. Стаття не лише документує сучасний стан “дронової війни”, але й робить спробу сформувати системне бачення її впливу на характер бойових дій, підкреслюючи технологічну динаміку як ключовий фактор сучасної війни.

Виклад основного матеріалу

Сучасна війна на території України висуває принципово нові вимоги до тактики, технологій і темпів адаптації. Однією з головних особливостей цієї фази бойових дій стало перетворення безпілотних літальних апаратів із допоміжного засобу на повноцінну бойову систему. Як для України, так і для росії дрони стали інструментом, який вирішує не лише

тактичні, а й стратегічні завдання – від точкових ударів і ведення розвідки до деморалізації цивільного населення й прориву енергетичної інфраструктури.

Нарощування масового виробництва дронів, яке демонструє рф, і постійне вдосконалення тактичних моделей в Україні призвели до якісного переходу у самій природі безпілотних систем. Йдеться не лише про габарити, бойове навантаження чи дальність польоту, а й про здатність дронів автономно орієнтуватися у просторі, розпізнавати цілі та приймати рішення без участі оператора. Це означає, що війна входить у фазу, де штучний інтелект стає визначальним компонентом у проєктуванні, управлінні, й застосуванні БПЛА. Відтак, у зоні бойових дій з'являються не просто дрони, а автоматизовані бойові платформи, здатні діяти в складному інформаційному середовищі.

У червні 2025 року рф почала активно використовувати на Сумському напрямку новітній ударний російський безпілотник V2U. Особливістю дрона є його здатність до автономного пошуку та вибору цілей за допомогою штучного інтелекту [3].

Центральною складовою обчислювальної системи став китайський мінікомп'ютер Leetop A203, у якому використовується високошвидкісна збірка на базі американського процесора NVIDIA Jetson Orin.

Дрон V2U має лише один GPS-модуль, що може свідчити про відмову від класичної супутникової навігації через роботу українських систем РЕБ. Імовірно, застосовується навігація за допомогою "комп'ютерного зору". Дрон орієнтується за зображеннями з камери, які співвідносить із заздалегідь завантаженими фото місцевості.

Для дистанційного керування у форматі FPV використовується LTE-зв'язок. У дроні встановлено модем-роутер Microdrive Tandem-4GS-oem11, що працює через SIM-картку одного з українських операторів. Хоча пристрій маркований як російський, його елементна база має китайське походження.

Серед іншого, дрон V2U зібраний із переважно іноземних компонентів: китайських двигуна, GPS-модуля, сервоприводів, SSD-накопичувача, далекоміра, контролерів обертів і акумуляторів. Також встановлено японський сенсор Sony, електромагнітне реле ірландської компанії Te Connectivity і згаданий модуль Jetson Orin. Китайські компоненти були помічені у рушійній частині, а саме у безщітковому двигуні виробництва Shanghai Dualsky Models, платі виробництва Leetoptech, електронному регуляторі обертів від T-MOTOR та інших компонентах.

Комбінація цих компонентів дозволила забезпечити безпілотник відносно непоганими характеристиками. V2U має розмах крила 1,2 м, корисне навантаження до 3,5 кг, електродвигун, крейсерську швидкість 60 км/год і тривалість польоту до 1 години; зв'язок здійснюється через двосторонній LTE-канал, енергоживлення забезпечує батарея ємністю 34 А·год, а система штучного інтелекту відповідає за розпізнавання об'єктів і здатна автоматично наводити боєприпас на ціль [3].

У червні, вперше з початку вторгнення, було зафіксовано удар по Харкову дроном-камікадзе "Черника". Дрони цієї серії виготовляються у двох варіантах, легка "Черника-1" та важча "Черника-2" [4].

Рф має ці дрони у своєму розпорядженні вже досить давно, й у березні 2024 року повідомлялося, що було виготовлено понад 7,5 тисяч одиниць "Черника-1". А вже у квітні 2024 року – про виготовлення понад 4 тисяч одиниць "Черника-2".

Дрон-камікадзе "Черника-1" являє собою безпілотник типу "літаюче крило", виготовлений з пінопласту. Він має максимальну дальність ураження до 80 км, крейсерська швидкість 75 км/год, максимальна висота польоту до 1,5 км.

Запуск відбувається з катапульти або з рук. Бойова частина масою 0,7 кг, ймовірно, уламково-фугасного типу, здебільшого цей дрон застосовується проти автотранспортної техніки та піхоти.

Більша версія “Черника-2” є небезпечнішою у порівнянні з першою моделлю. Вона має більшу бойову частину масою до 3,5 кг, яка вже призначена для ураження бліндажів та важкої техніки. Також він має збільшений радіус дії до 100 км.

Проте найголовніше: деякі російські джерела повідомляють про наявність функції донаведення на ціль, через що під час атаки він може бути не сприйнятливий до дії РЕБ. Також “Черника-2” обладнана функцією автопілоту до визначеного району цілі, завдяки чому оператору не потрібно постійно здійснювати керування, а тільки на кінцевій ділянці польоту.

Це у поєднанні з їхньою, ймовірно, низькою вартістю, робить їх масовими та дуже небезпечним. За своєю концепцією їх можна порівняти з іншим російським дроном “Молния”, який також у своїй конструкції використовує прості матеріали.

Слід зауважити, що насьогодні рф почала оснащати безпілотники Shahed 90-кілограмовими боєголовками, що говорить про поглиблення співпраці з Іраном. Нові боєголовки випускають двох типів: обидві вагою 90 кг, але одну з них збирають у росії, а іншу в – в Ірані. Про це пише The Telegraph [2].

Розроблена на росії модель, відома як КОФЗБЧ, поєднує в собі кумулятивну, осколкову, вибухову та запальну дію. Це означає, що вона може руйнувати будівлі, розкидати смертоносні уламки, викликати пожежі та створювати потужну ударну хвилю. Такі боєголовки застосовуються не для того, щоб знищити конкретну ціль, а щоб створити максимальний хаос у радіусі ураження. На відміну від російської, іранська модифікація випускається без запального компонента, але однаково завдає потужного удару.

Росії необхідно збільшити потужність “Шахедів”, щоб вони могли пробити антидроновий захист, встановлений на українських енергетичних об’єктах. З цією комбінованою боєголовкою головна мета – енергетична інфраструктура. Але українські енергетичні компанії будують бетонні укриття та встановлюють сталеві сітки. Тому росії потрібно щось, щоб пробити цю захисну інфраструктуру. Збільшивши боєголовку, рф домоглася посилення дії ураження, проте таким дронам потрібно більше палива, тому вони значно втратили в дальності польоту [2].

Особливо небезпечними є ударні “дрони-камікадзе” та FPV-апарати, які разом зі спостережними й навіть протидроновими безпілотниками створили навколо лінії фронту смертоносну “зону ураження”. При цьому агресор почав застосовувати імітаційні дрони-“мішені” одночасно з масованими ударами “Шахедами”, що ускладнює систему ППО. Держава-агресор також розробляє нові носії зброї – наприклад, крилату ракету S8000 “Бандероль”, яку можуть нести сучасні дрони “Оріон”. Усі ці тенденції суттєво підвищують стратегічну небезпеку для України, вимагаючи негайної адаптації тактики та технологій захисту.

У зв’язку з масовістю, максимальною дальністю ураження та тим, що ці дрони застосовуються на фронті вже понад рік, дивно, що перший удар по Харкову стався тільки зараз, адже північні райони Харкова знаходиться лише за 25 км від кордону [4].

Російські військовослужбовці розробили імпровізовану систему озброєння для дронів типу Mavic, яка дає змогу використовувати 12-каліберні дробові патрони для знищення ворожих безпілотників. Для підготовки боєприпасів у стандартному патроні 12 калібру вручну видаляють частину пороху, на його місце встановлюють електросірник, що слугує запальником. Потім патрон герметизується в посиленій скловолокном поліпропіленовій трубі, утворюючи одноразовий картридж.

Такі картриджі закріплюються під корпусом дрона за допомогою хомутів. Постріл здійснюється дистанційно, шляхом активації вбудованого світлодіода, який запускає займання електросірника. Під час пострілу картридж викидається віддачею, у такий спосіб унеможливлюючи її вплив на літальний апарат і зберігаючи його стійкість. Це рішення має свої недоліки – кожен картридж одноразовий, що збільшує трудовитрати на підготовку

бойового дрона. Управління таким БПЛА вимагає швидкої реакції та точного вибору моменту для пострілу, проте в іншому їхнє застосування не викликає складнощів [5].

Армія держави-агресора нарощує кількість БПЛА, які використовує під час масованих обстрілів України, і серед цих дронів є "обманки"-імітатори. У Повітряних силах ЗСУ визначають, де справжні "Шахеди", а де ні, спираючись на радіолокаційні особливості параметрів польоту, а також візуальні й акустичні характеристики [6].

Визначити їх можна під час відбиття обстрілу – спочатку залітають саме "обманки". Залітають у складі груп, можуть летіти доволі кучно один до одного, тому радіолокаційно може бути видно, що це один Shahed, а насправді там може бути чотири, або ж імітатор один, а можуть бути чотири-п'ять. Потім вони вже можуть розділятися й летіти у різних напрямках, із різних боків атакувати ту чи іншу ціль.

Звісно, є особливості параметрів польоту, якщо говоримо про радіолокаційне виявлення – маркер на моніторі. При наближенні до цілі об'єкта, до пунктів спостереження, де візуально й акустично теж іде ідентифікація тієї чи іншої цілі, і вже ухвалюється рішення, коли знаємо, що це Shahed чи дрон-імітатор, на визначення засобу щодо їхнього знищення.

Із травня-червня противник запускає все більше безпілотників-імітаторів разом із "Шахедами". Під час атаки в ніч на 9 липня ворог запустив по Україні 728 дронів різних типів, "Шахедів" із них було понад три сотні. Основним напрямком ворожого удару була Волинь [6].

Рф якийсь час використовує для ударів по Україні неідентифіковане озброєння, яке спершу було визначене, як ударний дрон типу "Бандероль", і все, що про нього було відомо до цього часу – це наявність реактивного двигуна, а також здатність розвивати швидкість до 500 км/год і той факт, що ворог використовує це озброєння передусім для ударів по півдню України [7].

У травні на порталі "Війна та санкції" від ГУР МОУ розкрили більше інформації про це озброєння. Як зрештою виявилося, під "Бандероллю" все ж таки ховається нова російська крилата ракета, яка отримала позначення S8000. Йдеться про дійсно новий зразок озброєння, який візуально схожий на американську протикорабельну ракету великої дальності типу AGM-158C LRASM (Long Range Anti-Ship Missile), але у даному випадку ідеться про спробу зробити дешеву крилату ракету із метою налагодити масове виробництва ще одного типу озброєння для терористичних обстрілів України. Вона використовує турбореактивний двигун SW800Pro-A95 від китайської компанії Swiwin – продукцію цієї компанії можна легко знайти на тому ж AliExpress. Тому рф, схоже, не склало проблем налагодити постачання двигунів.

В основі навігації крилата ракета типу "Бандероль" використовує вже відпрацьоване рішення, а саме завадозахищену CRP-антену "Комета-М8" АО "ВНИИР-ПРОГРЕСС". "Комети" використовуються у тих же ударних далекобійних дронах типу "Шахед" або в УМПК (Уніфікований модуль планування та корекції).

Російська крилата ракета "Бандероль" використовує низку різних компонентів з таких країн, як Австралія, Республіка Корея, США, Швейцарія та Японія. Так, наприклад, акумуляторна батарея – від японської компанії Murata; модуль обміну телеметричною інформацією – від австралійської RF Design; сервоприводи – від південнокорейської Dynamixel, радіочастотний посилювач потужності – від американської Maxim Integrated Products (Analog Devices) і так далі.

Тактико-технічні характеристики крилатої ракети "Бандероль": вона може розвивати максимальну швидкість до 650 км/год, крейсерську – до 560 км/год. Дальність польоту становить до 500 км. Габарити ракети: довжина – близько 5 м, розмах крил – 2,2 м, діаметр корпусу – 30 см. Бойова частина ракети – ОФБЧ-150, має масу у 114,3 кг, з них вага вибухової речовини – 49,5 кг. Носієм цієї крилатої ракети є безпілотний літальний

апарат типу “Орион”, у подальшому “Бандероль” планують інтегрувати до гелікоптерів Ми-28Н [7].

Українська дронова революція позбавила росію головних переваг – в артилерії, танках і чисельності військ – і саме це, як пише Reuters, змінило хід війни [8]. Дрони-камікадзе, дрони спостереження, дрони-бомбардувальники, дрони, що знищують інші дрони, – усі вони масово заполонили небо і створили так звану kill-zone, або “зону знищення”, приблизно по 10 км з обох боків лінії зіткнення, смертельно небезпечну для будь-якої техніки чи живої сили.

Це не дозволяє просуватись так, як у 2022 році: колони бронетехніки стали надто легкими мішенями. Тепер ворог атакує інакше: групами по 5-6 людей, пішки чи на мотоциклах або квадроциклах – і здебільшого лише для того, щоб виявити українські позиції, а тоді атакувати їх безпілотниками (у виробництві яких росіяни теж не відстають). Посилаючись на власні джерела серед українських командирів, виробників зброї та аналітиків, Reuters розповідає, що зараз Київ здатен протриматись без нової допомоги США місяці – на відміну від, наприклад, 2023 року, коли йшлося про дні чи тижні. Утім, польський військовий аналітик Конрад Музика застерігає від ілюзій: попри дронову перевагу Україна не має достатньо ресурсів для наступу, і, найімовірніше, Силам оборони доведеться вести виснажливу оборонну війну з обмеженими можливостями в артилерії та людях [8].

Безпілотні авіаційні комплекси розвідувального призначення.

Багатофункціональні безпілотні комплекси серії “ZALA”. Серед найбільш затребуваних (зокрема силовими відомствами) зразків БпАК серії ZALA є такі: ZALA 421-16EM; ZALA 421-16; ZALA 421-20. *Тактичний безпілотний авіаційний комплекс ZALA 421-16EM* є комплексом подвійного призначення і передбачає використання в інтересах збройних сил для ведення повітряної розвідки та спостереження за противником і місцевістю, здійснення цілевказання, корегування вогню вогневих засобів і виконання інших завдань в інтересах тактичної ланки (взводного та ротного рівня). Модель також застосовується в проведенні аерофотозйомки для геодезичних і картографічних робіт. Удосконалені цільові навантаження класу “16Е +”, що не мають аналогів у категорії безпілотних апаратів до 20 кг, здійснюють високоякісну фото-, відео- та тепловізійну зйомку, що дозволяє проводити пошук різних об’єктів і людей з точним визначенням їхніх географічних координат. Система кореляції дозволяє БпЛА стежити за статичними і рухомими об’єктами в автоматичному режимі. ZALA 421-16EM має у складі комплексу безпілотний літак з системою автоматичного керування (автопілот), з інерціальною навігаційною системою з корекцією (GPS/ГЛОНАСС), вбудованою цифровою системою телеметрії, вбудованим триосьовим магнітометром, модулем утримання й активного супроводу цілі, цифровим убудованим фотоапаратом, цифровим широкосмуговим відеопередавачем C-OFDM модуляції, радіомодемом з приймачем супутникових навігаційних сигналів, радіодалекоміром для роботи без прийому супутникових навігаційних сигналів, системою самодіагностики і пошуковим передавачем.

Тактичний безпілотний авіаційний комплекс ZALA 421-16 є комплексом подвійного призначення і вирішує завдання дистанційного моніторингу, спостереження в широкому діапазоні метеоумов підстильної поверхні (в тому числі складного рельєфу місцевості, водної поверхні), пошуку й виявлення об’єктів. Забезпечує отримання та передачу в режимі реального часу телевізійних і тепловізійних зображень місцевості, визначає координати об'єктів спостереження, виконує функції ретранслятора, здійснює збір, накопичення та обробку інформації.

Комплекс з БпЛА ZALA 421-16 є вигідним рішенням для масштабної аерофотозйомки. Можливе використання БпАК у ЗС для ведення повітряної розвідки та спостереження за противником і місцевістю, здійснення цілевказання, корегування вогню вогневих засобів і виконання інших завдань в інтересах тактичної ланки (батальйонного та

полкового/бригадного рівня). Дана модель безпілотного літака у своєму класі відрізняється високою тривалістю безперервного польоту – 4 години (при двотактному двигуні) і 8 годин (при чотиритактному двигуні) та великою швидкістю польоту – 130-200 км/год.

Оперативно-тактичний безпілотний авіаційний комплекс ZALA 421-20 є комплексом подвійного призначення і вирішує завдання довготривалого спостереження, охорони кордонів, моніторингу трубопроводів, морської розвідки, моніторингу пожеж та інших надзвичайних ситуацій на значній відстані.

Можливе використання БпАК у ЗС для ведення повітряної розвідки та спостереження за противником і місцевістю, здійснення цілевказання, корегування вогню вогневих засобів та виконання інших завдань в інтересах оперативно-тактичної ланки (полкового/бригадного та дивізійного рівня). БпЛА ZALA 421-20 має можливість перевозити до 50 кг цільового навантаження в різних комбінаціях, включаючи реєстратор аеронавігаційних даних, систему лазерного цілевказання, ІЧ-камеру високої роздільної здатності. При 400-кілометровому тактичному радіусі літак має повне сполучення з іншими системами ZALA, що дозволяє інтегрувати платформу з усіма операторами наземних станцій керування ZALA.

Також варто звернути увагу на *БПЛА типу "Форпост"*. Максимальна злітна маса – 454 кг; максимальна вага корисного навантаження – 100 кг; довжина – 5,85 м; розмах крил – 8,55 м; робоча швидкість 126-148 км/год; практична стеля – 5797 м; тривалість польоту 17,5 год; максимальна дальність дії системи – 250 км. У комплектацію БПЛА "Форпост" входить відео і інфрачервоне обладнання, яке дозволяє передавати інформацію в фото- і відеорежимах оператору комплексу. Для зльоту і посадки використовується аеродромна інфраструктура (злітна дистанція не менше 250 м). Апарат має систему з двох незалежних гіроскопів, також дублюються датчики GPS, розташовані зверху на крилах. Апарат укомплектований багатофункціональною системою відеоспостереження з платами відеозахоплення, потужною інфрачервоною камерою з охолоджувальною матрицею високої роздільної здатності, може визначати відстані, координати і здійснювати балістичні обчислення. Орієнтовна вартість головного пристрою відеореєстрації з інфрачервоною камерою становить 1 млн. дол США.

Війна стала потужним стимулом для поглибленої роботи з пошуку інновацій у сфері БПЛА. Один з актуальних напрямів – розробка дронів-перехоплювачів и створення дієвої сили для протистояння масованим атакам дронів з боку рф. В роботі задіяні як волонтерські організації, так і бізнес. Дрони-перехоплювачі – це відповідь України на нову загрозу з повітря. У сучасній війні FPV-дрони стали смертоносною зброєю, здатною завдати удару за лічені секунди. Класичні методи захисту вже не дають потрібного ефекту. Саме тому на передовій з'явилися нові "мисливці" – безпілотники, які виявляють, наздоганяють і знищують ворожі дрони ще до того, як ті завдають шкоди. Боротьба в форматі дрон проти дрона стає новою реальністю війни [9].

Основною метою розробки дронів-перехоплювачів було створення БПЛА, що можуть полювати на ворожі дрони (виявляти, переслідувати, атакувати). Завдання такого апарату – знищити ціль до того, як вона виконає свою місію – нанесе удар або отримає розвіддані, що особливо важливо, коли мова йде про російські дрони-розвідники (Zala, Orlan тощо). Проникаючи у тил противника та зависаючи над об'єктом, вони наводять ударні БПЛА на цілі. Цей "ланцюжок" вже добре відомий мешканцям територій воюючих сторін – "розвідник-загроза-вибух". Перервати цю послідовність допомагають перехоплювачі. Вони можуть працювати в різних напрямках та різними методами:

– можуть здійснювати фізичне перехоплення противника за допомогою сітки, тарана чи лопатей;

– впливають на здатність ворожого дрону орієнтуватися в просторі за допомогою глушіння сигналів управління чи GPS;

– здійснюють ударну атаку, врізаючись у дрон противника і самознищуючись разом з ним.

Фізичні дрони-перехоплювачі. Саме вони виконують завдання "вполювати та знищити". Для цього перехоплювач обладнаний спеціальним приладдям. Спіймати ворожий БПЛА можна використовуючи сітку або за допомогою прямого зіткнення (таран). Для пошкодження гвинтів супротивника можуть використовуватися частини самого перехоплювача – лопаті.

Дрони з глушилками. Завдання цих безпілотників – залишити супротивника без можливості "бачити" та орієнтуватися в просторі. Апарати обладнані глушилками, що глушать сигнали управління та навігацію. Ці дрони-перехоплювачі працюють, як компактні мобільні станції РЕБ. Вони знаходять в повітрі ворога, наближуються до нього та глушать сигнал. Ефективність дронів-глушилок менша за дієвість моделей з фізичним знищенням, але шанси на збереження апарату цілим та його подальше використання значно більші.

Дрони-камікадзе. Вони не мають за мету вполювати та схопити дрон ворога. Їхня задача проста – знайти та знищити. Дрон-перехоплювач помічає ціль, наздоганяє її та врізається в неї. Використовуються швидкі та маневрені FPV-дрони з простою конструкцією та недорогим ПЗ, адже їх служба недовга і ці БПЛА є "одноразовими".

Експерименти з перетворення FPV-дронів на перехоплювачі проводяться підрозділами аеророзвідки, в числі яких – славнозвісні "Птахи Мадяра". Бригада активно застосовує перехоплювачі для знищення ворожих FPV, в тому числі – оптоволоконних моделей. Для виявлення цілей застосовуються мобільні радари, що діють на відстані до кількох кілометрів. Після виявлення цілі здійснюється запуск дронів-перехоплювачів. Такий принцип "полювання" дозволяє ефективно знищувати навіть ті цілі, які нечутливі до РЕБ.

Українських ініціатив зі створення систем перехоплення ворожих дронів дійсно багато. Одне з рішень пропонує команда Ptashka Drones – вони розробили сіткомети, які можна встановити на різні типи дронів, в тому числі – популярні в Україні Mavic, Autel або FPV. Завдяки сіткам дрони можна застосовувати більше ніж один раз, що зберігає кошти та кількість перехоплювачів на фронті. В атаці на ворога дрон втрачає лише саму сітку, що коштує близько 1200 гривень – набагато менше за дрон [9].

Більш дорога за вартістю, але й більш ефективна розробка була здійснена німецьким стартапом Tytan Technology. Сили оборони України провели випробування німецького дрона-перехоплювача Tytan, створеного для боротьби з Shahed та іншими безпілотниками супротивника [10].

Tytan є безпілотним літальним апаратом, спеціально створеним для швидкого і точного перехоплення ворожих дронів. Основні технічні характеристики включають швидкість понад 250 км/год, дальність понад 15 кілометрів та злітну вагу 5 кг. Дрон здатний нести корисне навантаження до 1 кг, що дозволяє йому бути адаптованим як для знищення цілей, так і для розвідки. Корпус апарату виготовлено з використанням 3D-друку, що значно знижує вартість виробництва, а також спрощує ремонт та модифікації.

Однією з унікальних особливостей *Tytan* є можливість керування за допомогою портативної консолі Steam Deck. Ця консоль вже зарекомендувала себе як зручний та універсальний інструмент для керування різними видами роботизованої техніки, включаючи безпілотні системи. Впровадження такого підходу спрощує навчання операторів та дозволяє ефективно інтегрувати дрон у існуючі системи управління.

Розробка Tytan почалася близько року тому і була натхненна досвідом війни в Україні. Актуальність полягає в необхідності мати недорогі та ефективні засоби боротьби з масово застосовуваними дронами, такими як Shahed. Виробник планує подальший розвиток моделі. Серед нововведень – системи автоматичного наведення засновані на машинному зорі, які дозволять дрону самостійно ідентифікувати та захоплювати цілі. Це

підвищить точність та швидкість реагування в реальному часі, що особливо важливо в умовах високодинамічних бойових дій [10].

Команда українського miltech-проєкту ODIN розробила і випробувала ефективне рішення щодо знищення дронів типу "Шахед" за допомогою високошвидкісного дрона-перехоплювача ODIN Win_Hit власної розробки [11].

Характеристики дрона-перехоплювача ODIN Win_Hit:

– швидкість: крейсерська – 200-220 км/год, атакувальна – 280-300 км/год;

– тривалість місії польоту – 7-10 хв;

– діапазон висот для ефективного ураження – від 100 до 5000 м;

– способи запуску дрону: ручна платформа, наземний пусковий комплекс, повітряна платформа-носій.

Ударна група Night ODIN Crew вже успішно знищувала російські дрони "Шахед" та "Гербера" у небі над центральною частиною України. Окрім того, завершується виготовлення першої партії зі 100 дронів-перехоплювачів ODIN Win_Hit. Невдовзі їх передадуть до верифікованих підрозділів [10].

Українські інженери та військові провели бойове випробування нового *безпілотного літального апарату "Ватра"*, створеного для ефективного перехоплення боєприпасів "Шахед", що баражують. У ході тестів "Ватра" продемонструвала здатність підніматися на висоту до 7 кілометрів, що дозволяє безпілотнику знищувати цілі, що знаходяться на висоті 3-4 кілометри, пікіруючи на них зверху [11].

Безпілотник "Ватра" відноситься до класу безпілотників типу FPV (First-Person View), що означає, що оператор керує ним у реальному часі, ніби бачачи те, що відбувається від першої особи. Це дозволяє вести точний та динамічний контроль за дронами "Шахед" в умовах бойових операцій. "Ватра" має форму невеликого літака з округлим корпусом, що покращує його аеродинаміку та підвищує стійкість у польоті.

Ключові характеристики БПЛА "Ватра" підкреслюють її ефективність:

– загальна тривалість польоту (із поверненням) становить 90 хв;

– режим очікування на висоті 4 км дозволяє перебувати у повітрі від 30 до 40 хв;

– вертикальна швидкість набору висоти – 20 м/с, що дозволяє швидко підніматися на потрібні висоти;

– швидкість у режимі атаки досягає 230 км/год;

– швидкість у режимі пікірування на ціль становить до 280 км/год, що забезпечує високу ймовірність знищення цілі [11].

Українська компанія "Вінницькі бджоли" завершила міжвідомчі тестування свого нового *безпілотника VB140 Flamingo* [12]. Цей дрон розроблений для ефективної роботи проти повітряних цілей противника, що дозволяє значно покращити захист українського неба від ворожих дронів-розвідників, таким як Орлан.

Під час тестування VB140 Flamingo продемонстрував свою ефективність, показуючи надійну здатність виявляти, переслідувати та знешкоджувати ворожі дрони, що завдає значної шкоди розвідувальним можливостям супротивника.

Розробники наголошують, – "VB140 Flamingo – це важливий крок уперед у технологічному розвитку України. Його потенціал у боротьбі з ворожими розвідниками може суттєво знизити ефективність розвідки та коригування вогню, що конче необхідно для захисту мирного населення та наших воїнів".

Безпілотник VB140 Flamingo має такі характеристики:

– Перехоплення ворожих БПЛА – забезпечує надійний захист українських позицій та підрозділів завдяки сучасним технологіям та високоточним сенсорам.

– Висота польоту – здатний працювати на висоті до 4,5 км, що збільшує його ефективність у виявленні загроз.

– Дальність польоту – дрон може літати на відстань до 50 км, що дозволяє йому оперативно реагувати на загрози, що виникають.

– Адаптивність – додаткова гнучкість в налаштуваннях дозволяє дрону працювати як вдень, так і вночі.

Високий рівень автономності робить Flamingo незамінним інструментом для моніторингу та перехоплення повітряних цілей [12].

Skyfall, один із найбільших виробників дронів в Україні, адаптує свої FPV для боротьби з повітряними цілями. Їхній дрон Shrike, вартістю від $300 до $500, може цілитися в розвідувальні та ударні дрони, хоча й не дістає до висоти польоту Shahed [13].

“Ми зосереджені на перехопленні дронів-камікадзе та дронів-бомбардувальників”, – пояснив Карл Ларсон, керівник Defense Tech for Ukraine. Він підкреслює: Україні потрібні “недорогі та масштабовані рішення”, а не “модні та дорогі системи” західного виробництва. На сьогодні, дрони-перехоплювачі ще не можуть повністю замінити ППО, однак це крок до зниження залежності від дорогих систем типу Patriot. Альтернатива – низькотехнологічні засоби, як-от кулемети на пікапах або обмежене використання F-16” [13].

Українські розробники представили в 2024 р. ще одну нову модель баражуючого боєприпасу. Дрон знаходиться на етапі тестування у зоні бойових дій. Завдяки модулям шифрованого зв’язку він може працювати за умов придушення системами РЕБ. Новий дрон здатний завдавати ударів по цілям супротивника на глибині понад 100 км [14].

Новий безпілотник має високонадійний модуль шифрованого зв’язку AES256. Це дозволяє працювати в умовах придушення системами РЕБ, а “машинний зір” забезпечує захоплення об’єктів та автоматичне донаведення на ціль. Безпілотник має електричний двигун, його запускають із катапульти. Завдяки Х-подібному фюзеляжу він маневрений і здатний вражати статичні та рухливі цілі на різних траєкторіях, у тому числі під прямим кутом.

Максимальна швидкість дрону – 180 км/год, він може вражати об’єкти, чия швидкість до 130 км/год, це БПЛА типу Орлан-10, Zala, Ланцет, а також вертольоти, що пролітають на зустрічних курсах.

Бойова частина представлена у кількох версіях – осколкова, термобарична, бронебійна з ударним ядром, яка може пробити до 40 мм броні та завдати ураження ворожій техніці [14].

Міністерство оборони кодифікувало та допустило до експлуатації у Збройних Силах України безпілотний авіаційний комплекс українського виробництва Chief-1 [15].

Цей дрон призначений для ураження літальних апаратів або живої сили супротивника з модуля ураження патронами зі шротом. Chief-1 має легку та міцну раму, потужні двигуни, високу маневреність, вдалу конструкцію для повітряного бою.

Безпілотники обладнані системами автоматичного розпізнавання та досягнення оптимальної дистанції для ураження цілі. Можуть здійснювати постріли в ручному або автоматичному режимі. Chief-1 знищують ворожі FPV, бомбери, окремі зразки корегувальників, розвідників [15].

І українські, і російські війська сьогодні шукають способи ліквідації дронів на оптоволокні, тож в обох сторін з’являються нові гвинтівкові кулі. Як пояснює Business Insider [16], за рахунок спеціально розробленої бойової частини вони можуть щільно та швидко “розкидати” осколки, що дозволяє ліквідовувати БпЛА на більшій відстані, ніж це може зробити дробовик. Такі кулі мають калібр 5,56 мм, а заряджають їх у гвинтівки по типу CZ Bren 2.

У ВІ пояснили перевагу таких куль: “Технологія дасть змогу солдатам вистрілити кулею, яка пролетить деяку відстань, перш ніж розсіяти дріб, що вражає FPV-дрон або квадрокоптер... А піхоті – почати стрільбу по ударних дронах з більш безпечної відстані, ніж спроба усунути загрозу за допомогою дробовика, що зараз є нормою в українських підрозділах”. Тобто ця розробка дозволить захисникам неба просто брати з собою додаткові патрони, а не окрему зброю.

Втім, ці кулі вже є у російської армії. Ще торік у листопаді одна з бригад окупантів показала, як солдати стріляють з автомата Калашникова з наконечником з термозбіжною трубкою кулями калібру 5,45 мм. У таких трубках є чотири дробові гранули, призначені для розсіювання та вражання українських БпЛА. При цьому під час ручного зарядження патронів окупанти повинні чергувати нові кулі зі стандартними або трекерними патронами [16].

Раніше у ЗСУ розповідали, що російські дрони на оптоволокні здатні проникати далеко в тил українських позицій на відстань 20 км. Тим часом Сили оборони застосовують проти таких коптерів звичайні комерційні дрони типу Mavic – вони своїми пропелерами перерубують кабель і залишають ворожі апарати без управління – та інші експериментальні рішення [17].

Бійці підрозділу "Гострі картузи" показали, як вони збивають дрони на оптоволокні. У дописі на своїй сторінці у соцмережі вони розповіли, що ці безпілотники сьогодні є дуже небезпечними, оскільки проти них не діють системи РЕБ і наразі немає перевірених і гарантованих методів боротьби з ними. "Якщо ворог виявляє позицію пілотів БпЛА, то найчастіше відправляє туди FPV на оптиці. Така смертоносна пташка може літати по посадці і залетіти у бліндаж із пілотами". У таких дронів є і слабкі місця. Наприклад, через котушки вони більші за розміром і не дуже маневрені. Через це їх простіше збивати зі стрілецької зброї. "Головне їх не боятися, а збити їх простіше, ніж здається", – додали захисники [17].

Дрони-перехоплювачі – це не універсальний засіб проти всіх повітряних цілей. А точковий інструмент, ефективний проти повітряних цілей, що рухаються на малих швидкостях (до 200-250 км/год) та невисоких висотах (від 2 до 4 км). До цієї категорії належать розвідувальні дрони та ударні безпілотники типу "Шахед" [18].

Експерти категорично відкидають можливість ефективного застосування дронів-перехоплювачів проти крилатих чи балістичних ракет, а також проти КАБів (коригованих авіаційних бомб), які країна-агресор масовано використовує. Дрони-перехоплювачі – це системи мікрозахисту повітряного простору з малою дальністю дії, переважно 5-10 км. Рф може перейти на використання більш швидких та дорогих дронів, що зробить завдання їхнього перехоплення значно складнішим для України.

Раніше повідомлялося, дрон на оптоволокні потребує пілота, який ним керує, а зі штучним інтелектом може використовуватися автоматично, тож те, що Україна намагається наздогнати рф по дронах на оптоволокні, – стратегічно неправильне рішення [18].

Співвідношення витрат і результатів використання дронів-перехоплювачів проти ударних "Шахедів, на думку експертів, є неефективним і надто дорогим способом захисту [19].

Щоб знищити один "Шахед" удень, потрібно до п'яти перехоплювачів, а вночі – до десяти. Водночас вартість одного денного перехоплювача сягає $2-3 тисяч, нічного – до $4 тисяч. Таким чином, знищення одного ворожого дрона може стати у $10 тисяч удень і до $40 тисяч – уночі.

Крім того, дрони-перехоплювачі обмежені погодними умовами та не здатні довго перебувати в повітрі на відміну від "Шахедів". Ще один виклик – людський ресурс: для відбиття атаки з 400 дронів-камікадзе, як нещодавно в Києві, потрібно щонайменше 400 навчених операторів. Загальна вартість таких перехоплювачів сягнула б $16 млн. Водночас, за оцінками експерта, рф витрачає близько $32 млн на таку атаку (по $80 тисяч на кожен "Шахед").

Також експерт підкреслює, що для ефективного використання перехоплювачів потрібна інтеграція в систему ППО, надання кожному оператору якісного радара та точне скерування на маршрут ворожого дрона. З огляду на нові ризики в разі збільшення

кількості “Шахедів” до 1000 за ніч необхідно буде залучати вже понад тисячу операторів – і витрати зростатимуть у геометричній прогресії [19].

Голова ситуаційного центру по Україні в Міноборони Німеччини генерал-майор бундесверу Крістіан Фройдінг у подкасті Nachgefragt заявив, що рф має намір запускати по Україні до 2000 безпілотників одночасно [20].

За інформацією Фройдінга, рф суттєво розширює виробничі потужності для масового застосування безпілотників у війні проти України. За його словами, Москва планує одночасно запускати 2 тисячі дронів, що створить серйозний виклик для української системи протиповітряної оборони.

Генерал наголосив на необхідності розробки “розумних заходів протидії”, адже застосування традиційних засобів, зокрема ракет для системи ППО Patriot, є нелогічним проти “Шахедів”, вартість яких становить 30-50 тисяч євро, тоді як одна ракета Patriot коштує понад 5 мільйонів. За його оцінками, Україні потрібні недорогі засоби боротьби з безпілотниками вартістю від 2 до 4 тисяч євро, що дозволить ефективно реагувати на масовані атаки.

Ще одним методом протидії Фройдінг назвав удари по глибокому тилу рф – по військових літаках, аеродромах і оборонних заводах.

Також генерал-майор звернув увагу на те, що Китай припинив постачання комплектуючих до безпілотників в Україну і нині повністю зосередив свій експорт до росії. “Наразі ситуація така, що Китай, фактично, експортує виключно до росії, тоді як Україну виключено з цього ринку”, – зазначив Фройдінг [20].

Аналізуючи сучасні розробки та те, з якими темпами розвивається галузь, можна розраховувати на справжню повітряну революцію у сфері створення дронів перехоплювачів. З’являться автономні дрони-перехоплювачі на базі Штучного інтелекту. Це один з основних трендів останніх років – розробка безпілотників, що здатні самостійно знаходити та переслідувати БПЛА противника без участі пілота. Прототипи таких апаратів вже існують та проходять тестування (Anduril Interceptor, Fortem DroneHunter F700).

Вже розробляються та тестуються системи підтримки прийняття рішень на базі ШІ. Це дасть можливість заздалегідь попереджати про наближення FPV-дрона та оперативно підбирати методи протидії.

Інженери з Китаю, США, Ізраїлю та Туреччини спрямовують зусилля на розробку лазерних систем ближнього радіуса дії, які будуть спроможні випалювати ворожі дрони при наближенні. Аналогічні випробування вже були проведені в Великій Британії, де лазерна система DragonFire довела свою здатність знищувати дрони з великою точністю [21].

Пріоритетом №1 залишається пошук протидії дронам на оптоволокні. Більшість розробок спрямована на пошуки рішень з фізичного перехоплення. Над цим питанням працюють багато розробників. ШІ допоміг вивести дрони на новий рівень. Дрони з машинним зором можуть самостійно виявляти цілі, перехоплювати ворога, знищувати його. Вже зараз ведуться роботи з розробки максимально автономних “мисливців” на БПЛА, які зможуть працювати майже без втручання людини. Вже сьогодні створюються компактні дрони-перехоплювачі, здатні навчатися в процесі виконання бойових завдань.

Рф дедалі активніше використовує передові технології для посилення своїх наступальних можливостей, зокрема шляхом розгортання *нових типів БПЛА*. Якщо раніше основним інструментом російських атак були дрони-камікадзе Shahed-136, то з 2025 року фіксується перехід до використання реактивних *Shahed-238 (“Герань-3”),* які суттєво ускладнюють завдання української ППО.

У липні 2025 року російські збройні сили посилили повітряні атаки на Україну, зокрема на Київ, застосувавши новий тип ударних безпілотників – реактивні Shahed-238, відомі в рф як “Герань-3”. Ці дрони, розроблені на основі іранської моделі та адаптовані для локального виробництва, відзначаються високою швидкістю, дальністю польоту та

здатністю ухилятися від традиційних засобів ППО. Їхнє використання свідчить про намір росії ускладнити протидію української сторони, перевантажуючи системи ППО та підвищуючи ефективність атак на цивільну й критичну інфраструктуру. Водночас поява таких дронів ставить перед Україною завдання швидкої адаптації до нових загроз, що вимагає як технологічних інновацій, так і міжнародної підтримки.

Розглянемо технічні особливості *Shahed-238*, їхню роль у російській стратегії та виклики, які вони створюють для української ППО.

1. Реактивні Shahed-238, уперше зафіксовані в Україні 30-31 липня 2025 року, значно переважають попередні моделі Shahed-136 за ключовими параметрами. Оснащені турбореактивним двигуном Tolou-10/13 (іранська копія чеського PBS TJ100), вони розвивають швидкість до 550–600 км/год (до 700 км/год при пікіруванні), що втричі перевищує швидкість Shahed-136 (180–200 км/год). Дальність польоту сягає 2500 км, а висота до 9 км робить їх недосяжними для більшості мобільних засобів ППО. На відміну від поршневого двигуна Shahed-136, реактивний двигун забезпечує маневровість і ускладнює ідентифікацію, оскільки на радарах дрон виглядає як крилата ракета.

2. Рф використовує Shahed-238 вибірково для ураження стратегічних цілей, зокрема військових об'єктів та енергетичної інфраструктури. Їх інтегрують у комбіновані атаки з ракетами та масованими ударами Shahed-136, що спрямовані на перевантаження української ППО. Наприклад, під час атак на Київ 31 липня 2025 року дрони заходили з різних напрямків, а через годину після їхнього нальоту рф застосувала ракети. Така тактика ускладнює прогнозування траєкторій і розподіл ресурсів ППО. За оцінками експертів, Shahed-238 є частиною російської стратегії технологічної ескалації, спрямованої на підтримання ініціативи в умовах затяжного конфлікту.

Висока швидкість Shahed-238 скорочує час реакції ППО: від кордону до Києва дрон долітає за ~40 хвилин проти 2 годин для Shahed-136. Їхня недосяжність для дронів-перехоплювачів, вертольотів, легкомоторної авіації та мобільних вогневих груп зумовлена висотою польоту та маневровістю. Для ураження потрібні реактивна авіація, сучасні ЗРК або зенітна артилерія з програмованими снарядами. Однак такі системи, як IRIS-T (ракета вартістю $430,000), є економічно невигідними для перехоплення дронів вартістю ~$150,000. Крім того, програмовані снаряди калібру 35 мм коштують понад 1000 євро за одиницю, а їхнє виробництво є тривалим і обмеженим.

Українські дрони-перехоплювачі (наприклад, FPV-дрони) не можуть протистояти Shahed-238 через їхню швидкість і висоту. Для протидії потрібні нові технології, такі як реактивні перехоплювачі ("Пекло", "Паляниця") або сучасні ЗРК. Однак висока вартість таких систем і їхня обмежена доступність створюють економічні та логістичні виклики. Наприклад, дефіцит програмованих снарядів і залежність від поставок від країн-партнерів обмежують здатність України оперативно адаптуватися до нової загрози.

Висновки

Підсумки проведеного дослідження показують, що безпілотні системи радикально змінили ситуацію на фронті. Українська "дронова революція" ефективно зрівняла шанси у конфлікті: вона позбавила Росію переваги в кількості танків та артилерії і сформувала над лінією фронту неймовірно небезпечну "зону ураження". При цьому стрімке розростання FPV-"камікадзе" і масове застосування модернізованих боєголовок (наприклад 90-кілограмових бойових частин "Шахедів" і "Бандеролі") свідчать про загострення протиборства технологій. З технічного боку спостерігається зростання потужностей у обох сторін, а стратегічно – виникнення потреби утримувати ініціативу у технологічному змаганні. У відповідь на нові загрози Україна розпочала розробку автоматичних дронів-перехоплювачів з використанням штучного інтелекту, що є одним з ключових трендів.

Таким чином, аналіз свідчить: хоча дрони вирівнюють сили на полі бою, це також означає постійне нарощування інновацій.

Аналіз технічних характеристик бойових дронів, що активно застосовуються у російсько-українській війні, дозволяє зробити кілька суттєвих висновків:

1. Держава-агрсеор зосередилась на масовості та ударній потужності. Зразки на кшталт Shahed із боєгоовками вагою 90 кг, дрони "Черника-2" з донаведенням і ракети "Бандероль" із дальністю до 500 км орієнтовані на створення ефекту перевантаження протиповітряної оборони, руйнування критичної інфаструктури та терору цивільного населення. Це – технологія навмисної руйнації.

2. Україна зосереджена на маневреності, гнучкості та інноваціях. Дрони типу "ODIN WIN-HIT", "Ватра", VB140 Flamingo демонструють перевагу швидкості, висотності, розпізнавання цілей, перехоплення БПЛА противника та використанні інтелектуальних систем. Ключовим є поєднання волонтерського сектору, miltech-проєктів і швидкої інтеграції іноземних технологій. Окрім того, використання дешевих FPV-дронів, створення власних перехоплювачів і адаптація ігрових консолей (Steam Deck) до керування БПЛА – приклади того, як нестандарнті рішення формують бойову ефективність.

3. Штучний інтелект стає зоною майбутньої переваги. Дрони з компютерним зором, самонаведенням, використанням Jetson Orin, відмовою від GPS на користь візуального орієнтування (як у V2U) – свідчення того, що обидві сторони вже працюють над БПЛА, здатними діяти у складних умовах електронної війни.

4. Поява реактивних Shahed-238 ("Герань-3") у російському арсеналі знаменує новий етап технологічної ескалації в російсько-українській війні, спрямований на підвищення ефективності атак і перевантаження української ППО. Їхні характеристики – висока швидкість, дальність і схожість із крилатими ракетами – ускладнюють перехоплення традиційними засобами, вимагаючи від України швидкої адаптації. Асиметрична стратегія України, яка раніше дозволяла ефективно протидіяти Shahed-136 за допомогою дешевих дронів-перехоплювачів і мобільних груп, потребує перегляду. Розвиток реактивних перехоплювачів і модернізація ППО є визначальним у системі стримування, але обмежені ресурси та висока вартість сучасних систем створюють значні виклики.

Для ефективної протидії Україні необхідно не лише розвивати власні технології, а й поглиблювати співпрацю з міжнародними партнерами для отримання передових ЗРК, програмованих снарядів і фінансової підтримки. Водночас поява Shahed-238 підкреслює потребу в посиленні санкційного тиску на Іран і Росію для обмеження трансферу технологій, що порушують міжнародні норми. У довгостроковій перспективі успіх України в цій асиметричній війні залежатиме від поєднання інновацій у сфері безпілотних систем, економічно ефективних рішень для ППО та міжнародної підтримки, що дозволить нейтралізувати зростаючу загрозу реактивних дронів і зберегти стійкість у протистоянні технологічній агресії противника.

Список літератури

1. Putin Ramps Up Drone-Making to Unleash Attacks on Ukrainian Cities. URL: https://www.bloomberg.com/news/articles/2025-06-10/putin-ramps-up-drone-making-to-unleash-attacks-on-ukrainian-cities.
2. Russia's Shahed drone arsenal has just become more deadly. URL: https://www.telegraph.co.uk/world-news/2025/05/27/russia-deadly-drone-arsenal-more-powerful-iran-ukraine/.
3. ГУР розповіло про характеристики російського дрона V2U. URL: https://irtafax.com/hur-rozpovilo-pro-kharakterystyky-rosijskoho-drona-v2u.

4. “Черника” на 100 км з донаведенням: що це за дрон, що вперше вдарив по Харкову та чому він небезпечний. URL: https://defence-ua.com/news/chernika_na_100_km_z_do_navedennjam_scho_tse_za_dron _scho_vpershe_vdariv_po_harkovu_ta_chomu_vin_nebezpechnij-19349.html.
5. 12 калібр проти дронів: у рф створили дробовик для БпЛА типу Mavic (відео). URL: https://focus.ua/uk/voennye-novosti/703086-12-kalibr-proti-droniv-u-rf-stvorili-drobovik-dlya-bpla-tipu-mavic-video.
6. “Є особливості параметрів польоту”: у Повітряних силах пояснили, як відрізняють “Шахеди” від дронів-імітаторів. URL: https://war.obozrevatel.com/ukr/e-osoblivosti-parametriv-polotu-u-povitryanih-silah-poyasnili-yak-vidriznyayut-shahedi-vid-droniv-imitatoriv.htm.
7. Розкрито деталі про нову ракету рашистів, яку вони можуть пускати з “Орионов”. URL: https://defence-ua.com/weapon_and_tech/rozkrito_detali_pro_novu_raketu_rashistiv_jaku_voni_mozhut_puskati_z_orionov-18800.html.
8. Enter the kill zone: Ukraine’s drone-infested front slows Russian advance. URL: https://www.reuters.com/business/aerospace-defense/enter-kill-zone-ukraines-drone-infested-front-slows-russian-advance-2025-07-17/.
9. Мисливці за дронами: як працюють дрони-перехоплювачі на фронті. URL: https://vgi.com.ua/myslyvczi-za-dronamy-yak-praczyuyut-drony-perehoplyuvachi-na-fronti/.
10. З’явилися фото українських дронів-перехоплювачів ODIN Win_Hit. https://tsn.ua/ukrayina/ziavylysia-foto-ukrayinskykh-droniv-perekhopliuvachiv-odin-win-hit-2870894.html.
11. Українські розробники тестують інноваційний дрон-перехоплювач “Ватра” для боротьби з ворожими “Шахедами”. URL: https://building-tech.org /ukraynskye-razrabotchyky-testyruyut-ynnovatsyonniy-dron-perekhvatchyk-% vatra -s-vrazheskymy-shakhedamy.
12. Українська компанія “Вінницькі пчелі” представила безпілотник-перехоплювач VB140 Flamingo для боротьби з розвідувальними дронами. URL: https://building-ukraynskaya-kompanyya- vinnytski-bdzholy -predstavyla-bespylotnyk-perekhvatchyk-vb140-flamingo-dlya-borbi-s-razvedivatelnimy-dronamy-rf.
13. Україна запускає “дрони-мисливці” під час масованих атак рф, – Bloomberg. URL: https://www.unian.ua/weapons/ukrajina-zapuskaye-droni-mislivci-shcho-pro-nih-vidomo-13026738.html.
14. Новий дрон-камікадзе, української розробки, здатний збивати ворожі “Орлан” та “Ланцет” у повітрі. URL: https://building-tech.org/noviy-dron-kamykadze-ukraynskoy-razrabotky-sposoben-sbyvat-vrazheskye-%C2%ABorlan%C2%BB-y-%C2%ABlantset%C2%BB-v-vozdukhe.
15. Chief-1 – мисливців за ворожими дронами стає більше. URL: https://armyinform.com.ua/2025/06/04/chief-1-myslyvcziv-za-vorozhymy-dronamy-staye-bilshe/.
16. A new type of rifle bullet in Ukraine could give infantry a better way to survive unjammable drone attacks. URL: https://www.businessinsider.com/rifle-bullet-fpv-anti-drones-ukraine-war-unjammable-nato-2025-7.
17. Головне – не боятися: “Гострі картузи” збивають дрони на оптоволокні зі стрілецької зброї. URL: https://zn.ua/ukr/war/holovne-ne-bojatisja-hostri-kartuz-zbivajut-droni-na-optovolokni-zi-striletskoji-zbroji.
18. Дрони-перехоплювачі не врятують від ракет: авіаексперт пояснив чому https://tsn.ua/ato/drony-perekhopliuvachi-ne-vriatuiut-vid-raket-aviaekspert-poiasnyv-chomu-2863070.html.
19. Математика війни: чому перехоплювати “Шахеди” – не найкраще рішення. URL: https://tsn.ua/ato/matematyka-viyny-chomu-perekhopliuvaty-shakhedy-ne-naykrashche-rishennia-2869841.html.
20. Ukraine unter druck. Drohnenterror und grossoffensive. Nachgefragt: Neue Drohnentaktik in der Ukraine | Bundeswehr. URL: https://www.youtube.com/watch?v=KtgNJqp-6BA.
21. Лазерна зброя Dragonfire, яку Британія з часом може дати Україні. URL: https://www.youtube.com/watch?v=PjBe8t0dp0w.

УДК 327.56:355.021,35.071:327.56,327.56:930 DOI: 10.63978/3083-6476.2025.2.2.09

Гурковський Володимир Ігорович
доктор наук з державного управління, професор, начальник відділу
Центральний науково-дослідний інститут Збройних Сил України
Київ, Україна
e-mail: volodymyr.gurkovskyi@gmail.com
ORCID: 0000-0003-2021-5204

Романенко Євген Олександрович
доктор наук з державного управління, професор, начальник управління
Центральний науково-дослідний інститут Збройних Сил України
Київ, Україна
e-mail: poboss1978@gmail.com
ORCID: 0000-0003-2285-0543

Череп Василь Леонідович
кандидат військових наук, старший дослідник, начальник управління
Центральний науково-дослідний інститут Збройних Сил України
Київ, Україна
e-mail: vasya.cherep1976@gmail.com
ORCID: 0000-0003-3305-4518

Ільницький Сергій Валерійович
науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
Київ, Україна
e-mail: anastx85@icloud.com
ORCID: 0009-0009-3000-9034

ІСТОРИЧНІ УРОКИ ЄВРОПЕЙСЬКОЇ БЕЗПЕКИ: РОЛЬ УКРАЇНИ У ФОРМУВАННІ ЗАХИСНОГО ПОЯСУ ВІД СХОДУ

Анотація. *У статті досліджується формування поясу європейської безпеки як механізму протидії агресії Російської Федерації, із акцентом на історичний досвід України як щита Європи. Розглядається роль України як стратегічного чинника забезпечення воєнного аспекту безпеки Європи в умовах війни та післявоєнного миру. Основною метою дослідження є поєднання історичного, міжнародно-політичного та управлінського аналізу для виявлення уроків минулого – від часів Русі Київської та Середньовіччя до сучасних геополітичних викликів – і визначення шляхів інтеграції України у сучасну систему європейської безпеки.*

Аналізується історичний досвід формування європейської єдності від часів Римської імперії до наших днів, з метою визначення релевантних уроків для сучасної Європи. На основі історичної фактології в дослідженні систематизовано події, які засвідчують системну неспроможність міжнародних безпекових інституцій ефективно реагувати на прояви агресії та запобігати ескалації конфліктів.У роботі проаналізовано роль держав, що протягом століть виконували функцію щита Європи проти східних загроз, а також наведено приклади успішного протистояння менших коаліцій більш потужним агресорам. Особлива увага приділяється сучасним безпековим ініціативам, зокрема "Трьох морів" (3SI), та виявленню "вікна можливостей" для України у зміцненні континентального поясу безпеки. У статті також розглядається проблема збереження якості безпекової організації Європи з урахуванням маневрів Вашингтону та необхідності адаптації до нових реалій. Проаналізовано європейські ініціативи, спрямовані на модернізацію системи безпеки Європи, та потенційна роль України в ній. Розглянуто основні заходи, що мають бути здійснені урядом України та європейськими партнерами для побудови системи надійного поясу безпеки проти агресії зі сходу.

Особливу увагу в статті приділено аналізу вікна можливостей, що відкривається для України та європейських партнерів в сучасній непростій геополітичній ситуації. Автори вказують на позитивні зрушення, що відбуваються в побудові поясу європейської безпеки, особливо в зв'язку з розвитком ініціативи 3SI та можливістю для України підсилити її. Водночас, підкреслюється важливість подальших кроків щодо реалізації цього проєкту в умовах військової агресії, що потребує швидкого впровадження адаптивних практик європейського співробітництва в оборонній сфері.

Результати дослідження можуть слугувати методологічною основою для розробки національних та регіональних ініціатив України у сфері національної безпеки, державного управління та оборони, спрямованих на формування ефективної післявоєнної безпекової архітектури Європи.

***Ключові слова**: історичний досвід, щит Європи, пояс безпеки, європейський пояс безпеки, вікно можливостей України, міжнародна безпека, європейська безпека, державне управління.*

Volodymyr Gurkovsky
Doctor of Science in Public Administration,
Professor, Head of Department
Central Research Institute of the Armed
Forces of Ukraine
Kyiv, Ukraine
e-mail: volodymyr.gurkovskyi@gmail.com
ORCID: 0000-0003-2021-5204

Yevhen Romanenko
Doctor of Science in Public Administration
Professor
Leading Researcher
Central Research Institute of the Armed
Forces of Ukraine
Kyiv, Ukraine
e-mail: poboss1978@gmail.com
ORCID: 0000-0003-2285-0543

Vasyl Cherep
Candidate of Military Sciences,
Senior Researcher
Head of Central
Central Research Institute of the Armed
Forces of Ukraine
Kyiv, Ukraine
e-mail: vasya.cherep1976@gmail.com
ORCID: 0000-0003-3305-4518

Serhii Ilnytskyi
Researcher
Central Research Institute of the Armed Forces of Ukraine
Kyiv, Ukraine
e-mail: anastx85@icloud.com
ORCID: 0009-0009-3000-9034

HISTORICAL LESSONS FOR EUROPEAN SECURITY: UKRAINE'S PIVOTAL ROLE IN SHAPING A DEFENSIVE BARRIER AGAINST EASTERN THREATS

Abstract. *This study examines the establishment of a European security belt as a strategic countermeasure to Russian aggression, emphasizing Ukraine's historical role as a bulwark of European defense. It explores Ukraine's significance as a critical factor in ensuring the military dimension of European security during wartime and in the post-war period. The research integrates historical, international-political, and governance perspectives to distill lessons from the past—spanning from Kyivan Rus and the Middle Ages to present-day geopolitical challenges—and to propose pathways for Ukraine's integration into the contemporary European security framework.*

The analysis traces the evolution of European unity from the Roman Empire to the present, identifying lessons applicable to modern Europe. Drawing on historical evidence, the study systematizes events that reveal the consistent shortcomings of international security institutions in effectively addressing aggression and preventing conflict escalation. It highlights the roles of states that have historically served as Europe's defensive shield against eastern threats, citing instances where smaller coalitions successfully resisted more powerful adversaries. Particular focus is placed on modern security initiatives, such as the Three Seas Initiative (3SI), and the identification of strategic opportunities for Ukraine to bolster the continental security framework.

The article also addresses the challenge of maintaining a robust European security architecture amidst shifting U.S. policies and the need to adapt to emerging realities. It evaluates European initiatives aimed at modernizing the continent's security system and delineates Ukraine's potential contributions. Key measures are outlined for the Ukrainian government and its European partners to establish a resilient security belt to counter eastern aggression.

Special attention is given to the strategic window of opportunity for Ukraine and its European allies in the current complex geopolitical environment. The authors highlight positive developments in the construction of the European security belt, particularly through the advancement of the 3SI, and underscore Ukraine's potential to strengthen this initiative. However, the study emphasizes the urgency of implementing adaptive defense cooperation practices in response to ongoing military aggression.

The findings provide a methodological foundation for developing national and regional initiatives in Ukraine's national security, public administration, and defense sectors, aimed at shaping an effective post-war European security architecture.

Keywords: *historical lessons, Europe's defensive shield, security belt, European security framework, Ukraine's strategic opportunity, international security, European security, public governance.*

Вступ

Постановка проблеми. На перший погляд може здаватися, що саме російсько-українська війна вперше продемонструвала глобальну неспроможність міжнародних організацій, таких як ООН та НАТО, ефективно стримувати агресорів і забезпечувати виконання власних рішень. Однак ця проблема має довшу історію. Її витоки сягають XX століття: від нездатності Ліги Націй гарантувати стабільний мир після Першої світової війни до невдалих спроб новоствореної ООН зупинити безперервну низку збройних конфліктів після завершення Другої світової війни. Корейська та В'єтнамська війни, арабо-ізраїльські протистояння, численні конфлікти в Африці, Ірано-іракська, індо-пакистанські та індо-китайська війни, Фолклендський конфлікт, війни в Афганістані, агресія росії в Грузії та Чечні – ці події свідчать про системну кризу міжнародних механізмів безпеки.

Війна в Україні стала кульмінацією цієї тенденції. Вона є своєрідним індикатором, що сигналізує світові про загрозу занурення в хаос і моральну деградацію міжнародної політики. Вирішення питання встановлення миру після завершення війни між Україною та росією стане випробуванням для людства: від його результатів залежить перспектива подальшого розвитку глобальної цивілізації та можливість співіснування держав із різними масштабами ресурсів і воєнного потенціалу.

Останні події демонструють ознаки трансформації світових центрів сили. Цю перебудову варто аналізувати у парадигмі постмодерну та навіть постпостмодерну, де зростаючий вплив механізмів "постправди" визначає суспільні настрої та політичні рішення. В політичному просторі намітились ознаки нової системи, де абсолютно відсутня відповідальність за заяви та обіцянки. Якщо Джорж Орвел у своїй епохальній роботі – антиутопії "1984" ще періоду модерну розглядав технічний прогрес як підставу для створення тиранії з реальним контролем за всіма аспектами життя людини фізичної, то порстмодерн, з його розвитком інформаційних технологій та соціальних мереж і систем контролінгу за рахунок збору та обробки великих об'ємів інформації, їхньої інтерпретації та адресної видачі саме "в ці руки", "саме для тебе" поставив питання про наявність правди і істини на рівні вибірковості інформаційних потоків. Слід визнати, інформаційні технології, соціальні мережі та системи обробки великих масивів даних створили нову реальність, у якій істина та факти набувають вибіркового характеру. Це дало змогу авторитарним режимам, зокрема росії, використовувати гібридні методи війни, прикриваючись "ядерною парасолькою" та експлуатуючи страхи Заходу, фактично узаконюючи безкарність власної агресії.

У цих умовах сподівання на забезпечення післявоєнної безпеки лише міжнародними угодами залишаються декларативними, а дискусії про гарантування глобальної безпеки за рахунок системи міжнародних угод стає, як заяви про завершення війни за 50 днів – "деклараціями без виконання".

Світу, і особливо Європі, необхідна нова система стримування агресорів, здатна закласти основи тривалого миру та створити передумови для позитивної перебудови глобального порядку.

У цій статті на основі історичних фактів здійснено спробу проаналізувати можливості побудови "поясу безпеки", що підсилить чинні механізми європейської, а в перспективі й євразійської, безпекової взаємодії, формуючи перший оборонний рубіж від Балтійського до Чорного моря (рис. 1).

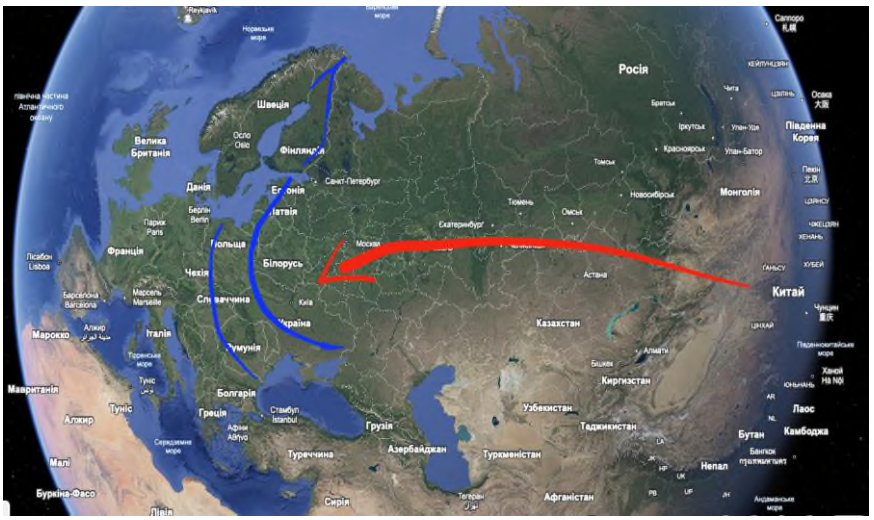


Рис. 1. Перший пояс європейської безпеки

Аналіз останніх досліджень і публікацій. У контексті формування європейського поясу безпеки для протидії загрозам зі Сходу та визначальної ролі України в ньому наразі відсутні комплексні системні дослідження. Наявні наукові та аналітичні праці здебільшого зосереджені на загальних аспектах військової, економічної та політичної підтримки України у відсічі широкомасштабній агресії рф.

Аналіз відкритих джерел свідчить, що висвітлення даної проблематики обмежується публікаціями та звітами аналітичних центрів, таких як Institute for the Study of War (США), які розглядають окремі теми, пов'язані з протидією російській агресії. Паралельно, у працях західних дослідницьких інституцій – зокрема, Royal United Services Institute (RUSI, Велика Британія), German Council on Foreign Relations (DGAP, Німеччина), Carnegie Endowment for International Peace (США-ЄС), а також European Council on Foreign Relations (ECFR, ЄС) – увага приділяється питанням трансформації системи європейської безпеки, зміцненню інфраструктури та підготовці східного флангу НАТО до потенційної агресії зі сходу. Офіційні інтернет ресурси НАТО описують ініціативу Збільшення Передової Присутності, Enhanced Forward Presence (eFP).

Водночас питання проактивного впливу України на стійкість європейської архітектури безпеки під час війни та у післявоєнний період залишається недостатньо вивченим. Йдеться насамперед про унікальну роль України як носія сучасної військової експертизи та практичного бойового досвіду, що може стати фундаментальним ресурсом у формуванні нового європейського поясу безпеки.

Методологія. Дослідження базується на міждисциплінарному підході, що поєднує історичну науку, теорію міжнародних відносин та безпекознавство. Методологія побудована на чотирьох рівнях аналізу: історико-порівняльному, інституційному, нормативно-правовому та стратегічному.

1. *Історико-порівняльний метод.* Використано для виявлення спільних рис та відмінностей у формуванні європейської системи безпеки від часів Київської Русі до сучасності. Порівняння здійснювалося за критеріями: баланс сил між провідними європейськими державами; роль України як форпосту на східному напрямі; механізми формування союзів та альянсів.

2. *Системний підхід*. Розглянуто європейську безпеку як цілісну систему, в якій Україна виступає не лише периферійним актором, а ключовим елементом захисного поясу. Цей підхід дозволив дослідити взаємозалежність між геополітичними, військовими та соціокультурними чинниками.

3. *Метод історичної ретроспекції*. Застосований для аналізу конкретних історичних епізодів: ролі Київської Русі, участі українських земель у війнах Речі Посполитої та Габсбурзької монархії, а також уроків XX століття, включно з двома світовими війнами.

4. *Аналіз міжнародних документів та стратегій*. Залучено офіційні матеріали НАТО, ЄС, ОБСЄ, Institute for the Study of War (США), Royal United Services Institute (RUSI, Велика Британія), German Council on Foreign Relations (DGAP, Німеччина), Carnegie Endowment for International Peace (США – ЄС), а також European Council on Foreign Relations (ECFR, ЄС) Стратегії національної безпеки України (2020), для зіставлення історичного досвіду з сучасними інституційними практиками.

5. *Форсайт-елементи*. Застосовано методи сценарного прогнозування для оцінки майбутнього значення України як частини східного флангу НАТО та потенційного ядра нових регіональних альянсів безпеки.

Методологічна основа забезпечує комплексність аналізу, дозволяє інтегрувати історичний досвід із сучасними викликами та сформулювати висновки щодо сталості ролі України як елементу захисного поясу Європи.

Мета статті – дослідити історичні приклади проєктів європейської єдності та спроби формування поясу безпеки для стримування загроз зі сходу. У цьому контексті розглядається сучасний стан європейського безпекового проєкту, зокрема ініціативи "Трьох

морів". Завданням дослідження є також виявлення "вікна можливостей", що відкривається для України у світлі розвитку означеної ініціативи, визначення перспектив її долучення до процесу створення європейського поясу безпеки та аргументація щодо визначальної ролі України у гарантуванні воєнної безпеки Європи як захисного щита від східної загрози.

Виклад основного матеріалу

Дослідження ґрунтується на історико-порівняльному методі. По-перше, враховуючи той факт, що війна України з рф досі триває, проводити саме історичні дослідження, саме по собі, складна задача в силу "аберації зору" за рахунок наближеності до подій та заангажованістю емоційних реакцій безпосередніх учасників подій. З метою подолання описаної складності, в дослідженні прослідковуються паралелі з історичними формами об'єднання Європи та протистояння агресії зі сходу, що пронизує весь історичний процес.

Оптимізм з'являється при погляді в історію, яка наповнена прикладами переможної битви меньшої сили з тою, що значно переважає. Наприклад, битва ізраїльтян з філістімлянами, знана по поєдинку Давида проти Голіафа; Радянсько-фінська війна (1940); Афіно-Перська війна (480 р. до н.е.); похід Олександра Великого на Персію (334-324 рр. до н.е.); радянсько-Афганська війна (1980-1989 рр.). У всіх цих війнах сильніший противник був подоланий рішучістю та відповідною тактикою, які доводили, що жодна тиранія не може бути ефективною.

Історія знає немало значних перемог коаліційних сил не найбільших держав над переважаючим ворогом, як правило, деспотичного режиму. Так у V столітті до н.е. коаліція Грецьких полісів перемогла в битвах під Марафоном (490 до н.е.), Саламіні (480 до н.е.), Платеями (479 до н.е.). У XIV–XV ст. малі альпійські громади Урі, Швіц, Унтервальден протидіяли експансії Габсбургів, та здобули перемоги в битвах під Моргартеном (1315) та Земпахом (1386).

Епоха постправди, що характеризується нечуваною раніше безвідповідальністю лідерів навіть найпотужніших країн за слова та виконання обіцянок, непомітно заповнила собою політичний та соціальний простір та створила благодатне підгрунтя для гібридної війни. Таким чином, саме ці риси нової психології, пов'язаної з феноменом постправди та дивергенцією відповідальності лідерів держав за слова та підписи на договорах, будуть ключовими викликами при формуванні пропозицій щодо забезпечення стабільності повоєнного світу. Об'єднана Європа, таким чином, не має іншого виходу, як дбати самостійно про пояс безпеки проти загрози зі сходу. Україна в означеному контексті виступає як найбільш згуртована та загартована сила, готова всіма способами протидіяти агресору і послужити центром нової системи колективної безпеки між Балтикою та Чорним морем.

Історія Європи знає низку проєктів європейської єдності. Першим із відомих в історичний час можемо вважати Римську імперію, що панувала на величезних просторах від Британії до Близького Сходу, утворюючи пояс від Германського (Північного) моря до Понту Евксинського (Чорного моря) власною територією та майже до Гірканського (Каспійського) моря – тимчасово залежними територіями давніх Вірменії, Іберії та Албанії (рис. 2).

Рис. 2. Територія Римської імперії в I ст. до н.е. - II ст. н.е.

У VIII-IX ст. франкський король Карл Великий створив імперію, що охоплювала більшу частину Західної та Центральної Європи: сучасні Франція, Німеччина, Нідерланди, Бельгія, Люксембург, північна Італія, частини Іспанії та Центральної Європи (рис. 3).

Рис. 3. Імперія Карла Великого

В якості ідеї без повної реалізації зазначимо, що папство, будучи духовним центром Західного християнства, у XI-XIII ст. шукало способи консолідувати християнські держави навколо спільної мети – боротьби з мусульманським світом, особливо на Близькому Сході. В контексті нашої роботи цікавим аспектом саме цієї спроби об’єднання є виокремлення конкретного ворога, проти якого, в цілому, задумувалось об’єднання. Держави, лишаючись в стані “самостійності” в цивільному адмініструванні, скликались саме для воєнного союзу і хрестових походів.

Наполеон Бонапарт у XIX ст. створив “континентальну систему” – фактично політичний та економічний союз під владою Франції, який мав елементи сучасної інтеграції: єдиний ринок, спільні закони, що були закріплені у Кодексі Наполеона.

Французький прем’єр Арістід Бріан у 1929-1930 рр. запропонував “Федерацію Європи” в рамках Ліги Націй.

Вінстон Черчилль у Цюриху у 1946 році закликав до створення Сполучених Штатів Європи.

Наразі у 1993 році було створено Євросоюз, що об’єднав 27 країн Європи.

Щодо захисного поясу Європи (хоч це так не називалося в ті часи і не мало сучасного вигляду) – до певної міри він був реалізований ще в часи об’єднаної Київської Руси проти “Великого степу”, тобто кочової загрози. Київська коаліція князівств виступала в ролі буфера в XI-XIII століттях. Київська Русь розташовувалася між Скандинавією, Центральною Європою і степами Північного Причорномор’я і слугувала природнім буфером “християнського світу”. З урахуванням втрачених північних територій (нині під довготривалою окупацію росії) Пскова та Новгорода, Суздалі, Рязані, Смоленська, Чуді (Карелія) Україна виконала ту саму функцію “захисного пояса” Європи, через який намагаються прорватись ново-ординські дикі кочовики із росії (рис. 4).

Рис. 4. Київська Русь

У геополітичниму плані Австрія в XVI-XVIII століттях виступала буфером Європи проти османів.

У XV-XVII столітті Польща виступала буфером проти російської експансії та стримувала експансію москви на Захід.

Таким чином, ми бачимо низку історичних спроб політичного та військового об’єднання Європи, проти загрози зі сходу, що можуть слугувати підгрунтям для сучасного створення поясу захисту від нової євразіййської “осі зла”. Європа наразі виступає в багатьох аспектах природньо об’єднаним геополітичним простором протягом більш ніж тисячі років.

Щодо більш широких проєктів об’єднання вже у масштабі Євразії, першим прикладом постає Східний похід Олександра Великого (Македонського) 334-323 рр. до н.е.. Він об’єднав території від Балкан до Гімалайських районів Індії (рис. 5). Держава Олександра створює той пояс, що являє цікавість для продовження серії статей, що

пропонують розширення першого поясу безпеки Європи на Схід і створюють план стратегічного охоплення країни-агресора.

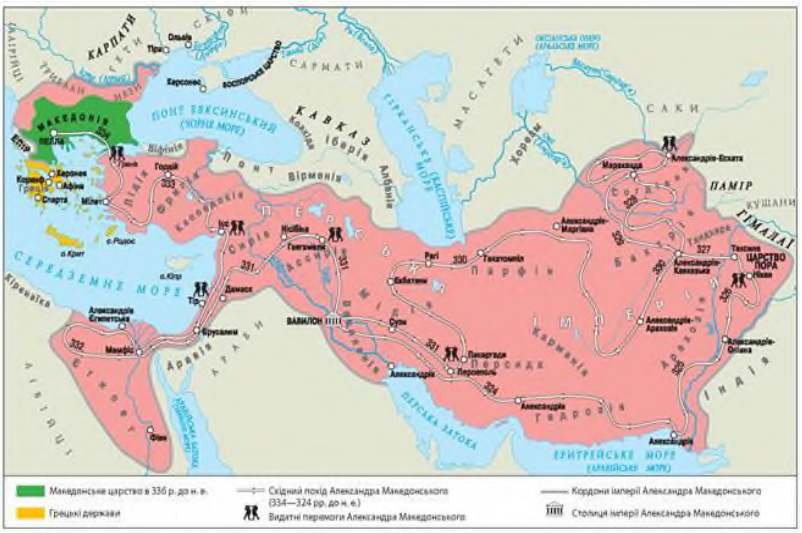


Рис. 5. Держава Олександра Великого

Історія міжнародної безпеки містить численні приклади невдач організацій, створених для запобігання війнам та агресії. Зокрема, Ліга Націй, попри свої благородні цілі, не змогла зупинити агресію Італії в Ефіопії у 1935 році, оскільки накладені санкції були обмеженими та неефективними. Подібно, Організація Об'єднаних Націй не змогла запобігти геноциду в Руанді у 1994 році, коли миротворці, незважаючи на наявність мандату, не змогли зупинити масові вбивства через обмеження в правилах ведення бою та відсутність політичної волі. Також НАТО, незважаючи на свою потужність, не змогло ефективно запобігти агресії Росії в Україні, що поставило під сумнів здатність альянсу захищати своїх членів від зовнішніх загроз.

Зважаючи на міждисциплінарний характер статті, що поєднує історичний аналіз, міжнародну безпеку та державне управління, нижче наведено таблицю з прикладами провалів безпекових інтситуцій, засновану на історичній фактології [9-12].

Наведені в табл. 1 приклади засвідчують системну неспроможність міжнародних безпекових інституцій ефективно реагувати на прояви агресії та запобігати ескалації конфліктів. Незалежно від регіону чи масштабу протистояння, Ліга Націй, ООН та інші структури виявляли обмеженість своїх механізмів дії, що пояснюється як політичною залежністю від великих держав, так і браком інструментів примусу. У результаті світова безпекова архітектура протягом XX–XXI століть не змогла виробити універсальних і дієвих механізмів запобігання агресії. Цей факт підтверджує актуальність пошуку нових моделей колективної безпеки, серед яких ініціатива створення європейського "поясу безпеки" може стати центральним елементом для стримування загроз у майбутньому.

Таблиця 1

Приклади провалів міжнародних безпекових інституцій

Період / Подія	Роль міжнародних організацій	Наслідки
1930-ті: Ліга Націй	Нездатність Ліги Націй запобігти агресії Італії проти Ефіопії та агресії Японії в Маньчжурії	Ліга Націй втратила авторитет і була розпущена
1950–1953: Корейська війна	ООН не змогла запобігти війні, втручання відбулося лише через коаліцію під проводом США	Мільйони жертв, поділ Кореї зберігся донині

Продовження табл. 1

1955–1975: В'єтнамська війна	ООН фактично не вплинула на перебіг конфлікту	Величезні людські втрати, стратегічна поразка США
1967, 1973: Арабо-ізраїльські війни	ООН та Рада Безпеки ООН не зупинили військові дії	Збереження затяжного конфлікту на Близькому Сході
1979–1989: Афганська війна (СРСР)	ООН виявилася безсилою перед радянською інтервенцією	Десятки тисяч загиблих, радикалізація регіону
1992–1995: Війна в Боснії	ООН та НАТО діяли повільно, що спричинило масові жертви	Етнічні чистки, понад 100 тис. жертв
1999: Косово	Рада Безпеки ООН була паралізована через вето рф	Гуманітарна катастрофа, втручання НАТО поза рамками ООН
2008: Російська агресія в Грузії	Міжнародні організації не запобігли окупації частини території Грузії	Фактична легалізація сфери впливу рф на Кавказі
2014: Анексія Криму	ООН і ОБСЄ не зупинили анексію Криму	Порушення міжнародного права, посилення агресивності рф
2022: Повномасштабна агресія РФ проти України	ООН, ОБСЄ та інші інституції не змогли стримати російську агресію	Найбільша війна в Європі з часів Другої світової війни

Щодо сучасного формату роботи елементів та ініціатив "поясу безпеки", що можуть бути включені в майбутню інтегровану систему, варто зазначити Three Seas Initiative (3SI) як ініціативу 12-ти держав між Балтійським, Адріатичним та Чорним морями для розвитку транспортної, енергетичної та цифрової інфраструктури.

Хоча 3SI офіційно не є військовим альянсом, вона має стратегічний і безпековий вплив.

По-перше, пропрацьовується проблематика енергетичної незалежність, шантаж якою завжди був козирною картою рф. Проєкт має на увазі зменшення залежності від російського газу і нафти через LNG-термінали, трубопроводи (Baltic Pipe, інші газові коридори). Всі енергетичні проєкти зміцнюють стійкість до економічного та гібридного тиску РФ.

Другою складовою постає інфраструктурна інтеграція, в якій поліпшення транспортних коридорів (дороги, залізниця, порти) між Балтійським і Чорним морями покращує спроможність забезпечити швидке переміщення військ та матеріалів у разі криз, тобто потенційно підвищує колективну обороноздатність.

Наступним аспектом постає політична координація, оскільки 3SI створює міжурядовий майданчик для узгодження позицій країн щодо безпеки, економіки та енергетики, а також підтримує співпрацю з НАТО та ЄС, інтегруючи безпекові та стратегічні ініціативи [1-3]. За винятком Угорщини, країни 3SI цілковито підтримують Україну в відбитті агресії рф, як і допомогу Україні будь-якими третіми країнами [2].

В ініціативах описаних вище немає присутності США. Європейські країни виступають в ініціативі 3SI як самостійні і ті, що можуть дати раду проєкту. Вельми цікавою в означеному контексті є публікація провідного видання Financial Times 20 лютого 2025 року: "Балтійська самодостатність – це попередження для Вашингтона", і далі – "Перетворення американської військової підтримки з життєво необхідної на таку, що лише "добре мати", послабить глобальний вплив США" [4]. Нагадаємо, що означені публікації почали мати місце після того, як в результаті незрозумілого маневрування китайського контейнеровозу Ньюнью Полярний Ведмідь було пошкоджено декілька підводних

інфраструктурних кабелів та у газопроводі Balticconnector було втрачено тиск [4]. Означена подія надає нового звучання всьому проєкту Європейського поясу безпеки, включаючи Китай до євразійської "осі зла".

Наразі найбільша співпраця в оборонній сфері відбувається саме в Балтійському морі. Згуртованість Європейських країн посилюється риторикою президента США Дональда Трампа щодо необхідності збільшення воєнних витрат європейськими країнами та всіма членами НАТО [5; 6].

У той же час на суходолі саме воєнних ініціатив бракує. Офіційні джерела НАТО/ОТАН [7] описують ініціативу НАТО Збільшення Передової Присутності, Enhanced Forward Presence (eFP). А саме: "В останні роки союзники посилили передову присутність НАТО, створивши багатонаціональні бойові групи в Болгарії, Естонії, Угорщині, Латвії, Литві, Польщі, Румунії та Словаччині. Також вони направили більше кораблів, літаків і військ уздовж східного флангу НАТО". Більш детально – станом на лютий 2025 року вісім батальйонно-тактичних груп розміщені на території таких країн: Болгарія, Естонія, Угорщина, Латвія, Литва, Польща, Румунія, Словаччина. Представлені сили наступних країн: Албанія, Хорватія, Греція, Італія, Чорногорія, Північна Македонія, Туреччина, США, Великобританія, Чехія, Ісландія, Північна Македонія, Польща, Словаччина, Словенія, Іспанія, Швеція, Бельгія, Люксембург, Нідерланди, Норвегія, Румунія, Португалія. Усі вісім бойових груп інтегровані у командну структуру НАТО для забезпечення необхідної готовності та оперативності [8]. Строк розгортання бойових груп ставиться в 30 днів [8]. Проте, якщо взяти до уваги зухвалу атаку 24 лютого 2022 року рф, колонами вздовж автодоріг, то існує висока вірогідність, що просування буде швидшим і необхідно мати сили, які стримають російські війська протягом 30 днів.

Якщо прийняти до уваги останні події в геополітичному просторі, який потрясають неперебачувані дії Вашингтону, європейські держави опинилися ситуації, коли пріортитетним стає розвиток автономної системи безпеки та зміцнення власних оборонних союзів. Україна в даному контексті може виступити як ініціатор побудови сухопутної лінії оборони, враховуючи чотирьохрічний досвід відбиття повномасштабного вторгнення рф, та у повоєнному світі стати лідером поясу європейської безпеки трьох морів.

Висновки

Дослідження засвідчило численні випадки, коли міжнародні безпекові інституції не змогли ефективно реагувати на агресію та конфлікти, що призводило до значних людських та територіальних втрат. Водночас аналіз показав низку історичних епізодів, зокрема, коли територія нашої держави виступала своріднім щитом Європи від східних загроз, а також приклади результативної протидії ворогам, які мали чисельну перевагу. Україна, як спадкоємниця Русі Київської, була в історичному періоді IX-XIII століття щитом-буфером-форпостом проти Великого степу.

На Сході існує вислів: "Навіщо мене знову тиснуть обставини? Невже я сам не міг возвиситись?" В умовах війни, нерішучості європейських партнерів та хаотичних впливів з боку Вашингтону, Україна отримує нові можливості на міжнародній арені. У народі кажуть: "Не було б дощу – не зійшло б жито", що символізує здатність перетворювати труднощі на шанс для розвитку.

Необхідність захисту сучасної Європи від навали зі Сходу, що не обмежується лише російською воєнною загрозою, а все більше висуває проблему китайського розповсюдження гегемонії, виводить Україну в позицію стрижневого ресурсу та партнера Євросоюза та 3SI в побудові захисного поясу Європи на суходолі, де позиції 13 країн 3SI не такі міцні, як у водах Балтики.

Україна як держава, що з одного боку найбільше постраждала від агресії рф, а з іншого – побудувала армію, здатну ефективно протидіяти агресору, має можливість стати

центром, навколо якого згуртуються нації поясу від Балтики до Чорного моря. Перебуваючи на передовій боротьби з агресором, наша держава може стати визначальним елементом у формуванні нового європейського поясу безпеки, використовуючи свій досвід та географічне розташування. Потрібно скористатись тим статусом, що дає досвід війни в очах країн-партнерів.

Україна має можливість, підключившись до ініціатив 3SI, надати нову хвилю співробітництву країн угоди "Трьох морів" та почати розбудову воєнної складової союзу: лінії оборони, ППО, взаємодія центрів управління, обмін розвідданими, регіональні навчання, в перспективі спільна військова доктрина регіону.

Насамперед, саме наша держава в силу багатьох чинників війни усвідомлює "червоний рівень" загрози та готова до прийняття рішучих дій по укріпленню захисного поясу Європи. Україна, як ніхто інший відчуває гостроту проблеми. Ця готовність, насамперед покликана не допустити зволікання у процесі розвитку воєнного поясу захисту Європи. Кожен день зволікання помножує жертви, а з іншого боку дозволяє зростати нахабству та самовпевненості країни-агресора, що буде коштувати багатьох жертв.

Рекомендації щодо зміцнення європейського поясу безпеки за участі України

1. Розширення дипломатичних консультацій та інтеграція у регіональні ініціативи

Міністерству закордонних справ України рекомендується активізувати постійні консультації з партнерами ЄС, державами-членами НАТО та учасниками ініціативи "Трьох морів" (3SI) з метою формалізації участі України у регіональних безпекових проєктах. Необхідно визначити конкретні інструменти співпраці, включно з правовими та фінансовими механізмами, що дозволять інтегрувати український досвід війни у стратегії колективної безпеки Європи. Виходячи з потреби країн Європи захиститись від російської загрози найменшою кров'ю, чи взагалі, не проливаючи кров своїх громадян, Україна може зайняти лідируюче положення саме в аспекті створення та реалізації єдиної військової доктрини регіону.

2. Формування спільної військової доктрини регіону

Україна має взяти активну роль у розробці регіональної військової доктрини, що поєднує сучасні концепції колективної оборони, використання технологій протидії гібридним загрозам та інтеграцію засобів ППО. Основна мета – мінімізувати ризики для країн Європи при протидії агресії, забезпечуючи оперативну та ефективну реакцію без значних людських втрат. Водночас, в інтересах підвищення оборонної спроможності ЄС необхідно інвестувати в розвиток власних оборонних технологій та зменшити залежність від зовнішніх постачальників, зокрема США.

3. Створення інтегрованої системи раннього попередження агресії

Поступово розробити та впровадити міжурядові угоди щодо обміну розвідувальною інформацією, логістичної підтримки та координації регіональних навчань. Розробити спільні платформи для обміну розвідданими між країнами ЄС, НАТО та іншими партнерами, що дозволить оперативно реагувати на потенційні загрози. Окрім того, доцільно формувати єдину європейську систему управління повітряною обороною та протиповітряного захисту в межах регіонального поясу безпеки, зокрема шляхом інтеграції центрів управління та навчально-тренувальних програм для військ різних держав.

4. Використання "вікна можливостей" для зміцнення позицій України

Визнати вагому роль України як чинника стабільності та оборони Європи та надати їй більшу роль у прийнятті рішень у рамках європейських безпекових структур. З огляду на досвід війни та набуту військову спроможність, Україна має скористатися унікальним статусом надійного партнера, який реально відчуває загрози та здатен швидко реагувати на них. Рекомендовано визначити стратегічні пріоритети, що дозволять прискорити інтеграцію українських оборонних здобутків у регіональні безпекові системи, включно з координацією оборонних ініціатив, стандартизацією навчань та модернізацією озброєнь.

Список літератури

1. Joint Declaration of the Eighth Summit of the Three Seas Initiative, Bucharest, 2023. URL: https://3seas.eu/media/joint-declaration-of-the-eighth-summit-of-the-three-seas-initiative?
2. Joint Declaration of the 10th Summit of the Three Seas Initiative, Warsaw, Polland, 2025. URL: https://3seas.eu/media/news/joint-declaration-of-the-10th-summit-of-the-three-seas-initiative.
3. Research Papers. Selection of research papers and reports on the Three Seas Initiative. URL: https://3seas.eu/about/research-papers.
4. Baltic self-sufficiency is a warning for Washington, 20FEB2025, Financial Times. URL: https://www.ft.com/content/d72e37c7-8597-4807-879c-dca1074924cb.
5. The Baltic Nimes. Trump dubs Baltic states as example for other NATO countries for defense financing. URL: https://www.baltictimes.com/trump_dubs_baltic_states_as_example_for_other_nato_countries_for_defense_financing/.
6. US Department of Defence, NATO Leaders Pledge to Increase Defense Spending, 25JUN2025. URL: https://www.defense.gov/News/News-Stories/Article/article/4226009/nato-leaders-pledge-to-increase-defense-spending/.
7. NATO/OTAN, NATO’s military presence in the east of the Alliance, 6JUN2025. URL: https://www.nato.int/cps/en/natohq/topics_136388.htm.
8. NATO/OTAN ALLIED LAND COMMAND, Enhanced Forward Presence (eFP). URL: https://lc.nato.int/operations/enhanced-forward-presence-efp.
9. Gooch G.P. History of Modern Europe, 1878-1919. 2nd ed. London: Longmans, Green, and Co., 1932.
10. United Nations. UN Peacekeeping: 70 Years of Service & Sacrifice. United Nations, 2018.
11. Warren T.D. ISAF and Afghanistan: The Impact of Failure on NATO's Future. ResearchGate, 2010.
12. Stracquadanio D. Europe’s Humiliating Exclusion From Ukraine Talks Is Its Own Fault. The Moscow Times, 19 Feb. 2025.

УДК 351.864:006.063 DOI: 10.63978/3083-6476.2025.2.2.10

Пацек Богуслав
доктор хабілітований, професор
Ягеллонський університет
Краков, Польща
e-mail: bpacek@op.pl
ORCID: 0000-0001-8111-1682

Пєвцов Геннадій Володимирович
доктор технічних наук, професор
Інститут проблем реєстрації інформації
НАН України
Київ, Україна
ORCID: 0000-0002-0426-6768

ВІЙСЬКОВА ДОКТРИНА РОСІЙСЬКОЇ ФЕДЕРАЦІЇ: ІСТОРИЧНА ЕВОЛЮЦІЯ ТА ЗАСТОСУВАННЯ В КОНТЕКСТІ ВІЙНИ В УКРАЇНІ

Анотація. *Стаття присвячена аналізу історичної еволюції та трансформації російської військової доктрини від початку XX століття до сьогодення. Розглянуто ключові етапи та військові конфлікти, зокрема польсько-радянську війну, Зимову війну, війну в Афганістані, Чеченські та Грузинська війни, а також їхній вплив на розвиток російської військової думки. Особливу увагу приділено пострадянським військовим доктринам і впливу так званої "концепції Герасимова" на сучасну російську військову стратегію. Визначено спільні риси російських військових дій, зокрема обґрунтувань агресії, готовність до значних людських втрат і схильність до вчинення воєнних злочинів. Метою дослідження є визначення ключових етапів та факторів, що сформували російське військове мислення, а також окреслення основних тенденцій і характеристик сучасної військової доктрини росії в контексті її тривалої агресії проти України.*

Ключові слова: *військова доктрина, російська федерація, гібридна війна, Україна.*

Bohuslav Patsek
Doctor of Habilitation, Professor
Jagiellonian University
Krakow, Poland
e-mail: bpacek@op.pl
ORCID: 0000-0001-8111-1682

Hennadii Pievtsov
Doctor of Engineering Science, Professor
Institute for Information Recording
of the NAS of Ukraine
Kyiv, Ukraine
ORCID: 0000-0002-0426-6768

THE MILITARY DOCTRINE OF THE RUSSIAN FEDERATION: HISTORICAL EVOLUTION AND APPLICATION IN THE CONTEXT OF THE WAR IN UKRAINE

Abstract. *The article is dedicated to analyzing the historical evolution and transformation of russian military doctrine from the early 20th century to the present day. It examines key periods and military conflicts-such as the*

Polish-Soviet War, the Winter War, the war in Afghanistan, the Chechen and Georgian wars-highlighting their impact on the development of Russian military thought. Special attention is paid to post-Soviet military doctrines and the influence of the so-called "Gerasimov Doctrine" on contemporary Russian military strategy. The article identifies common features of Russian military operations, including the justification of aggression, readiness to sustain heavy human losses, and a tendency to commit war crimes. The goal of the study is to identify the key stages and factors that have shaped Russian military thinking, as well as to outline the main trends and characteristics of Russia's current military doctrine within the context of its ongoing aggression against Ukraine. The analysis demonstrates that during the initial phase of the full-scale invasion of Ukraine, the Russian Federation implemented its 2014 military doctrine and General Gerasimov's concept, which emphasized non-military means and rapid, decisive action. However, failures during the first year of the war-due to a variety of factors-forced Russia to adjust its tactics and methods of combat employment. Since 2024, modern drone technologies and electronic warfare have become a central element of combat operations for both sides, providing advantages in intelligence gathering, precision strikes, and countermeasures. As a result, the Russo-Ukrainian War has fundamentally transformed the nature of modern warfare, making the prospect of victory directly dependent on the development and integration of new technologies.

Keywords: *military doctrine, Russian Federation, hybrid warfare, Ukraine.*

Вступ

Постановка проблеми. Росія, як одна з наддержав, тривалий час брала активну участь у формуванні світової історії. Протягом років російська військова думка зазнавала значної еволюції, відображаючи як внутрішні соціально-політичні процеси, так і зміни в міжнародній обстановці. Історична трансформація військової доктрини росії є складним і багатогранним процесом, вивчення якого має важливе значення для розуміння сучасної російської зовнішньої та оборонної політики, а також для оцінки потенційних загроз і викликів міжнародній безпеці.

Цікавим явищем є те, що, незважаючи на великі зміни у світі, пояснення росією причин своїх військових дій завжди залишаються незмінними та обґрунтовуються необхідністю захисту своєї країни від потенційної агресії або порятунку пригноблених груп російськомовного населення. Так, під час польсько-радянської війни 1919-1921 років це був порятунок пролетаріату від гніту правлячих еліт, під час Зимової війни – порятунок населення північної росії від агресії фінів, під час нападу на Польщу у 1939 році – порятунок українського та білоруського населення, а під час вторгнення в Україну – захист від НАТО та порятунок російськомовного населення [1-2].

Одною з головних рис російських війн та конфліктів є продовження їх ведення навіть ціною великих людських втрат, що обумовлено наявністю значних людських ресурсів, особливо в порівняні з європейськими країнами. Незмінною для ведення воєнних дій росіянами також залишається схильність до скоєння масових воєнних злочинів. Цей елемент завжди є важливим чинником російських війн та конфліктів та має за мету зниження морального духу противника та ліквідацію потенційного опору цивільних. Це відбувалося у Фінляндії, Афганістані, Чечні, Сирії, Катині та Україні [3-8].

Під час конфліктів з багатьма країнами росіяни допускали чимало помилок, але водночас демонстрували здатність до навчання та адаптації в нових умовах. Здатність до адаптації може дати перевагу над противником, тому важливо відстежувати зміни, що відбуваються, і використовувати їхні слабкі сторони [9].

Аналіз останніх досліджень і публікацій. Багато дослідників зробили значний внесок у вивчення російської військової доктрини. Так, Гудрун Перссон у роботі "Російська військова думка: еволюція стратегії з часів Кримської війни" аналізує історичний контекст і відкидає спрощені уявлення багатьох західних експертів про російське військове мислення [10]. В подальшому Марк Галеотті, ввів термін "доктрина Герасимова". Погляди Галеотті істотно вплинули на початкове західне розуміння підходу Росії до сучасної війни, підкресливши інтеграцію невійськових і військових тактик. У той же час робота Дмитра Адамського "Російський спосіб стримування", показує, що російський підхід до примусу,

який він називає стримуванням, заснований насамперед на культурних, ідейних та історичних факторах [11]. До цього висновку також приходять Павло Лузін і Євген Рощин у своєму дослідженні "Стратегія і військове мислення росії: Еволюціонуючий дискурс до 2025 року". Вони виділяють три різні групи, що, на їхню думку, істотно впливають на військову стратегію росії: ідеологію, публічні стратегії і практики [12]. Показано, що військова доктрина не є монолітною, а розуміння різних ідеологічних та інституційних аспектів допомагає передбачати можливі зміни в ядерній доктрині та тактиці наземних операцій.

Мета статті присвячена аналізу формування та трансформації російської військової доктрини. Метою дослідження є виявлення ключових етапів та факторів, що вплинули на розвиток російського військового мислення, а також визначення основних тенденцій і характеристик сучасної військової доктрини росії з урахуванням її тривалої агресії проти України.

Виклад основного матеріалу

Розвиток російської держави, централізованої навколо Москви, почався відносно пізно порівняно з іншими європейськими державами. Протягом більшої частини Середньовіччя росія займала невеликі території навколо Москви, перебуваючи в багатьох конфліктах з іншими слов'янськими князівствами та монголо-татарами. Під владою Золотої Орди Московське князівство залишалося аж до Куликовської битві 1380 року. З того часу почалися успіхи Москви та поступове зміцнення її впливу в регіоні. Завдяки православній церкві, яка об'єднувала більшість слов'янських племен, була реалізована концепція об'єднання земель в один державний організм [13].

Важливою подією, яка стала початком російського експансіонізму, був занепад Константинополя та шлюб Івана III із Зоєю Палеолог, племінницею останнього візантійського імператора. Іван III прийняв як герб візантійського двоголового орла оголосив себе спадкоємцем Римської імперії . Онук Івана III та Зої, Іван IV Грозний, першим назвав себе російським царем [14]. Перші роки його правління пройшли під знаком реформ, що централізували владу в значно розширеній, після завоювань його діда та батька, державі, та військових походів, завдяки яким він підкорив собі ханства, що виникли після розпаду Золотої Орди. Після завоювання казанської землі Іван IV одразу розпочав християнізацію місцевого населення, що мало збільшити його залежність від Москви. Природний кордон у вигляді річки Волги та збудовані вдовж неї укріплення забезпечували Москві та землям на схід від неї безпеку від монгольських набігів та сприяли їхньому значному економічному розвитку. Завдяки новим завоюванням виникли торгові шляхи до Китаю, Індії та Персії. Щоб покращити цей торговий потік, на Білому морі в Архангельську був побудований порт. Однак гирло Волги контролювалося Астраханським ханством. Тому Іван IV вирішив завоювати ці землі, а відразу після їхнього завоювання, подібно до Казані, охрестив їх, підпорядкував центральній владі в Москві [14]. В подальшому це відкрило росії можливість колонізації Сибіру за аналогічною схемою. Після зміцнення своєї влади на сході Іван розпочав кампанію на заході, бажаючи збільшити російські впливи в Європі.

Під час правління царя Петра I росія розпочала кампанії, щоб здобути доступ до стратегічних морів та Світового океану. Щоправда, існував порт в Архангельську, але Біле море надовго замерзло протягом зими, що значно ускладнювало рух товарів. Петро I вирішив, що російська імперія, яка вже була частиною Священної ліги, використає війну з Османською імперією та здобуде доступ до Азовського моря [15]. Після його завоювання він наказав збудувати військово-морську базу Таганрог. Перемога в битві під Полтавою увінчала багаторічні зусилля росії та надала їй доступ до Балтійського моря [15]. Незважаючи на пізніші втрати на півдні, зокрема Азова та Таганрога, саме Петро I визначив

напрямок майбутніх західних російських експансій у Балтійському, Азовському та Чорному морях, а також на Кавказі, які здійснювали наступні правителі російської імперії, СРСР, а потім і сучасної росії.

1. Формування основ (1919-1991)

Після поразки в Першій світовій війні та революції 1917 року більшовики вже у 1919 році розпочали свої перші наступальні військові операції. Їхньою метою було повернення територій, які ще недавно належали російській імперії і на яких почали виникати національні держави – Польща, Українська Народна Республіка, Латвійська Республіка та Білоруська Народна Республіка. Більшовики також прагнули, згідно з філософією Леніна, розпочати всесвітню революцію пролетаріату та активну боротьбу з капіталізмом. Використовуючи відступ німецьких окупаційних військ, більшовицькі війська почали займати покинуті території в околицях Мінська, Вільнюса, Молодечна, Поневежа, Слоніма та Сарн [16].

Важливі дії відбулися у 1920 році, коли основні воєнні дії точилися на території Польщі – на двох головних напрямках: північному – з територій так званої Смоленської брами, та південному – з територій сучасної України. Їх розділяло Полісся, яке через велику кількість боліт і заболочених ділянок не підходило для ведення активних воєнних дій. Незважаючи на початкові успіхи більшовиків на півночі, польським підрозділам вдалося зупинити наступ на територіях сучасної Білорусі. Однак на півдні більшовикам вдалося захопити Київ, замкнувши його в оточенні. Воєнні дії, що велися більшовиками, мали ознаки маневрової, а не позиційної війни, як це було під час Першої світової війни [17]. Активність північного фронту почала слабшати на початку серпня 1920 року. Остаточну поразку більшовицьких військ було спричинено, насамперед, надмірним розтягненням армій, які, ведучи бойові дії на двох окремих фронтах, не мали достатньої наступальної сили, щоб остаточно знищити польську армію. Частина командування Червоної армії піддалася ілюзії легкості досягнення здобутків та можливості проведення комуністичних революцій не лише в Польщі, а й в інших європейських країнах. Крім того, негативну роль відіграли особисті амбіції головних командирів Південного фронту, які ігнорували накази підтримати наступ військ Північного фронту й натомість намагалися збільшити свої перемоги на півдні, що ще більше підірвало наступальні можливості більшовиків [17].

Після поразки у війні з Польщею Червона армія зазнала значної реформи. Через робітничі та селянські повстання, а також складну економічну ситуацію було вирішено суттєво скоротити її чисельність і реформувати систему підготовки військових кадрів. Уже у 1925 році була сформована концепція кадрових змін і матеріального переоснащення Червоної армії. Окремо підкреслювалася важливість якнайшвидшого перенесення воєнних дій на територію ворога та можливість ефективного стримування потенційної агресії за допомогою чисельної та сучасно оснащеної армії. Радянські військові, спираючись на досвід Першої світової війни та війни з Польщею, в 1930-х роках розробили сильно централізовану доктрину глибоких операцій, яка підкреслювала роль мобільності, зосередженні різних видів збройних сил на одному напрямку, а також на розширенні ролі бронетанкових підрозділів [18]. У веденні бойових дій найефективнішим способом прориву оборони противника вважалося створення пролому в обороні, проникнення штурмових підрозділів у глибокий тил для нівелювання можливостей відновлення оборони, з подальшим наступом основної частини військ через пролом в обороні. Крім того, велика увага приділялася логістичному забезпеченню та охороні ліній постачання – задля збереження наступального потенціалу військ [19]. Важливу роль відігравала провідна комуністична ідея, яка передбачала боротьбу пролетаріату, незалежно від національності, та повне знищення капіталістичних держав [18]. Однак через чистки, проведені Сталіним у 1930-х роках, жертвами яких стали насамперед найбільш досвідчені й підготовлені офіцери,

концепція глибоких операцій не могла бути реалізована в повному обсязі під час Другої світової війни [19].

Першою такою спробою стало вторгнення до Фінляндії та Зимова війна. Перед початком бойових дій деякі радянські військові високопосадовці очікували швидкого розгрому фінського опору та включення цих територій до СРСР. Було навіть замовлено спеціальну сюїту у Дмитра Шостаковича, яку планували виконати на параді в Гельсінкі. Радянські війська напали на Фінляндію без формального оголошення війни 30 листопада 1939 року. Вторгнення відбувалося за одним головним напрямком – Карельський перешийок та місто Віїпурі, а також трьома додатковими: на північ від Ладозького озера з фланговою атакою, що мала на меті оточення фінських військ; у напрямку Ботнічної затоки, щоб розділити Фінляндію на дві частини; та в напрямку Петсамо. Спочатку СРСР досяг певних успіхів, проте доктрина глибоких операцій, розроблена для рівнин Східної Європи, виявилася надзвичайно неефективною в умовах густо залісненої й болотистої місцевості Фінляндії, з обмеженою кількістю доріг. Така місцевість унеможливлювала ефективну координацію різних родів військ та знижувала мобільність моторизованих та механізованих підрозділів. Крім того, радянські війська не мали належної розвідувальної підготовки та не були готові до ведення бойових дій у зимових умовах. Втрати на початковому етапі, а також неможливість подальшого просування змусили командування сил СРСР змінити стратегію ведення війни, зосередившись на захопленні окремих регіонів і примушенні фінів до мирних переговорів. Також, усупереч доктрині глибоких операцій, було здійснено децентралізацію управління. На оперативному рівні покращено логістичне забезпечення та вжито заходів для підвищення морального духу солдатів. Використовуючи чисельну перевагу, радянські війська зосередили основні зусилля на фронтальних атаках укріплень і перевантаженні фінської оборони, навіть ціною значних людських втрат. На тактичному рівні вдалося суттєво покращити можливості розвідки, використовуючи літаки та аеростати. Також було збільшено кількість артилерії, яка проводила підготовчі обстріли перед штурмами піхоти, а штурмові підрозділи отримали базові бронежилети. Усе це сприяло прориву фінського опору на західній частині лінії Маннергейма й змусило фінський уряд розпочати мирні переговори та піти на поступки СРСР [3].

Після закінчення Другої світової війни СРСР та Сполучені Штати увійшли в стан, який згодом отримав назву “холодна війна”. Найхарактернішою рисою цього періоду стала гонка озброєнь між двома наддержавами, яка супроводжувалася розвитком нового виду зброї – ядерної. Стратегія володіння таким озброєнням була продиктована його безпрецедентною руйнівною силою. Доктрина, відома під назвою взаємно гарантованого знищення, теоретично мала гарантувати мир та запобігти ядерній війні. Завдяки дотриманню цієї доктрини, з часів Другої світової війни жодна ядерна зброя не була використана в бойових цілях, хоча загрози її застосування все ж виникали (наприклад, під час Карибської кризи).

Інтервенція військ СРСР в Афганістані мала на меті збільшення власного впливу в цьому регіоні, багатому на природні ресурси, та встановлення уряду, прихильного до співпраці з Радянським Союзом. Вона розпочалася з операції “Шторм-333”, у результаті якої, після десанту підрозділів ВДВ та штурму президентського палацу, загинув Хафізулла Амін, а його місце обійняв прихильний до Москви Бабрак Кармаль. Одночасно на територію Афганістану було введено дві дивізії. Війська СРСР не могли розміщуватися по всій країні, тому були обрані стратегічні пункти, які вони контролювали. Такими пунктами були найважливіші міста, дороги, місця видобутку природних ресурсів та лінія кордону з СРСР. Наприкінці 1980-х років було ухвалено рішення про виведення радянських військ з Афганістану. Причин цієї поразки можна назвати кілька. По-перше, радянські війська були підготовлені до конвенційних бойових дій, а не до партизанської війни. По-друге, СРСР приділяв недостатньо уваги культурним чинникам і не зміг переконати афганців у соціалістичному баченні держави [20-21].

2. Воєнні доктрини російської федерації

Після розпаду СРСР у 1991 році в росії відбулося багато змін, зокрема, щодо державних кордонів, ставлення до Заходу та відкритості до іноземних інвестицій. Перше десятиліття після розпаду стало періодом пошуку росією військової ідентичності та розробки доктринальних основ, які б відповідали новим геополітичним реаліям. На початковому етапі простежувався період роззброєння, співробітництва та транспарентності у відносинах між росією і США [22].

Військова доктрина 1993 року: Пострадянські погляди

У 1993 році була ухвалена перша після розпаду СРСР воєнна доктрина. Її формування значною мірою зумовили геополітичний контекст і проблеми безпеки того періоду. Доктрина була спрямована на захист національних інтересів росії, а однією з найбільш суттєвих змін стало офіційна відмова від радянського зобов'язання не застосовувати ядерну зброю першими. Це рішення пояснювалося істотним ослабленням звичайних збройних сил, унаслідок чого ядерна зброя почала розглядатися як основний інструмент стримування агресії.

Сама доктрина характеризувалася як оборонна, і в ній підкреслювалося, що росія не має потенційних противників [23]. Основну небезпеку становили локальні війни та регіональні конфлікти. У доктрині розрізнялись зовнішні військові небезпеки та військові загрози. Зокрема, як загрози розглядалися територіальні претензії та втручання у внутрішні справи росії. Доктрина відображала перехід від радянської орієнтації на глобальну конфронтацію до занепокоєння щодо регіональної нестабільності на пострадянському просторі.

Ключовими військово-політичними принципами та стратегічними цілями доктрини були запобігання війні та відбиття агресії, перевага надавалася невійськовим засобам врегулювання конфліктів. Доктрина була спрямована на захист національних інтересів російської федерації, стратегічні цілі були насамперед зосереджені на національній обороні та підтримці стабільності в безпосередній близькості від кордонів країни, що відображало зниження глобального впливу росії.

Роль та умови застосування ядерної зброї в доктрині полягали головним чином у стримуванні. У цьому росія зблизилася з ядерною доктриною західних країн.

Принципи застосування звичайних збройних сил передбачали створення менших за чисельністю, легших та мобільніших збройних сил з покращеними можливостями швидкого розгортання. Проте реалізація цих змін виявилася складною. Збройні сили також могли застосовуватися для захисту від антиконституційних дій та незаконного збройного насильства, що загрожують територіальній цілісності країни. Акцент на мобільність і швидке розгортання військ вказував на прагнення реагувати на регіональні конфлікти та внутрішню нестабільність, а не на ведення широкомасштабної війни. Створення нової доктрини мало на меті показати міжнародній спільноті шлях, яким російська федерація хоче йти. Росія мала залишатися однією з наддержав, але вже згадувала США та НАТО як партнерів, а не як загрозу [22; 24].

Військова доктрина 2000 року: адаптація до нових реалій

Важливим етапом подальшої трансформації російської військової доктрини стала війна в Косово 1999 року та Друга чеченська війна. Олексій Арбатов у праці "Трансформація російської військової доктрини: уроки Косово та Чечні" зазначає, що ці війни мали глибокий вплив на російське мислення у сфері безпеки та військову доктрину [22]. Арбатов стверджує, що росія винесла з Косово низку ключових уроків, зокрема сприйняття того, що мета виправдовує засоби, ефективність масованого застосування сили, зневагу до міжнародного права та важливість контролю над інформаційним простором.

Це, а також досвід чеченської війни, сприяло перегляду російської військової доктрини, що знайшло відображення у Воєнній доктрині 2000 року.

Доктрина 2000 року також характеризувалася як оборонна, розглядала як внутрішні, так і зовнішні військові загрози, підкреслюючи важливість стримування агресії та забезпечення військової безпеки. Військово-політична обстановка характеризувалася зниженням загрози великомасштабної війни, але зростанням впливу нетрадиційних загроз, таких як тероризм, та можливістю ескалації регіональних конфліктів [25].

Військово-політичні принципи та стратегічні цілі зазнали певних змін. Доктрина була спрямована на забезпечення військової безпеки росії та підкреслювала важливість захисту національних інтересів та етнічних росіян.

Порівняно з 1993 роком, у доктрині 2000 року відбулися зміни в ролі та умовах застосування ядерної зброї. Допускалося перше застосування ядерної зброї у відповідь на великомасштабну агресію із застосуванням звичайних озброєнь при загрозі національній безпеці. Поріг її застосування був знижений порівняно з позицією 1993 року, що відображало побоювання мінливого характеру можливих конфліктів.

Принципи застосування військової сили також еволюціонували. Доктрина передбачала застосування сили проти незаконних збройних формувань усередині росії та підкреслювала необхідність всебічної оцінки військово-політичної обстановки. Згідно з положеннями доктрини, прийнятої у 2000 році, яка вважала дискримінацію та позбавлення прав громадян росії загрозою для всієї держави, у 2008 році було проведено військову операцію в Грузії, обґрунтовану необхідністю захисту громадян російської федерації та етнічних росіян. Ця операція була добре спланована, а підрозділи — підготовлені для бойових дій у кавказькій гірській місцевості. Стратегія росії в цій війні була продиктована насамперед домінуванням у кількості та якості військ і техніки, а також висновками, зробленими з війни в Чечні. Ефективність скоординованих атак за участю різних родів військ дозволила домінувати в цій війні та успішно її завершити протягом п’яти днів [26].

Військова доктрина 2010 року: відповідь на розширення НАТО

Після завершення Другої війни в Чечні та війни в Грузії у 2010 році відбулися чергові зміни воєнної доктрини російської федерації. Першою значною відмінністю стало конкретне визначення НАТО та його розширення новими державами-членами як потенційної зовнішньої небезпеки для російської федерації [27-28]. Внутрішні військові небезпеки включали спроби насильницької зміни конституційного ладу та дезорганізацію функціонування державних органів. Військові загрози охоплювали різке загострення військово-політичної обстановки та перешкоджання роботі систем державного управління. Сучасні конфлікти характеризувалися комплексним застосуванням військової сили та невійськових засобів, зокрема інформаційної війни. Визнання характеристик “гібридної війни” стало важливою еволюцією в оцінці сучасних збройних протистоянь.

Ядерна складова доктрини також зазнала змін: було підвищено поріг застосування ядерної зброї. Відтепер її можна було застосовувати лише у разі загрози самому існуванню держави, що було суворішим критерієм, ніж “критичні ситуації” у 2000 році. Попри це, доктрина, як і раніше, передбачала можливість першого застосування у випадку екзистенційних загроз та інтегрувала звичайні високоточні озброєння в стратегію стримування, що свідчило про складне розуміння ролі ядерної зброї.

Принципи застосування військової сили були адаптовані з урахуванням концепції неядерного стримування. Було остаточно визначена обґрунтованість застосування збройних сил для захисту громадян за кордоном та підкреслено розвиток неядерного стримування. Доктрина чітко визнала зростаючу важливість невійськових інструментів і необхідність комплексного підходу до безпеки, що виходить за рамки суто військового аспекту.

Військова доктрина 2014 року: зміни у світовій архітектурі небезпеки

Наступну доктрину було прийнято у 2014 році, невдовзі після подій, що суттєво вплинули на міжнародну безпекову ситуацію. Вона ознаменувала значне посилення позиції росії щодо Заходу, особливо до НАТО, яке розглядалося лише як потенційний партнер для "рівноправного діалогу".

Військова доктрина 2014 року зазначала, що значна кількість конфліктів у світі залишаються невирішеними, а такий стан часто призводить до їхнього остаточного врегулювання військовим шляхом. Підкреслювалося, що чинна на той час архітектура безпеки у світі не забезпечує однакового рівня безпеки для всіх держав. До переліку зовнішніх небезпек, зазначених у доктрині 2010 року, було додано встановлення політичних режимів ворожих до росії на території сусідніх з нею держав, особливо якщо вони були встановлені шляхом повалення законно правлячого уряду. Найімовірніше, це пов'язано із ситуацією в Україні, де за кілька місяців до цього було встановлено уряд, який росія не визнавала [29].

Військові небезпеки було розширено включенням "інформаційного простору та внутрішньої сфери". Вперше як військова небезпека згадувалася концепція "миттєвого глобального удару".

Стратегічні цілі змістилися в бік посилення впливу росії у "ближньому зарубіжжі" та протидії загрозам стабільності союзних режимів. Пріоритетне значення надавалося співробітництву з Шанхайською організацією співробітництва (ШОС) та Організацією Договору про колективну безпеку (ОДКБ). Було заявлено за мету проведення регіональної оборонної політики для забезпечення безпеки кордонів від потенційних загроз.

Хоча умови застосування ядерної зброї залишилися незмінними, посилення акценту на неядерному стримуванні вказувало на потенційний довгостроковий зсув у бік переважного використання звичайних високоточних озброєнь.

Принципи застосування військової сили еволюціонували з урахуванням аспектів гібридної війни. Підкреслювалося, що росія вдаватиметься до військових засобів лише після вичерпання некінетичних засобів. Доктрина 2014 року формально визнала важливість невійськових інструментів сили та потенціал гібридної війни, що відображало уроки нещодавніх конфліктів та еволюцію стратегічного мислення.

Аналіз військових доктрин пострадянської росії демонструє значні трансформації, зумовлені змінами геополітичної обстановки та внутрішніх пріоритетів країни. Спостерігається послідовне розширення спектра сприйнятих загроз, зміщення стратегічних цілей від оборонних до більш агресивних, а також зміна поглядів на роль ядерної зброї та принципи застосування військової сили (табл. 1).

Таблиця 1

Ключові відмінності у військових доктринах російської федерації (1993-2014)

Характеристика	1993	2000	2010	2014
Сприйняття загроз	регіональні конфлікти; внутрішня нестабільність	тероризм; послаблення міжнародних механізмів безпеки	НАТО; внутрішні політичні загрози; гібридна війна	внутрішні загрози; інформаційна війна; НАТО; зміна режимів у сусідніх країнах

Продовження табл. 1

Характеристика	1993	2000	2010	2014
Стратегічні цілі	пострадянська адаптація; стабільність у ближньому зарубіжжі	утвердження регіонального впливу; захист національних інтересів	підтримання балансу сил; розвиток неядерного стримування; внутрішня стабільність	консолідація сфери впливу; протидія загрозам союзним режимам; посилення неядерного стримування
Ядерна зброя	відмова від незастосування першим; стримування агресії	перше застосування у відповідь на загрози національній безпеці; стримування регіональних воєн	підвищення порогу (екзистенційна загроза); інтеграція звичайних високоточних озброєнь у стримування	продовження акценту на ядерному стримуванні; посилення неядерного стримування
Застосування сили	регіональні конфлікти; внутрішня стабільність; швидке розгортання	включення внутрішніх загроз; ретельна оцінка перед застосуванням сили	захист громадян за кордоном; розвиток неядерного стримування	пріоритезація некінетичних засобів; визнання гібридної війни; занепокоєння військовою активністю в сусідніх країнах

Джерело: розроблено авторами.

3. Концепції війн генерала Герасимова

Розглянуті військові доктрини росії були доповнені окремими концепціями ведення війни, сформульовані начальником ГШ ВС рф генералом Валерієм Герасимовим. У січні 2013 року генерал Валерій Герасимов, призначений на посаду за кілька місяців до того, оприлюднив свою доповідь “Основные тенденции развития форм и способов применения ВС, актуальные задачи военной науки по их совершенствованию” на засіданні Академії військових наук росії. В основі запропонованої ним концепції війни було адаптивне використання військової сили в умовах “стирання відмінностей між станом війни та миру, коли війни вже не оголошуються, а розпочавшись – йдуть за незвичним шаблоном”. Акцептувалась роль невійськових способів у досягненні політичних та стратегічних цілей, які в окремих випадках за своєю ефективністю можуть значно перевершувати силу зброї. До невійськових засобів було віднесено формування та підтримку політичної опозиції, економічні санкції та ембарго, політичний та дипломатичний тиск та, як наслідок, зміну уряду. Відкрите застосування військової сили розглядалось лише на певному етапі, переважно для досягнення остаточного успіху у конфлікті. Водночас генерал Герасимов підкреслював, що “кожен конфлікт є унікальним, і не завжди можливо застосовувати цю схему” (рис. 1) [30].

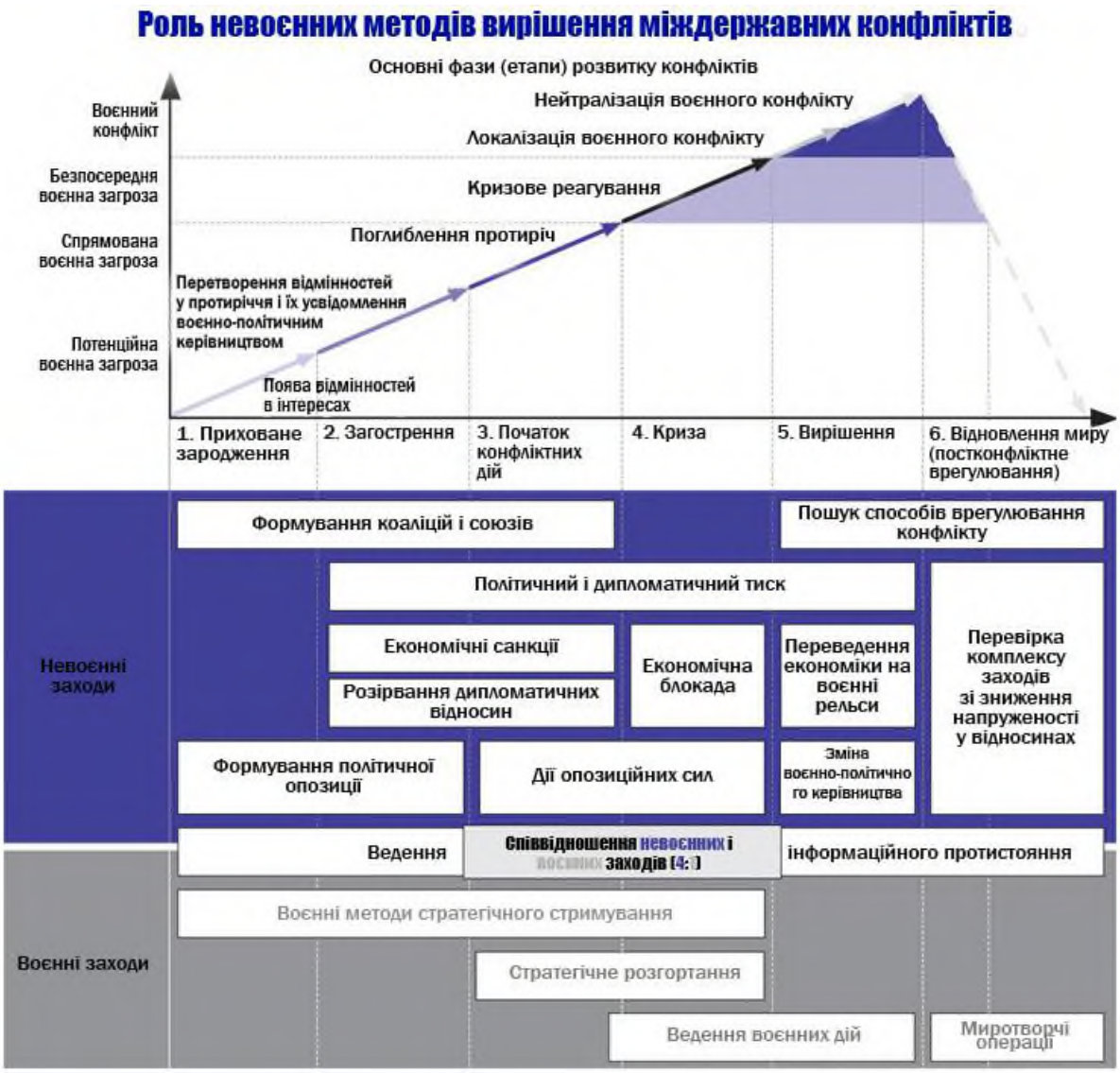


Рис.1. Роль невійськових методів під час вирішення міждержавних конфліктів
Джерело: [30]

Він представив також новий підхід до безпосереднього ведення війни, де найважливішими аспектами мали бути:

– бойові дії, що уникають безпосереднього контакту завдяки високій мобільності підрозділів;

– зменшення економічного потенціалу держави через атаки на критичну інфраструктуру;

– масове використання високоточної зброї, безпілотників, спеціальних підрозділів та повстанських формувань;

– атаки, що проводяться на території всієї держави, а не лише на лінії зіткнення;

– ведення інформаційної війни.

– Частиною західного світу це сприймалося як певна схема відносно нової концепції гібридної війни, згідно з якою росія мала проводити свою кампанію в Україні, захоплюючи за допомогою неозначених солдатів Крим та дестабілізуючи Донбас.

На початку 2019 року Валерій Герасимов оголосив нову, змінену концепцію війни [31]. Обговорюючи сучасні війни, Герасимов звернув увагу на необхідність активного використання потенціалу “п’ятої колони” для дестабілізації ситуації разом з одночасними ударами з повітря по найважливіших об’єктах. Нову стратегію росії він назвав “стратегією

активної оборони". Вона передбачає одночасне та комплексне використання політичних, економічних, інформаційних та інших невоєнних інструментів. Але найважливішим є відповідна підготовка та застосування збройних сил. Решта, невійськові інструменти, лише створюють умови для застосування військових сил і мають вплив на перебіг війни. Кожен з цих інструментів має свою окрему стратегію. Важливою є їхня відповідна координація та керування всіма цими інструментами. Стратегії повинні передбачати майбутній характер воєн, майбутні дії та їхні наслідки.

Однак нова концепція вже не передбачала боротьби "за душі" та не підкреслювала значення психологічних дій, як це було у виступі Герасимова у 2013 році. Тепер пріоритетом визначалися сучасні технології та новітні озброєння. Цифрові технології, роботизація, безпілотні системи та радіоелектронна боротьба ставали головною метою розвитку російських збройних сил. Щодо способу ведення бойових дій, на перший план висувалося ведення війни поза межами власної держави в рамках стратегії обмежених дій. Її основою було створення самостійно діючих військових угруповань (тактичних груп) з високою мобільністю та можливостями виконання найскладніших завдань [31].

4. Воєнні стратегії росії, використані в повномасштабній війні проти України

Війна в Україні розпочалася ще у 2014 році із захоплення Кримського півострова так званими "зеленими чоловічками", які фактично були російськими військовослужбовцями, та захоплення контролю над частиною Донбасу сепаратистськими силами, підтримуваними Москвою. Росія скористалася тимчасовою слабкістю України та хаосом, спричиненим Революцією Гідності, відстороненням президента Януковича й кардинальними змінами в критичних інституціях, щоб зайняти територію Криму "без пострілу" та підтримувати так звані "сепаратистські республіки" Донецька та Луганська. Відкритий конфлікт частково заморозився у 2015 році, а росія продовжила гібридну війну проти України, яка тривала аж до 24 лютого 2022 року.

Майже повна реалізація оголошеної у 2019 році Герасимовим концепції відбулася 24 лютого 2022 року, коли росія завдала удару з чотирьох напрямків. Головним напрямком атаки був центр країни, який атакували з півночі, з території Білорусі, а метою було захоплення Києва, усунення чинного уряду та встановлення нового, прихильного до співпраці з росією. Окрім колон армії, що вже на другий день дійшли до околиць столиці, допоміжними діями мали стати десанти на аеропорти в Гостомелі та Борисполі. План передбачав забезпечення місця для посадки транспортних літаків Іл-76 підрозділами повітряно-десантних військ, які вже використовувалися для подібних операцій в Афганістані, та безпосередню доставку військ і техніки на аеродроми, розташовані приблизно за 30 кілометрів від Києва. Спроби десанту на аеродром у Гостомелі були швидко знівельовані, і вже наприкінці першого дня Україна встановила над ним контроль. Атаки на Київ та Гостомель супроводжувалися ударами в бік Харкова з Бєлгорода, у напрямку Запоріжжя та Маріуполя з Донецька, а також в бік Херсона та Мелітополя з Кримського півострова. Вже за кілька днів росіяни взяли в оточення або напівоточення найважливіші міські центри регіонів: Київ, Чернігів, Суми, Харків, Маріуполь, Херсон та Миколаїв. За задумом, через оточення планувалося створення "котлів", у яких війська, що обороняли міста, регулярно обстрілювалися б артилерією, а шляхи постачання блокувалися б, як це сталося під час облоги Грозного в 1999 році. Завдяки цьому виснажені війська мали здаватися або вести відчайдушну оборону, яка б незначною мірою могла загрожувати російським підрозділам. Така тактика дозволила захопити Мелітополь і Херсон, а після понад двомісячної облоги — Маріуполь. Аналогічно діяли й на наступних етапах війни, захоплюючи Сєвєродонецьк, Лисичанськ та Бахмут. Паралельно росіяни завдавали ракетних ударів по важливих об'єктах військової інфраструктури по всій території України, намагаючись послабити таким чином потенціал української армії та змусити українців розсіювати сили, які повинні бути готові до оборони та посиленого захисту об'єктів у різних

частинах держави. Однак, попри окремі успіхи, на початковому етапі війни 2022 року росія зазнала поразки.

Причин цієї поразки було щонайменше кілька. Першою стало недооцінення потенціалу та залученості Збройних Сил України, а також спротиву українського народу військовим діям, диктованим росією, подібно до того, як російські війська зустрічали опір у Фінляндії, Афганістані чи Чечні. Планована блискавична війна не вдалася через запеклий опір та переконання українського суспільства в необхідності тотальної оборони. Розраховуючи на швидке захоплення влади, росіяни не повною мірою використали потенціал артилерії, що значно обмежило їхні наступальні можливості. Другою помилкою була відсутність встановлення повної переваги в повітрі. Хоча росія мала значну перевагу за кількістю літаків і вертольотів, однак широке застосування систем протиповітряної оборони, а також відносно дешевих переносних зенітних ракетних комплексів Україною та значні втрати в бойових вертольотах обмежили використання російської авіації. Відсутність взаємодії між підрозділами авіації та наземними військами призвела до провалу доктрини, заснованої на одночасному застосуванні різних родів військ. Третьою помилкою стала слабка координація дій і надмірне розосередження батальйонних тактичних груп. Вразливі до українських атак малими мобільними підрозділами, вони досягали своїх цілей лише зі значними втратами. Багатокілометрові колони з постачанням були слабо захищені й ставали легкою ціллю, а за кілька днів повністю були зупинені. Через це війська, що оточували різні міста України, мали дуже обмежені можливості та, подібно до підрозділів СРСР під час фінської Зимової війни, були змушені відступити з-під Києва, Чернігова, Сум і частково Харкова. Четвертою помилкою росіян було недооцінення міжнародної підтримки України, особливо з боку держав-членів НАТО. Також вчинення жорстоких злочинів проти цивільного населення у Бучі та Ірпені призвело до ще активнішого залучення суспільств західних країн до допомоги Україні й посилило тиск на міжнародну спільноту.

Під кінець літа 2022 року російські війська втратили близько 15 000 солдатів, що відповідає втратам, яких СРСР зазнав за 10 років війни в Афганістані [32]. Це обумовило зміни в тактиці росії, яка зосередила основні зусилля на розширення окупованих територій. Після поразки під Києвом росіяни розпочали будівництво укріплень уздовж усієї лінії фронту і підготовку до можливого контрнаступу українських військ. Водночас восени 2022 року росія розпочала кампанію ракетних і дронових атак, спрямованих переважно на знищення української критичної інфраструктури. При цьому вона використала слабкість української протиповітряної оборони, що базувалася переважно на радянській техніці з майже вичерпаними на той час запасами зенітних ракет. Унаслідок цих атак були знищені електростанції, нафтопереробні заводи, нафтобази, теплоцентралі, об’єкти водної інфраструктури, склади з продовольством, переважно зерном. Це суттєво вплинуло на цивільне населення, яке зіткнулося з нестачею електроенергії та перебоями в теплопостачанні. У відповідь на ці атаки західні держави збільшили постачання систем протиповітряної оборони та боєприпасів до них.

У 2023 році відбувся перехід росії до оборонної війни, яка полягала в організації міцної позиційної оборони з епізодичними контрударами. Затримка поставок Україні далекобійних ракет і танків дозволила росії здійснити перегрупування та зміцнити оборону після її прориву на півдні Харківської області та на півночі Херсонської. Готуючись до українського контрнаступу, росіяни збудували укріплення, відомі як “лінія Суровікіна”. До їхнього складу входили мінні поля, протитанкові загородження та системи окопів. Щоб знищити наступальний потенціал українців, російські війська почали масово використовувати дрони-камікадзе “Ланцет”, квадрокоптери, оснащені різними видами гранат, та здійснювати регулярні артилерійські обстріли. В рамках контрударів використовувалися танки, броньовані бойові машини, що діяли за підтримки артилерії та авіації. Масштабне використання дронів кардинально змінило характер бойових дій.

Водночас застосування засобів РЕБ знизило ефективність застосування високоточних боєприпасів, наданих Україні США. У своєму аналізі війни в листопаді 2023 року Головнокомандувач Збройних Сил України генерал Валерій Залужний зазначив, що "Україна за п'ять місяців свого контрнаступу змогла просунутися лише на 17 кілометрів. Як і в Першій світовій війні, ми досягли такого рівня технологій, який заводить нас у глухий кут. Для виходу з цієї патової ситуації потрібен значний технологічний стрибок" [33].

З 2024 року війна набула характеру виснаження, де обидві сторони прагнуть підірвати ресурси та боєздатність одна одної протягом тривалого часу. При цьому, російська армія використовує комбіновану тактику, спрямовану на змушення українських сил відступати. Вона полягає в поєднанні масованого використання безпілотників для виявлення цілей із подальшим застосуванням потужних керованих авіаційних бомб та артилерії для підготовки наступу піхоті. Кожен елемент атаки підтримує інші, що відбуваються одночасно або хвилями, створюючи кумулятивний ефект, який чинить значний тиск на українських військових. У свою чергу, Україна також активно розвинула власні безпілотні та роботизовані системи, досягла значних успіхів у сфері радіоелектронної боротьби, що дозволило проводити операції глибокого ураження на території противника. Сучасні безпілотні технології та радіоелектронна боротьба стали ключовими елементами бойових дій, забезпечуючи перевагу в розвідці, завданні ударів і протидії для обох сторін. Таким чином російсько-українська війна повністю змінила характер сучасної війни, поставивши можливість досягнення перемоги в пряму залежність від розвитку нових технологій та їхнього впровадження.

Висновки

Російська військова доктрина пройшла значну еволюцію від початку XX століття, адаптуючись до змін геополітичної обстановки та досвіду військових конфліктів. Незважаючи на це, ключові риси російських військових дій залишаються незмінними: обґрунтування агресії, готовність до великих людських втрат та скоєння воєнних злочинів.

Після розпаду СРСР російські військові доктрини поступово зміщувалися від оборонної спрямованості до більш агресивної, розширюючи спектр загроз і змінюючи погляди на застосування військової сили. На перших етапах повномасштабного вторгнення в Україну російська федерація реалізовувала прийняту військову доктрину 2014 року та концепцію генерала Герасимова із застосуванням невійськових засобів та швидких, рішучих дій. Проте невдачі першого року війни, зумовлені низкою факторів, змусили росію змінити тактику і форми бойового застосування військ росії.

Сучасні безпілотні технології та засоби радіоелектронної боротьби стали ключовими елементами бойових дій, забезпечуючи перевагу в розвідці, завданні ударів та протидії для обох сторін. Таким чином, російсько-українська війна повністю змінила характер сучасної війни, поставивши можливість досягнення перемоги в пряму залежність від розвитку нових технологій та їхнього впровадження.

Список літератури

1. Nawrocki K. Agresja 17 września 1939 r. – historyczne kłamstwo bieżącej polityki Kremla. *Instytut Pamięci Narodowej*. URL: https://ipn.gov.pl/pl/aktualnosci/150154,Agresja-17-wrzesnia-1939-r-historyczne-klamstwo-biezacej-polityki-Kremla-Prezes-.html (accessed 10.05.2025).
2. Guardian News. Russia-Ukraine crisis: Putin orders military operation in Ukraine. *YouTube*. URL: https://www.youtube.com/watch?v=asuhx16wlWo (accessed 10.05.2025).
3. Kujala A. Illegal Killing of Soviet Prisoners of War by Finns during the Finno-Soviet Continuation War of 1941-44. *The Slavonic and East European Review*. 2009. № 87 (3). P. 429-451. URL: http://www.jstor.org/stable/40650407.

4. Magula J. Exploring factors and implications of violence against civilians: a case study of the Soviet-Afghan war. *Small Wars & Insurgencies*. 2023. Vol. 34. № 7. P. 1295-1321. URL: https://doi.org/10.1080/09592318.2023.2231198.
5. Memorandum on Accountability for Humanitarian Law Violations in Chechnya. *Human Rights Watch*. URL: https://www.hrw.org/news/2000/09/12/memorandum-accountability-humanitarian-law-violations-chechnya (accessed 10.05.2025).
6. SNHR's Ninth Annual Report on the Most Notable Violations by Russian Forces Since the Launch of Russia's Military Intervention in Syria on September 30, 2015. *Syrian Network for Human Rights*. URL: https://snhr.org/blog/2024/09/30/snhrs-ninth-annual-report-on-the-most-notable-violations-by-russian-forces-since-the-launch-of-russias-military-intervention-in-syria-on-september-30-2015/.
7. Kurczab J. Zbrodnia katyńska jako ludobójstwo. Próba systematyzacji kwalifikacji prawnokarnej. *Dzieje Najnowsze*. 2017. Vol. 49. № 3. P. 27–47. URL: https://doi.org/10.12775/DN.2017.3.02.
8. Renic N. The Cost of Atrocity: Strategic Implications of Russian Battlefield Misconduct in Ukraine. *Ethics & International Affairs*. 2024. № 38 (1). P. 6-16. URL: https://doi.org/10.1017/S0892679424000054.
9. Залужний В. Нова природа війни змінила сутність основ глобальної безпеки: український досвід і майбутній світовий порядок. *Українська правда*. URL: https://www.pravda.com.ua/columns/2025/04/25/7509135/ (дата звернення: 10.05.2025).
10. Persson G. Learning from Foreign Wars: Russian Military Thinking. Solihull: Helion and Company, 2013. 184 p.
11. Adamsky D., Vadis Q. Russian Deterrence? Strategic Culture and Coercion Innovations. *International Security*. 2025. № 49 (3). P. 50-83. URL: https://doi.org/10.1162/isec_a_00502.
12. Luzin P., Roshchin E. Russia's Strategy and Military Thinking: Evolving Discourse by 2025. *Center for European Policy Analysis (CEPA)*. URL: https://cepa.org/comprehensive-reports/russias-strategy-and-military-thinking-evolving-discourse-by-2025/ (accessed 10.05.2025).
13. Zieliński W. Rosja – strategia imperium. Ante Portas. *Studia nad Bezpieczeństwem*. 2016. № 1 (6). P. 349-366.
14. Surowiec K., Razin A. Założenia geopolityki Iwana IV Groźnego i jej realizacja w Rosji w latach 1547-1584. *Humanities and Social Sciences*. 2016. № 21 (1). P. 153-165.
15. Dimitrov A., Durev G. Peter I and the Birth of the Russian Empire: Political Leadership and Military Successes in Comparative Perspective. *Vestnik MGIMO-Universiteta*. 2021. № 6 (81). P. 71-88. https://doi.org/10.24833/2071-8160-2021-6-81-71-88.
16. Grzelak C. Armia Czerwona po wojnie polsko-rosyjskiej 1919–1921 roku. *Studia z Dziejów Wojskowości*. 2014. №. 3. P. 255-265.
17. Kontrofensywa bolszewicka 1920 roku. *Dzieje.pl*. URL: https://dzieje.pl/aktualnosci/kontrofensywa-bolszewicka-1920-roku (accessed 10.05.2025).
18. Thompson C. E. Miracle on the Vistula: The Red Army's Failure and the Birth of the Deep Operations Theory of Annihilation. *Defense Technical Information Center*. URL: https://archive.org/details/DTI_AD1039948 (accessed 12.10.2023).
19. Ziemke E. F. The Soviet Theory of Deep Operations. *Parameters*. 1983. № 13(1). P. 24-32. URL: https://doi.org/10.55540/0031-1723.1339.
20. Grau L. W., Gress M. A. The Soviet-Afghan War: How a Superpower Fought and Lost. Lawrence, KS: University Press of Kansas, 2002. 417 p.
21. Grau L. W. The Bear Went Over the Mountain: Soviet Combat Tactics in Afghanistan. Washington, D.C.: National Defense University Press, 1996. 223 p.
22. Arbatov A. The Transformation of Russian Military Doctrine: Lessons Learned from Kosovo and Chechnya. Marshall Center Papers. George C. Marshall European Center for Security Studies, 2000. 38 p.
23. Bakshi J. Russia's National Security Concepts and Military Doctrines: Continuity and Change. *Strategic Analysis*. 2000. Vol. 26. № 7. URL: https://ciaotest.cc.columbia.edu/olj/sa/sa_oct00baj01.html (accessed 10.05.2025).
24. The Basic Provisions of the Military Doctrine of the Russian Federation. *Federation of American Scientists*. URL: https://nuke.fas.org/guide/russia/doctrine/russia-mil-doc.html (accessed 10.05.2025).
25. Russia's Military Doctrine. *Arms Control Association*. URL: https://www.armscontrol.org/act/2000-05/russias-military-doctrine (accessed 10.05.2025).
26. Cohen A., Hamilton R. E. The Russian Military and the Georgia War: Lessons and Implications. *U.S. Army War College Press*. URL: https://press.armywarcollege.edu/monographs/576/ (accessed 10.05.2025).
27. Tsypkin M. What's New In Russia's New Military Doctrine? *Radio Free Europe/Radio Liberty*. URL: https://www.rferl.org/a/Whats_New_In_Russias_New_Military_Doctrine/1970150.html.
28. Российская Федерация. Военная доктрина Российской Федерации: утверждена Указом Президента Российской Федерации от 5 февраля 2010 г. № 146. *Российская газета*. 2010. URL: https://rg.ru/documents/2010/02/10/doktrina-dok.html (дата обращения: 10.05.2025).
29. Российская Федерация. Военная доктрина Российской Федерации: утверждена Указом Президента Российской Федерации от 25 декабря 2014 г. № Пр-2976 *Российская газета*. 2014. URL: https://rg.ru/documents/2014/12/30/doktrina-dok.html (дата обращения:10.05.2025).

30. Ценность науки в предвидении. *ВПК*. URL: https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html (дата обращения:12.05.2025).
31. Фельгенгауэр П. Добиться превосходства над остальным человечеством. *Новая газета*. URL: https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya-prevoshodstva-nad-ostalnym-chelovechestvom (дата обращения:12.05.2025).
32. Harris S., Duplain J. Russia to "run out of steam" soon in Ukraine: U.K. intelligence chief. *The Washington Post*. 2022. URL: https://www.washingtonpost.com/world/2022/07/22/russia-ukraine-mi6-intelligence-pause/ (accessed 12.05.2025).
33. Zaluzhny V. Ukraine's commander-in-chief on the breakthrough he needs to beat Russia. *The Economist*. 2023. URL: https://www.economist.com/europe/2023/11/01/ukraines-commander-in-chief-on-the-breakthrough-he-needs-to-beat-russia (accessed 12.05.2025).

НАУКОВЕ ВИДАННЯ

MILITARY STRATEGY AND TECHNOLOGY

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

№ 2(2) / 2025

Відповідальний за випуск *І.В. Івженко*

Ідентифікатор медіа R40-05944 згідно з рішенням Національної ради України з питань телебачення і радіомовлення від 10.04.2025 № 804

Засновник і видавець: Громадська організація "Центр воєнної стратегії і технологій"
Адреса: вул. Саксаганського, буд.41, місто Київ, 01033, Україна
Телефон: +38 (067) 42-61-105
E-mail редколегії: technical.sciences2025@gmail.com