



ISSN 2522-9842 (online)



Public organization
Ukrainian Scientific Community

Journal of Scientific Papers
**Social Development and
Security**

Volume 15, Issue 4, August, 2025



<https://paperssds.eu/index.php/JSPSDS/>



EDITORIAL BOARD**Chairman of Editorial Board:**

Volodymyr **Mirnenko**, Dr.Sc. (Technical), Prof, Ukraine.

Deputy Chairman of the Editorial Board:

Ivan **Tkach**, Dr.Sc. (Economics), Prof., Ukraine.

Technical Secretary, Member of the Editorial Board:

Mykola **Tkach**, Dr.Sc. Assoc. Prof., (Economics), Ukraine.

Members of the Editorial Board:

Victor **Antonyuk**, Dr.Sc. (Technical), Prof., Ukraine.
 Anatoly **Ballanda**, Dr.Sc. (Economics), Prof., Ukraine.
 Oleg **Barabash**, Dr.Sc. (Technical), Prof., Ukraine.
 Miroslaw **Banasik**, PhD, Assoc. Prof., Poland.
 Vitaliy **Begma**, Dr.Sc. (Economics), Prof., Ukraine.
 Vasyl **Bichenkov**, Dr.Sc. (Technical), Senior Researcher, Ukraine.
 Svitlana **Bondarenko**, Dr.Sc. (Economics), Prof., Ukraine.
 Igor **Britchenko**, Dr.Sc. (Economics), Prof., Poland.
 Vitaliy **Chorny**, Dr. of Philosophy, Prof, Ukraine.
 Pavel **Cubichek**, Dr. Sc. (Physical and Mathematical), Prof., Ukraine.
 Mikhail **Divizynuk**, Dr. Sc. (Physical and Mathematical), Prof., Ukraine.
 Darma **Dio Caisar**, Assist. Prof., Indonesia.
 Petr **Dikhtievsky**, Dr. of Law, Prof, Ukraine.
 Bogdan **Dolnytsky**, Dr. of Law, Prof, Poland.
 Larysa **Ivanchenkova**, Dr.Sc. (Economics), Assoc. Prof., Ukraine.
 Ross **Fetterly**, Dr.Sc., Canada.
 Piotr **Gawliczek**, PhD, Assist. Prof., Poland.
 Wojciech **Guzewicz**, PhD, Rev. Prof., Poland.
 Volodymyr **Kirylenko**, Dr.Sc. (Economics), Prof., Ukraine.
 Anatoly **Kolodiy**, Dr. of Law, Prof, Ukraine.
 Maksym **Korobchynskyi**, Dr. Sc. (Technical), Prof., Ukraine.
 Igor **Koropatnik**, Dr. of Law, Assoc. Prof, Ukraine.
 Timur **Kurseitov**, Dr. Sc. (Technical), Prof, Ukraine.
 Ribeiro **Luís Frólen**, Dr. in Mechanical Engineering, Portugal.
 Pavlo **Openko**, Candidate of Technical Sc., senior researcher, Ukraine.
 Michael J. **McCarthy**, USA.
 Oleksander **Matsko**, Candidate of Military Sciences, Prof., Ukraine.
 Jacek **Mrozek**, Ph.D, Poland.
 Volodymyr **Pashynsky**, Dr. of Law, Assoc. Prof, Ukraine.
 Artak **Sagradian**, Dr. Sc. (Technical), Prof, Armenia.
 Andre **Samberg**, Professor of Practice, PhD (civil protection), Belgium.
 Volodymyr **Shemayev**, Dr. Sc. (Military), Prof, Ukraine.
 Lyudmila **Shemayeva**, Dr.Sc. (Economics), Prof., Ukraine.
 Iryna **Shopina**, Dr. of Laws, Prof., Ukraine.
 Steven **Silverstein**, USA.
 Oleg **Vorobiov**, Dr. Sc. (Technical), Prof, Ukraine.
 Antonina **Voloshenko**, Dr.Sc. (Economics), Assoc. Prof., Ukraine.

РЕДАКЦІЙНА КОЛЕГІЯ**Голова редакційної колегії:**

Мірненко Володимир, д-р тех. наук, професор, Україна.

Заступники голови редакційної колегії:

Ткач Іван, д-р екон. наук, професор, Україна.

Технічний секретар, член редакційної колегії:

Ткач Микола, д-р екон. доц., наук, Україна.

Члени редакційної колегії:

Антонюк Віктор, д-р тех. наук, професор, Україна.
 Баланда Анатолій, д-р екон. наук, професор, Україна.
 Барабаш Олег, д-р тех. наук, професор, Україна.
 Банасик Мирослав, PhD, доц., Польща.
 Бегма Віталій, д-р екон. наук, професор, Україна.
 Биченков Василь, д-р тех. наук, с.н.с., Україна.
 Бондаренко Світлана, д-р екон. наук, професор, Україна.
 Брітченко Ігор, д-р екон. наук, професор, Польща.
 Чорний Віталій, д-р філ. наук, професор, Україна.
 Кубічек Павел, д-р права, професор, Словацька Республіка.
 Дівізінюк Михайло, д-р фіз-мат. наук, професор, Україна.
 Діо Кайсар Дарма, асистент професор, Індонезія.
 Діхтієвський Петро, д-р юр.наук, професор, Україна.
 Долницький Богдан, д-р юр.наук, професор, Польща.
 Іванченкова Лариса, д-р екон. наук, доцент, Україна.
 Феттерлі Росс, д-р наук, ад'юнкт-професор, Канада.
 Гавлічек Петро, PhD, доцент, Польща.
 Гузевич Войцех, PhD, професор, Польща.
 Кириленко Володимир, д-р екон. наук, професор, Україна.
 Колодій Анатолій, д-р юр.наук, професор, Україна.
 Коробчинський Максим, д-р тех. наук, професор, Україна.
 Коропатнік Ігор, д-р юр.наук, доцент, Україна.
 Курсеїтов Тимур, д-р тех. наук, професор, Україна.
 Рібейро Луїс Фрелен, д-р мех. наук, Португалія.
 Опенько Павло, кандидат тех. наук, старший дослідник, Україна.
 Маккарті Майкл, США.
 Мацько Олександр, кандидат військ. наук, професор, Україна.
 Мрозек Яцек, PhD, Польща.
 Пашинський Володимир, д-р юр.наук, доцент, Україна.
 Саградян Артак, д.т.н., професор, Армения.
 Самберг Андре, д-р тех. наук, кандидат тех. наук, Бельгія.
 Шемаєв Володимир, д-р військ. наук, професор, Україна.
 Шемаєва Людмила, д-р екон. наук, професор, Україна.
 Шопіна Ірина, д-р юр. наук, професор, Україна.
 Сільверштейн (Роберт) Стівен, США.
 Воробйов Олег, д-р тех. наук, професор, Україна.
 Волощенко Антоніна, д-р екон. наук, доцент, Україна.

FOUNDERS and PUBLISHER: Public Organization "Ukrainian Scientific Community" (Ukraine)

Executive secretary of the editorial board of the Journal of Scientific Papers "Social Development and Security" Mykola Tkach,

e-mail: tim68@ukr.net; tkachivan9@gmail.com

<https://paperssds.eu/index.php/JSPSDS/>, тел. +38(093) 752-81-56

The authors of articles are responsible for the authenticity of facts, quotes, their own names, geographical names, names of enterprises, organizations, institutions and other information. Opinions expressed in these articles may not coincide with the point of view of the editorial board and do not impose any obligations on it.

TABLE OF CONTENTS

National Security	
The Socioeconomic Impact of the Zangezur Corridor on the South Caucasus Region <i>Elshan Hashimov, Aziz Talibov, Khayal Iskandarov</i>	1
Military Operations for Law Enforcement. Joint Operation of the Army Special Forces Command and the Police during the Nemangkawi Operation in Papua 2018 <i>Mhd Halkis, Ida Bagus, Y.S.</i>	19
Mathematical Model of Maximizing the Value of the Integral Index of State Border Security <i>Vladyslav Shevchuk</i>	29
Key Steps of Ukraine in the Military and National Security System to Increase Cognitive Resilience (2025-2028): Recommendations in the Cognitive and Military-Economic Spheres <i>Oleh Semenenko, Oleksandr Kin, Liliia Semenenko, Volodymyr Remez, Serhii Mytchenko, Dmytro Rybak</i>	36
Ukrainian Security Diplomacy in the New Geopolitical Reality: Security Guarantees for Ukraine, Risks and Challenges <i>Volodymyr Gurkovskyi, Ivan Havryliuk, Yurii Kliat, Yuzef Dobrovolskyi, Evgen Romanenko, Serhii Ilnitskyi</i>	50
The Generational Division of Warfare and Controversial Issues <i>Zafar Nuri Najafov</i>	62
Military Security	
New Approaches in Military Personnel Training: A Pedagogical Evaluation of Teaching Methods <i>Mujkan Mammadzada</i>	72
Development of Evaluation Models for Surface-to-Air Missile Firing Effectiveness with Consideration of Air Target Kill Probabilities <i>Pavlo Openko, Oleksandr Piavchuk, Yurii Tselishev, Viktor Kudriashov, Oleksii Kolomiitsev, Valerii Voinov</i>	79
Forming a Regulatory Model of the Life Cycle for Military Ground Robotic Systems <i>Andrii Diadechko, Vitalii Zuiko</i>	95
Civil Security	
The The Features of Students' Awareness of Modern Road Safety Issues <i>Solomiya Pysarevska, Viktoriya Vashchuk, Zinoviy Yaremko</i>	106
Concepts of Occupational Protection, Occupational Safety and Health and Well-Being of Employees at Work <i>Vitaly Tsopa, Serhii Cheberyachko, Olena Sharovatova, Oleg Deryugin, Kyrylo Lapko</i>	116
Engineering and Technology	
Application of Neural Networks for Selecting Tools for Penetration Testing <i>Andriian Piskozub, Anastasiia Zhuravchak, Danyil Zhuravchak, Yurii Zhuravchak, Igor Beliaiev</i>	126
Selection of Organizational Forms for Metrological Support of Digital IT Projects <i>Vitalii Yarovyi, Oksana Andriienko, Viktor Hudyma</i>	133

A Framework to Secure Business Assets Against Social Engineering Attacks in State Corporations in Kenya <i>John Maiyo, Satwinder Singh Rupra, Daniel Otanga</i>	143
Protective Layered Model of a Multi-Component Architectural-Composite Structure of an Optoelectronic Information Leakage Channel <i>Nazarii Dzyany</i>	155
Automated System for Recognizing Air Targets Using Convolutional Neural Networks <i>Oleg Lavrov, Andrii Lavrov</i>	167
Social Sciences	
Organizational and Legal Principles of Accounting for Military Expenditures and Losses <i>Artem Filippov, Zlatina Marchuk</i>	179
The State of Russia's Economic Development in the Context of Full-Scale Aggression Against Ukraine <i>Mykola Tkach, Mykola Khomik, Ivan Tkach, Tetiana Cherneha, Dmytro Drynov</i>	187
Expenditures of the Ministry of Defence of Ukraine: Analysis from the Perspective of Transformational Economic Prospects <i>Maria Zozulinska, Oleksandr Artiushenko</i>	202
The Evolution of State Policy in Public and Defense Procurement in Ukraine: Challenges and Development Pathways <i>Olena Holota</i>	219
Storytelling in the Defense Sector <i>Kostyantyn Nizheiko, Oleksandra Lendel</i>	242
Decision Matrix as a Tool for Substantiating Options to Ensure Sufficient National Defense Capacity <i>Oleh Semenenko, Maryna Abramova, Polina Tolok, Olha Taran, Oleh Tarasov, Mariia Yarmolchuk</i>	250
Methodology for Assessing the Ability of a National Economy to Ensure Its Defense Potential: Structural and Logical Scheme and Algorithm <i>Ihor Moskalenko</i>	265
Views on the Formation of the Main Tasks and Functions of the System of Command Bodies of the Operational Group of Troops in the Armed Forces of Ukraine <i>Tymur Kurtseitov, Serhiy Baranov, Volodymyr Remez, Dmytro Rybak, Maksym Samsonenko, Yaroslav Yankovy</i>	287
Modernization of Ukraine's Defense-Industrial Complex under Wartime Challenges: Problems, Prospects, and Strategic Priorities <i>Vitalii Polovenko</i>	296
Strategic Analysis of the Transformation of Ukraine's Defense Industry Under the Influence of Military Threats and Global Technological Changes <i>Volodymyr Koval</i>	306

ЗМІСТ

Національна безпека	
Соціально-економічний вплив Зангезурського коридору на регіон Південного Кавказу <i>Ельшан Хашимов, Азіз Талібов, Хаял Іскандаров</i>	1
Військові операції з підтримання правопорядку. Спільна операція Командування сил спеціального призначення армії та поліції під час операції “Немангкаві” в Папуа, 2018 рік <i>Мухаммад Галькіс, Ida Bagus, Y.S.</i>	19
Математична модель максимізації значення інтегрального індексу безпеки державного кордону <i>Владислав Шевчук</i>	29
Ключові кроки України в системі воєнної та національної безпеки щодо підвищення когнітивної стійкості (2025-2028 рр.): рекомендації у когнітивній та воєнно-економічній сфері <i>Олег Семененко, Олександр Кінь, Лілія Семененко, Володимир Ремез, Сергій Митченко, Дмитро Рибак</i>	36
Українська дипломатія безпеки в новій геополітичній реальності: гарантії безпеки для України, ризики та виклики <i>Володимир Гурковський, Іван Гаврилюк, Юрій Клят, Юзеф Добровольський, Євген Романенко, Сергій Ільницький</i>	50
Класифікація воєн за поколіннями та дискусійні аспекти <i>Zafar Nuri Najafov</i>	62
Воєнна безпека	
Нові підходи до підготовки військових кадрів: педагогічна оцінка методів навчання <i>Mujkan Mammadzada</i>	72
Формування моделей оцінки ефективності стрільби зенітними керованими ракетами з урахуванням ймовірностей ураження повітряних цілей <i>Павло Опенько, Олександр П’явчук, Юрій Целіщев, Віктор Кудряшов, Олексій Коломійцев, Валерій Воїнов</i>	79
Формування нормативної моделі життєвого циклу військових наземних роботизованих комплексів <i>Андрій Дядечко, Віталій Зуйко</i>	95
Цивільна безпека	
Особливості усвідомлення студентами сучасних проблем безпеки дорожнього руху <i>Соломія Писаревська, Вікторія Ващук, Зіновій Яремко</i>	106
Концепції охорони праці, безпеки праці та здоров’я і благополуччя працівників на роботі <i>Віталій Цопа, Сергій Чеберячко, Олена Шароватова, Олег Дерюгін, Кирило Лапко</i>	116
Техніка і технології	
Застосування нейронних мереж для вибору інструментів для тестування на проникнення <i>Андріан Піскозуб, Анастасія Журавчак, Даниїл Журавчак, Юрій Журавчак, Ігор Беляєв</i>	126
Вибір організаційних форм метрологічного забезпечення цифрових ІТ-проектів <i>Віталій Яровий, Оксана Андрієнко, Віктор Гудима</i>	133

Рамкова модель захисту бізнес-активів від атак соціальної інженерії в державних корпораціях Кенії <i>Джон Маййоа, Сатвіндер Сінгх Рупраб, Даніел Отанґак</i>	143
Захисна пошарова модель багатокомпонентної архітектурно-компонованої структури оптоелектронного каналу витоку інформації <i>Назарій Дзяний</i>	155
Автоматизована система розпізнавання повітряних цілей за допомогою згорткових нейронних мереж <i>Олег Лавров, Андрій Лавров</i>	167
Суспільні науки	
Організаційно-правові засади обліку військових витрат та втрат <i>Артем Філіппов, Златіна Марчук</i>	179
Стан економічного розвитку росії в умовах повномасштабної агресії проти України <i>Микола Ткач, Микола Хомік, Іван Ткач, Тетяна Чернега, Дмитро Дриньов</i>	187
Видатки Міністерства оборони України: аналіз з точки зору трансформаційних економічних перспектив <i>Марія Зозулінська, Олександр Артюшенко</i>	202
Розвиток державної політики в публічних та оборонних закупівлях України: виклики та шляхи розвитку <i>Олена Голота</i>	219
Сторітелінг в оборонному секторі <i>Костянтин Ніжейко, Олександра Лендел</i>	242
Матриця прийняття рішень – як інструмент обґрунтування шляхів забезпечення необхідного рівня оборонної достатності держави <i>Олег Семененко, Марина Абрамова, Поліна Толок, Ольга Таран, Олег Тарасов, Марія Ярмольчик</i>	250
Методика оцінювання здатності національної економіки забезпечити її оборонний потенціал: структурно-логічна схема та алгоритм <i>Ігор Москаленко</i>	265
Погляди щодо формування основних завдань та функцій системи органів управління оперативного угруповання військ в Збройних Силах України <i>Тимур Куртсеїтов, Сергій Баранов, Володимир Ремез, Дмитро Рибак, Максим Самсоненко, Ярослав Янковий</i>	284
Модернізація оборонно-промислового комплексу України в умовах воєнних викликів: проблеми, перспективи та стратегічні пріоритети <i>Віталій Половенко</i>	296
Стратегічний аналіз трансформації оборонно-промислового комплексу України під впливом воєнних загроз та глобальних технологічних змін <i>Володимир Коваль</i>	306

The Socioeconomic Impact of the Zangezur Corridor on the South Caucasus Region

Соціально-економічний вплив Зангезурського коридору на регіон Південного Кавказу

Elshan Hashimov ^{A B}

Dr in National Security and Military Sciences, Professor, e-mail: hasimovel@gmail.com, ORCID: 0000-0001-8783-1277

Aziz Talibov ^B

Dr in National Security and Military Sciences, Professor, e-mail: talibovaziz65@gmail.com, ORCID: 0000-0002-0572-7212

Khayal Iskandarov ^C

Corresponding author: PhD in National Security and Military Sciences, e-mail: khayal1333@gmail.com, ORCID: 0000-0001-8975-6530

Ельшан Хашимов ^{A B}

доктор у галузі національної безпеки та військових наук, професор, e-mail: hasimovel@gmail.com, ORCID: 0000-0001-8783-1277

Азіз Талібов ^B

доктор у галузі національної безпеки та військових наук, професор, e-mail: talibovaziz65@gmail.com, ORCID: 0000-0002-0572-7212

Хаял Іскандаров ^C

Corresponding author: к. наук з національної безпеки та військових наук, e-mail: khayal1333@gmail.com, ORCID: 0000-0001-8975-6530

^A Azerbaijan Technical University, Baku, Azerbaijan

^B National Defense University, Baku, Azerbaijan

^C Institute of Control Systems, Baku, Azerbaijan

^A Азербайджанський технічний університет, Баку, Азербайджан

^B Національний університет оборони, Баку, Азербайджан

^C Інститут систем управління, Баку, Азербайджан

Received: June 06, 2025 | Revised: August 09, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.1>

Purpose. To critically assess the socio-economic impact of the Zangezur Corridor on the regions it traverses, with a focus on key indicators such as employment, income levels, migration trends, local business development, and social infrastructure.

Method. SWOT and PESTEL analyses, triangulation analysis.

Findings. The research is among the first academic studies evaluating the socio-economic effects of the Zangezur Corridor. Its operation has already led to the creation of new jobs in the region. According to the survey, 72% of respondents feel that new employment opportunities have emerged. Official statistical forecasts predict that while the unemployment rate stood at 8% in 2021, it will drop to 4.5% by 2025. Approximately 70% of respondents indicated a willingness to remain or return to the region. Enhanced employment opportunities and the development of social infrastructure have reduced migration to large cities and, in some cases, even encouraged reverse migration. The construction of new roads, transport networks, and logistics centers has accelerated economic development. The corridor has facilitated the market access of agricultural and industrial products, thereby expanding export possibilities. The results demonstrate that the Zangezur Corridor is not merely a transportation route but also a strategic project that fosters the region's socio-economic development. Successful implementation of the project requires stronger public-private partnerships and the formulation of long-term socio-economic plans.

Practical implications. Strategic recommendations are provided for future economic and infrastructure projects in the region. The results suggest that targeted investments in transport infrastructure can stimulate the growth of local businesses, enhance market access for agricultural and industrial goods, and diversify regional economies.

Value. This paper offers original empirical insight into one of the most strategically significant yet understudied infrastructure projects in the South Caucasus—the Zangezur Corridor.

Paper type. Empirical.

Мета дослідження. Критично оцінити соціально-економічний вплив Коридору Зангезур на регіони, через які він проходить, з акцентом на ключові показники, такі як зайнятість, рівень доходів, тенденції міграції, розвиток місцевого бізнесу та соціальна інфраструктура.

Метод дослідження. SWOT і PESTEL аналіз, триангуляційний аналіз.

Результати дослідження. Це перше академічне дослідження, яке оцінює соціально-економічні наслідки Коридору Зангезур. Його робота вже призвела до створення нових робочих місць у регіоні. За опитуванням, 72 % респондентів вважають, що з'явилися нові можливості працевлаштування. Офіційні статистичні прогнози прогнозують, що рівень безробіття, який у 2021 році становив 8 %, скоротиться до 4,5 % до 2025 року. Близько 70 % респондентів висловили готовність залишитися або повернутися до регіону. Посилення можливостей працевлаштування та розвиток соціальної інфраструктури зменшили міграцію до великих міст і, в деяких випадках, навіть сприяли зворотній міграції. Будівництво нових доріг, транспортних мереж і логістичних центрів сприяло економічному розвитку. Коридор полегшив вихід на ринок сільськогосподарської та промислової продукції, розширюючи можливості експорту. Результати свідчать, що Коридор Зангезур — це не просто транспортний маршрут, а стратегічний проект, який сприяє соціально-економічному розвитку регіону. Успішна реалізація проекту вимагає посилення державно-приватного партнерства та формулювання довгострокових соціально-економічних планів.

Практична цінність дослідження. Наведено стратегічні рекомендації щодо майбутніх економічних та інфраструктурних проектів у регіоні. Результати свідчать, що цілеспрямовані інвестиції в транспортну інфраструктуру можуть стимулювати зростання місцевого бізнесу, покращити доступ до ринку сільськогосподарської та промислової продукції і диверсифікувати регіональні економіки.

Цінність дослідження. Ця робота пропонує оригінальні емпіричні висновки щодо одного з найстратегічніших, але недосліджених інфраструктурних проектів у Південному Закавказзі — Коридору Зангезур.

Тип статті. Емпірична.

Key words: Zangezur corridor, social situation, regional integration, unemployment, logistics infrastructure, transport corridors, environmental security.

Ключові слова: коридор Зангезур, соціальна ситуація, регіональна інтеграція, безробіття, логістична інфраструктура, транспортні коридори, екологічна безпека.

Introduction

Geopolitical realities play a decisive role in shaping a state's foreign policy orientation. The geopolitics of the South Caucasus is particularly complex, volatile, and fragile. Comprising three independent states—Azerbaijan, Georgia, and Armenia—that once belonged to the same imperial structure, the region underwent significant transformation following the dissolution of the Soviet Union. Since gaining independence, each of the South Caucasus republics has pursued a distinct geopolitical trajectory: Armenia has aligned itself with the Collective Security Treaty Organization (CSTO), Azerbaijan has adopted a more independent and balanced foreign policy vis-à-vis major powers, while Georgia has consistently signaled a strong pro-NATO stance. The region's persistent instability is exacerbated by the absence of a comprehensive peace agreement between Armenia and Azerbaijan, Russia's growing assertiveness, and the lack of a substantive NATO presence—all of which are key factors in understanding the current geopolitical landscape of the South Caucasus (Iskandarov et al., 2019). Although the three republics of the South Caucasus have pursued divergent policy paths since the dissolution of the Soviet Union, their destinies remain inextricably intertwined. As Sadiyev and Iskandarov (2018) argue, it is impossible to assess emerging security threats in the region without accounting for the broader geopolitical and interdependent realities among these states. The strategic significance of the South Caucasus–Caspian region is further amplified by the presence of vital transport corridors that generate substantial economic benefits for a wide range of countries. One of the most secure, efficient, and geopolitically viable routes connecting East and West originates in China, traverses Central Asia, the Caspian Sea, the South Caucasus, and Türkiye, and ultimately extends to Europe.

In recent years, large-scale infrastructure projects—particularly in transport and logistics—have substantially elevated the South Caucasus region's geostrategic significance (Abdirakhimova, 2024; Talibov et al., 2023). In this context, the Zangezur Corridor assumes particular significance. Presently, there is a unique opportunity to enhance the abovementioned route's efficiency and security through the establishment of this corridor. By unlocking the full potential of this corridor, the region stands to benefit from strengthened economic and trade relations across a vast geography, thereby fostering greater regional development and integration. In this context, Azerbaijan's proactive role in developing and operationalizing the East–West transport corridor has been widely acknowledged and appreciated by partner nations. Azerbaijan continues to pursue a dynamic and multi-layered cooperation strategy aimed at enhancing the corridor's functionality and strategic value (Gawliczek & Iskandarov, 2023). Beyond enhancing trade and transport connectivity, this corridor has the potential to bring about qualitative shifts in the socio-economic landscape of the regions it traverses. Global experience demonstrates that large-scale transport initiatives not only expedite regional integration but also exert a profound influence on local livelihoods improving income levels, infrastructure development, and employment prospects.

It is important to underscore that initiatives like the Zangezur Corridor are not confined to bolstering economic power alone; they also hold considerable potential to foster social development and promote cultural integration (Hajiyeva, 2024). This is particularly vital in the post-conflict period, as it contributes to improving living standards, generating employment opportunities, and integrating local entrepreneurs into regional and global markets. Enhanced infrastructure in the region also strengthens key sectors such as agriculture, tourism, and industry. At the same time, pressing social challenges—including migration management, the prevention of rural depopulation, and even the stimulation of reverse migration—gain prominence.

The launch of the Zangezur Corridor, beyond its economic advantages, significantly accelerates the attraction of new investments in the construction, transport, and service sectors (Macid et al., 2024). This development creates broad opportunities for public–private sector collaboration. Enhancing logistics, production, and processing infrastructure, in turn, revitalizes the

region's agricultural sector by increasing the export capacity of agricultural products (Saqib & Naazer, 2023). Moreover, the planned infrastructure along the corridor extends beyond roads and transportation to include anticipated improvements in communications, energy, water supply, and other essential utilities.

The primary objective of this article is to undertake a comprehensive analysis of the Zangezur Corridor's impact on the social conditions of populations residing in the regions it traverses. The study begins by examining existing theoretical frameworks and practical experiences related to the integration of large-scale transport projects into the socio-economic sphere. Subsequently, drawing on surveys and official statistical data from the region, the research evaluates the corridor's effects on key indicators such as social welfare, employment, income levels, and migration dynamics. From a sustainable development perspective, the article also seeks to propose ways to uphold ecological integrity and social justice. Ultimately, the research aims to offer a holistic understanding of the opportunities and prospects that the Zangezur Corridor presents for local communities.

The implementation of large-scale transport projects stimulates economic activity and brings about positive changes in the social conditions of populations in the affected regions. Transport corridors often promote job creation, boost tourism development, and enable the faster and more efficient export of local products to international markets. While numerous studies on the Zangezur Corridor have primarily emphasized its geopolitical and logistical significance, research on its social impact remains relatively scarce. To address this gap, more comprehensive studies are needed—particularly those that explore aspects such as social welfare, migration patterns, and cultural-spiritual dynamics. Indeed, major international transport corridors not only enhance trade turnover but also lay the foundation for long-term infrastructure renewal and improvements in overall social well-being.

Theoretical background

Theories of regional integration suggest that the formation of transport corridors in any region serves to expand that region's economic, social, and even cultural ties. In this context, transport projects playing a transit role between Central Asia and Eastern Europe (e.g., the "One Belt, One Road" initiative) have significantly influenced regional integration (Saqib & Naazer, 2023). Aliyeva et.al (2023) claim that the success of such projects depends not only on economic factors but also on political stability, social support, and adherence to environmental standards.

Numerous studies underscore the substantial influence of transport corridors on social well-being, particularly through their positive effects on employment rates and income generation. The construction of new roads and rail infrastructure generates short-term employment in the construction sector while fostering long-term job creation in logistics and related services. For instance, a World Bank study demonstrates that the development of transport corridors not only revitalizes regional economies but also improves access to essential resources such as healthcare, education, and public services, thereby substantially enhancing overall social welfare (Stokenberga et al., 2024). Global experiences reveal that investments in transportation infrastructure—particularly fast and comfortable mobility—strengthen the so-called "multiplier effect" in the tourism sector. This effect helps local communities create additional jobs in lodging, dining, entertainment, and cultural activities (Frechtling & Horváth, 1999). In the agricultural sector, improvements in logistics infrastructure expand opportunities for processing and exporting products. For farmers, the formation of more favorable logistical networks helps reduce product losses and improve production efficiency. At the same time, local producers gain broader access to foreign markets, enabling them to gain additional income sources (Abbasov, 2024). Environmental impacts have also drawn scholarly attention, with some researchers specifically focusing on their assessment in the context of transport corridors (Teo et al., 2019). However, there is a noticeable paucity of scholarly research specifically addressing the prospects of the Zangezur Corridor, which

underscores the relevance and timeliness of this topic for academic inquiry. Shokri (2024), Gawliczek & Iskandarov (2022; 2023) discuss the plausibility of the Zangezur corridor being used and highlights its importance as an integral element of the global transit route. The authors conduct comparative analysis of different transit routes and justify the advantages of opening this corridor for all stakeholders and underscore the regional unity in the South Caucasus as a prerequisite for eliminating or at least mitigating economic dependence and healing the “regional fracture” of decades. Iskandarov et al. (2020) highlight the geopolitical importance of the Caspian basin and the impact of its energy resources on the energy security of non-regional countries. The book edited by Azhgaliyeva et al. (2024) provides an in-depth analysis of the development of the Middle Corridor within the Central Asia Regional Economic Cooperation (CAREC) region, with particular emphasis on supply chain resilience and trade facilitation. It explores the potential economic benefits of transport corridors, including the enhancement and diversification of cross-border trade, stimulation of domestic production, attraction of investment, job creation, and reduction of transportation costs. At the same time, the book highlights significant barriers to the further development of trade and transport infrastructure, such as difficulties in securing long-term financing, regulatory divergence, high initial costs, the complexity of managing large-scale investments, risk mitigation challenges, and uncertainties regarding the projected benefits. Deen et al. (2023) highlight the establishment of a transport link between mainland Azerbaijan and its exclave Nakhchivan—commonly known as the Zangezur Corridor—as one of the most contentious yet strategically significant elements of the Armenia–Azerbaijan normalization process. A segment of the existing literature posits that improved infrastructure can mitigate migration flows to major urban centers by stimulating economic activity within the region. Concurrently, the generation of new local employment opportunities may curb rural depopulation and even foster return migration. This perspective is particularly reinforced by studies examining socio-economic rehabilitation in post-conflict regions (Isgandarli, 2022).

In summary, a comprehensive review of the literature suggests that large-scale infrastructure projects such as the Zangezur Corridor have both direct and indirect effects across a range of economic sectors. These effects encompass employment, migration, agriculture, tourism, and the preservation of cultural and spiritual values. The analysis of existing studies underscores the importance of integrating environmental and social responsibility into such initiatives to ensure their contribution to sustainable development.

Data and methods

A mixed-method approach was employed to comprehensively assess the impact of the Zangezur Corridor on the social conditions of populations residing in the areas it traverses. The methodological framework integrates both quantitative and qualitative data collection and analysis, enabling a multifaceted evaluation of economic-statistical indicators alongside in-depth insights into the social welfare of local communities. The primary methods and analytical tools used are outlined below:

1. **Collection of Statistical Data:** Official reports and statistical bulletins from the State Statistics Committee, the Ministry of Labor and Social Protection, and other relevant governmental bodies were reviewed. Key indicators such as population growth, employment levels, average monthly incomes, and agricultural and industrial output were gathered. These data sets served as the basis for comparing socio-economic conditions before and after the operationalization of the corridor.

2. **Modeling Socio-Economic Indicators:** Descriptive and regression analyses were conducted using the compiled data. A multiple regression model was applied to explore the relationship between socio-economic outcomes and various independent variables—such as infrastructure spending, the number of logistics facilities, and population migration. The model helped establish statistically significant associations between the corridor’s development and changes in employment and income levels.

3. Semi-Structured Interviews: Interviews were carried out in several strategically selected regions along the corridor. Participants included local residents, farmers, municipal leaders, and representatives of local executive authorities. These interviews focused on perceived changes in social welfare, migration trends, employment opportunities, and public attitudes toward the corridor project. This qualitative data helped contextualize the observed trends in the quantitative analysis.

4. Focus Group Discussions: Focus groups were organized in the same regions, targeting specific social segments such as youth, women, farmers, and small and medium-sized entrepreneurs (SMEs). These discussions yielded rich, contextual insights into the corridor's socio-economic effects and captured current concerns and expectations regarding infrastructure development. Findings were cross-compared with interview data to identify convergences and discrepancies.

5. Triangulation Analysis: To enhance methodological robustness and reduce bias, a triangulation strategy was employed, comparing results from both quantitative and qualitative streams. This integrative analysis enabled the identification of inconsistencies and reinforced the overall validity of the findings.

6. SWOT and PESTEL Analyses: A SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) was conducted to evaluate internal and external factors influencing the corridor's development. Additionally, a PESTEL framework (Political, Economic, Social, Technological, Environmental, Legal) was applied at the macro level to systematically analyze broader structural influences affecting the corridor.

The main limitations of the methodology are as follows:

Restricted access to certain areas during fieldwork constrained direct observation efforts.

The subjectivity of respondents in interviews may have introduced bias; to mitigate this, data were triangulated by comparing inputs from multiple respondents within each category.

Temporal discrepancies in statistical datasets—owing to variations in reporting intervals and data coverage—posed challenges for conducting precise longitudinal comparisons.

This mixed-method research design facilitates a comprehensive and balanced analysis of both quantitative and qualitative dimensions of the socio-economic landscape in regions influenced by the Zangezur Corridor. By integrating diverse data sources and methodologies, the study enhances the reliability, validity, and objectivity of its findings, thereby offering a nuanced evaluation of the corridor's actual impact on social welfare and regional development.

Results

Building on the methodological framework outlined earlier, this study offers a comprehensive analysis of the socio-economic transformations in the regions affected by the Zangezur Corridor. The section begins with a presentation of the quantitative (statistical) data, followed by an examination of the qualitative findings derived from interviews and focus group discussions. Finally, the results from both approaches are triangulated to provide an integrated and holistic assessment.

Quantitative Analysis Results

Based on data from the State Statistics Committee, the Ministry of Labor and Social Protection, and other official sources, notable shifts were observed in several key socio-economic indicators along the Zangezur Corridor (see Table 1).

In the five years preceding the corridor's operationalization, the average annual population growth rate in the region stood at approximately 1.2 %. Following the expansion of infrastructure under the project, this figure increased to 1.8%, accompanied by signs of reverse migration in certain rural areas.

Additionally, the unemployment rate declined significantly—from 12.5 % to 7.5 %—with the majority of new employment opportunities emerging in construction, agriculture, logistics, and the service sector.

Table 1. Changes in Major Socio-Economic Indicators in the Region

Indicators	Before the Corridor	After the corridor (Forecast)
Population (thousands)	250	280
Unemployment Rate (%)	12.5	7.5
Average Income Growth (%)	2.0	6.5
Industrial & Business Growth (%)	5.0	15.0

Average monthly income increased from 2.0% to 6.5% compared to previous years. The growth rate of entrepreneurial activity nearly tripled, in parallel with the support of vocational training courses and local start-ups.

Due to reduced logistics costs, farmers' productivity rose by 15–20%. New enterprises focusing on product processing and packaging have enabled farmers to generate added value.

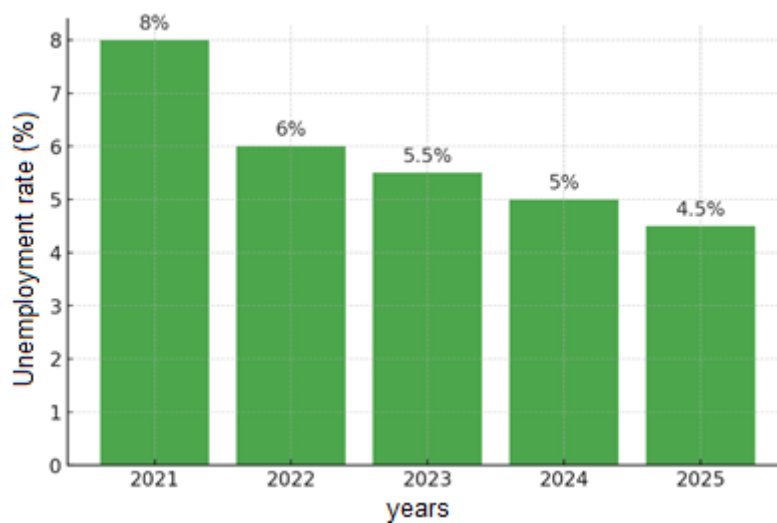


Figure 1. Comparison of unemployment rates before and after the launch of the Zangezur Corridor

A survey of 300 people was conducted to measure local awareness of the Zangezur Corridor, its impact on employment and income growth, and individuals' future plans regarding residence. The survey findings indicate that the majority of respondents (85%) are aware of the corridor and believe it has contributed to socio-economic changes in the region.

According to the survey:

72% of respondents feel that new employment opportunities have been created in the area;

65% believe their income has increased;

70% plan to remain in or return to the region.

Table 2 summarizes the survey results.

Table 2. Survey Data (n=300)

Question	Positive Response (%)	Negative Response (%)
Are you generally aware of the Zangezur Corridor?	85	15
Do you feel the corridor has created new job opportunities here?	72	28
Do you believe your income has increased?	65	35
Do you intend to stay in or return to the region in the future?	70	30

These findings are consistent with official statistical indicators. For example, the unemployment rate stood at 8 % in 2021 and is projected to decline to 4.5 % by 2025. This trend corresponds with survey results, where 72% of respondents reported observing the creation of new employment opportunities.

Official economic reports indicate that the average monthly income, which stood at 520 AZN in 2021, is projected to increase to approximately 750 AZN by 2025. This upward trend is supported by survey findings, with 65 % of respondents reporting an improvement in their income levels. Taken together, both the statistical data and public opinion surveys suggest that the socio-economic impact of the Zangezur Corridor is both substantial and far-reaching.

Qualitative Findings

Semi-Structured Interviews. Representatives from municipal and executive authorities highlighted not only the economic advantages of infrastructure projects but also their broader social benefits. In particular, they emphasized that infrastructure modernization has enhanced the quality of essential public services such as healthcare and education. Many farmers and rural residents also pointed out that improved transport networks have significantly increased their ability to deliver agricultural products to market, thereby enhancing their competitiveness in local economies. As market access has expanded, household incomes have risen, and in some instances, individuals who had previously migrated to urban areas have returned to their home communities. Furthermore, the opening of a major transport corridor has reduced shipping times for both raw materials and finished goods, prompting logistics companies to lower freight costs—thereby creating favorable conditions for the emergence of innovative business models.

Focus Group Discussions. As part of this study, focus group discussions were conducted to capture the perspectives of various social groups regarding the impact of the Zangezur Corridor. Participants included youth, women, farmers, entrepreneurs, and local community representatives. The primary objective was to assess how the economic and social effects of the corridor differ across groups and to identify the expectations of the local population.

Findings from the focus group discussions indicate that young people generally perceive the Zangezur Corridor positively, particularly in terms of enhanced employment opportunities. Many youth participants emphasized the scarcity of job prospects in the region, noting that new infrastructure projects are creating career pathways in fields such as logistics, trade, agriculture, the service sector, and tourism. However, some respondents highlighted the need to modernize local higher education and vocational training institutions, arguing that the long-term benefits of such infrastructure initiatives will be fully realized only through the development of a skilled workforce.

Women participating in the discussions reported that the corridor's operation, and the subsequent growth in service-sector employment—especially in tourism, hospitality, public catering, and small business—have contributed to increased female economic activity. Nonetheless, participants emphasized that the expansion of women's entrepreneurship is contingent upon improved access to investment, credit facilities, and targeted state support. Women engaged in household production and small-scale businesses particularly stressed the importance of gaining access to broader markets via the corridor as a key factor for future growth.

Representatives from the farming and agricultural sectors noted that, since the corridor became operational, market access for agricultural products has significantly improved. In the past, long delivery times and high transportation costs resulted in substantial post-harvest losses. The improved transport infrastructure has helped mitigate these challenges. Farmers also expressed strong support for the development of local processing and packaging facilities along the corridor, emphasizing that such infrastructure would increase the added value of agricultural goods and enhance their export potential.

Entrepreneurs highlighted the corridor's positive impact on the regional business climate. Participants pointed to reduced logistics costs, expanded access to new markets, and improved trade

linkages as drivers of increased commercial activity. However, they also identified the need for greater investment inflows and reinforced state support mechanisms to fully capitalize on these gains.

Local community representatives observed a decline in outward migration from the region, and in some cases, even a reversal of migration trends. One of the key factors prompting the return of former residents is the emergence of new employment opportunities generated by the corridor. At the same time, several respondents underscored the need for continued investment in social infrastructure—particularly in education, healthcare, and housing—to ensure sustainable regional development.

Focus group discussions revealed the following key insights:

New employment opportunities have emerged for youth, however, enhancements in vocational and higher education systems remain necessary.

Women have benefited from increased opportunities in small business and the service sector, yet, sustained state support is essential for advancing women’s economic participation.

Farmers have gained improved access to markets for agricultural products, however, the establishment of local processing and packaging facilities is critical for value addition.

Entrepreneurs have identified new trade opportunities, nevertheless, further investment and the introduction of concessional financing mechanisms are needed.

Outmigration from local communities has decreased; yet, continued development of social infrastructure—particularly in education, healthcare, and housing—is imperative.

These findings suggest that the Zangezur Corridor has a transformative impact not only on economic development but also on broader aspects of social welfare. To fully realize the corridor’s potential, it is essential to strengthen public-private partnerships, prioritize local needs, and develop comprehensive long-term strategies.

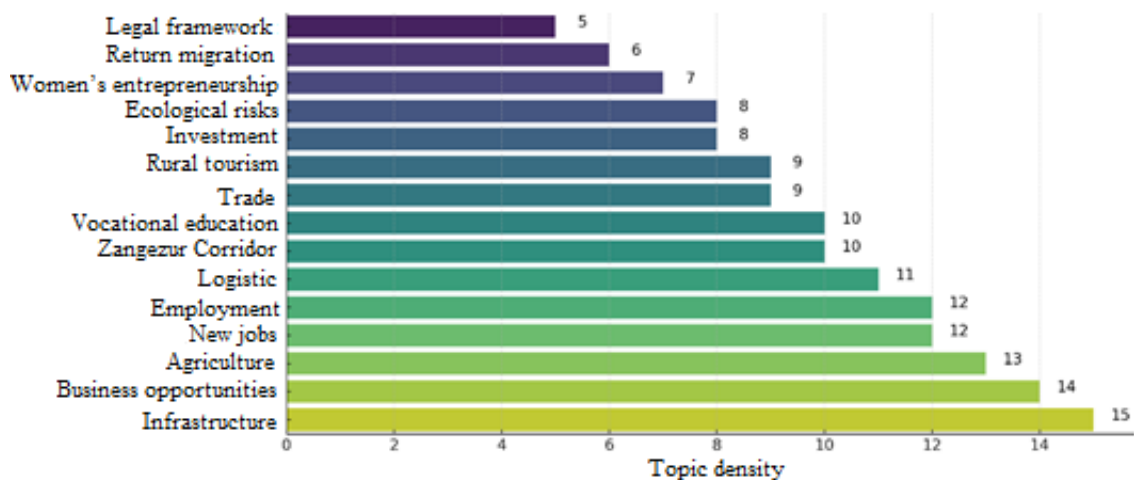


Figure 2. Key topics identified from focus group discussions – frequency diagram

Triangulation Analysis. In this study, a triangulation approach was adopted to ensure consistency and cross-validation between quantitative and qualitative data. By employing this method, the degree of convergence among data collected from various sources was assessed, thereby strengthening the objectivity and credibility of the findings. This approach is rooted in the comparative analysis of statistical (quantitative) data and field-based (qualitative) evidence.

During the triangulation process, official statistical indicators, field observations, interview responses, and focus group findings were systematically compared. The alignment across these data sources was evaluated according to the following key dimension:

1. Unemployment Rate and Expansion of Employment Opportunities:

Quantitative data: Statistical evidence shows that the unemployment rate stood at 8% in

2021 and is projected to decline to 4.5 % by 2025.

Qualitative data: Results from focus groups and field interviews confirm that new infrastructure projects—particularly in transport and logistics—have played a pivotal role in expanding employment opportunities.

Triangulation conclusion: Both data sets point to a marked decline in unemployment and a notable increase in job availability. However, some regions continue to face shortages of skilled labor, highlighting the need for targeted workforce development.

2. Income Growth and Local Economic Activity

Quantitative data: According to statistical projections, the average monthly income increased from 520 AZN in 2021 to an anticipated 750 AZN by 2025.

Qualitative data: Entrepreneurs interviewed and surveyed in focus groups reported that the development of new transport infrastructure has enhanced trade turnover and contributed positively to household incomes.

Triangulation conclusion: Both data sources converge, indicating a rise in average income levels. The key contributing factors include reduced logistics costs, expanded trade opportunities, and increased agricultural productivity.

3. Local Business Expansion and Investment Inflows

Quantitative data: The number of small and medium-sized enterprises (SMEs) in the region rose from approximately 1,200 in 2021 to a projected 2,000 by 2025.

Qualitative data: Field interviews confirmed notable growth in commerce and service sectors, driven by heightened demand along the corridor.

Triangulation conclusion: Both sources confirm the expansion of the business sector. Nevertheless, entrepreneurs emphasized the necessity for increased investment and more accessible concessional financing to sustain growth.

4. Migration and Settlement Patterns

Quantitative data: Official statistics indicate a decline in out-migration to urban centers and a modest rise in return migration to the region.

Qualitative data: Focus group discussions and resident interviews supported these trends, attributing them to improved local economic conditions and job creation along the corridor.

Triangulation conclusion: The alignment of qualitative and quantitative data suggests that the availability of new employment opportunities has mitigated rural-to-urban migration and, in some areas, stimulated reverse migration.

5. Assessment of Environmental and Social Issues

Quantitative data: Available statistical data on environmental impacts remain limited; however, the scale of infrastructure and industrial development may entail ecological risks.

Qualitative data: Several focus group participants expressed concerns regarding the environmental implications of infrastructure projects and noted deficiencies in social service provision in certain areas.

Triangulation conclusion: Environmental and social concerns are more prominently reflected in qualitative accounts. The lack of comprehensive statistical data underscores the need for further research to assess ecological sustainability and the adequacy of social infrastructure.

As a result of the triangulation analysis, the following key conclusions have been drawn:

Both official statistics and qualitative research consistently confirm a decrease in unemployment alongside an expansion of employment opportunities.

Rising average incomes and increased business activity are evident across both quantitative and qualitative data sets.

A decline in outward migration and a corresponding increase in regional settlement have been observed; however, further longitudinal research is necessary to assess the sustainability of this trend.

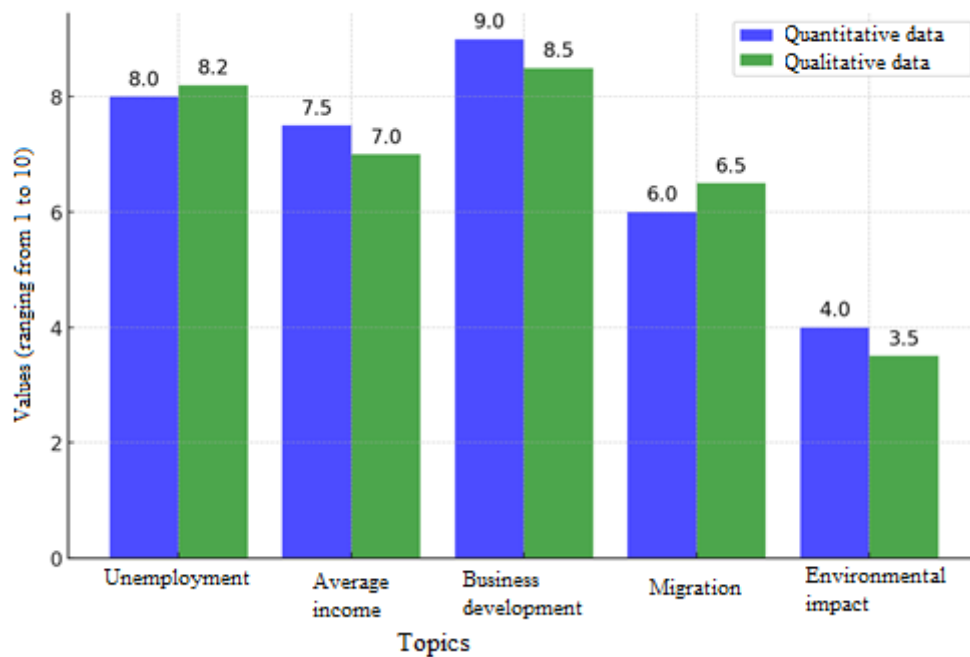


Figure 4. Triangulation analysis: a bar chart comparing quantitative and qualitative findings

Data on ecological and social impacts remain insufficient, with official statistics limited and local communities expressing diverse perspectives, underscoring the need for more comprehensive data collection.

These findings suggest that the socio-economic impact of the Zangezur Corridor is generally consistent across official statistics and field research. Nonetheless, additional investigations—particularly into ecological concerns and social infrastructure—are essential. The integration of diverse data sources has facilitated a more objective and balanced analysis, thereby informing strategic recommendations for future planning.

Table 3. Main indicators of the SWOT analysis

Category	Description
Strengths	Strengthened regional economic development, enhanced logistics and transport infrastructure, increased export potential, tourism development, and government/international support.
Weaknesses	Incomplete infrastructure projects, a shortage of skilled human resources, insufficient social services in certain areas, and inadequate assessment of environmental impacts.
Opportunities	Broader international trade, growth in agriculture and industry, adoption of technological innovations, increased investment flows.
Threats	Geopolitical risks, ecological and ecosystem-related challenges, financial constraints, and strains on the regional labor market.

PESTEL Analysis

The PESTEL framework provides a comprehensive lens through which to examine the political, economic, social, technological, environmental, and legal dimensions shaping the Zangezur Corridor's operations and long-term viability. The key findings are summarized below:

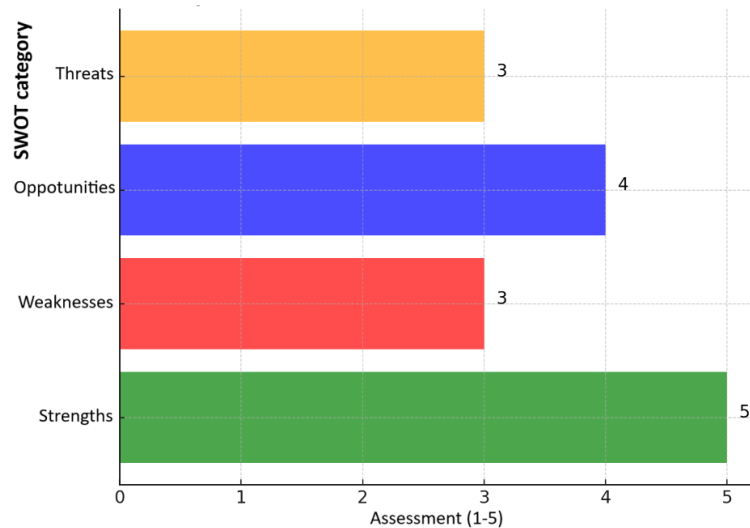


Figure 5. A bar chart illustrating key SWOT indicators

1. Political Factors

The Zangezur Corridor is a strategically significant transport and logistics initiative with both regional and international implications. Political dynamics and state involvement are central to its implementation:

The Azerbaijani government has played a proactive role, offering substantial financial and infrastructural support.

The corridor is poised to enhance regional trade connectivity and streamline international freight transportation.

Volatile inter-state relations and potential regional conflicts pose risks to long-term stability.

Nonetheless, by fostering interdependence through economic cooperation, the corridor may contribute to regional political stability.

2. Economic Factors

The economic implications of the Zangezur Corridor are among its most prominent features, promising to stimulate regional development:

Investment attraction: The corridor has increased the region's attractiveness to both domestic and foreign investors.

Employment generation: The development of logistics hubs and supporting sectors has contributed to a decline in unemployment.

SME growth: Enhanced connectivity has bolstered the competitiveness of small and medium-sized enterprises.

Infrastructure funding gap: Full operationalization of the corridor demands continued investment from public and private stakeholders.

Trade expansion: Improved export opportunities have emerged for both agricultural and industrial producers situated along the route.

3. Social Factors

The corridor's social implications are reflected in improved livelihoods, migration regulation, and expanding economic participation:

Job creation: The corridor has generated new employment opportunities, directly improving household incomes.

Migration reversal: Economic revitalization has slowed outward migration and encouraged return migration to the region.

Uneven access to services: Deficiencies in healthcare and education infrastructure remain, particularly in more remote areas.

Empowerment of women: Women's participation in the workforce has grown, particularly in service-oriented sectors such as tourism, hospitality, and retail.

4. Technological Factors

Technological modernization is a critical driver of the corridor's efficiency and future scalability:

Digital logistics: The deployment of automated freight systems and digital supply chain platforms has improved logistical performance.

E-commerce growth: Local businesses increasingly utilize digital trade platforms, expanding their market reach.

Innovation gaps: Full technological integration is constrained by funding limitations and a shortage of technical expertise in certain sectors.

Skills development: Strengthening vocational and technical education is essential to building a capable workforce aligned with modern logistics and IT standards.

5. Environmental Factors

Large-scale infrastructure initiatives inevitably interact with local ecosystems, necessitating a careful balance between development and sustainability:

Ecological disruption: Road and infrastructure construction pose risks to local biodiversity and landscapes.

Green transport solutions: Integrating renewable energy sources into logistics operations can mitigate environmental degradation.

Waste management concerns: Rising levels of industrial and agricultural waste require robust environmental monitoring systems.

Sustainable tourism: Promoting ecotourism and the green economy can add environmental and economic value to the region.

6. Legal Factors

A robust legal framework is essential to facilitate smooth operations, protect stakeholders, and ensure long-term success:

Alignment with international law: The corridor aligns with key legal frameworks governing cross-border trade and transit.

Regulatory reform needs: Gaps persist in legislation concerning environmental protection, transport safety, and trade facilitation.

Investor protections: Enhancing legal guarantees for private sector actors remains a priority to encourage sustained engagement.

The Zangezur Corridor is positioned as a transformative project capable of advancing regional development, international trade integration, and socio-economic welfare. However, its long-term success depends on addressing several structural challenges—including ecological sustainability, comprehensive technological integration, and legal reform. Realizing the full potential of the corridor will require robust public-private collaboration, with strategic emphasis on environmental stewardship and inclusive development.

Discussion

The analysis reveals that the socio-economic effects of the Zangezur Corridor are multifaceted and evolving. Prior to the corridor's establishment, socio-economic indicators in the region remained at moderate levels. However, the launch of large-scale infrastructure projects, the enhancement of logistics capacities, and the influx of new investments have collectively contributed to reshaping the region's macroeconomic landscape.

Employment and Labor Market Dynamics. A marked reduction in unemployment and the creation of new jobs—especially within the construction, agriculture, logistics, and service sectors—have significantly stimulated economic activity. Several rural localities that previously suffered from chronic unemployment have witnessed instances of reverse migration, which serves as a strong proxy for both economic revitalization and improved social well-being. To sustain this momentum, emphasis must be placed on workforce specialization and aligning local educational institutions with emerging labor market needs.

Income Growth and Entrepreneurial Expansion. The rise in average monthly income, coupled with the proliferation of entrepreneurial ventures, has strengthened the region's economic resilience and autonomy. The expansion of trade networks and access to new markets has particularly benefited small and medium-sized enterprises (SMEs), reinforcing their contribution to local economic dynamism. In this context, increasing the availability of concessional financing and enhancing government support frameworks could act as catalysts for accelerated and inclusive regional development.

Migration and Demographic Trends. The corridor has also had a stabilizing effect on regional migration flows. As employment prospects and infrastructure improve, a growing number of former migrants are contemplating a return to their home regions. Nevertheless, the long-term sustainability of this trend depends on the continued enhancement of social services, particularly in healthcare, education, and community infrastructure. Without such developments, the region may struggle to retain or attract populations in the long run.

Forecast models for the next 5-10 years

As part of this research, a series of forecast models were developed to examine the projected socio-economic impacts of the Zangezur Corridor over a 5–10 year horizon. These models facilitate the evaluation of key indicators such as unemployment rates, average monthly income trajectories, and migration dynamics.

The forecasting methodology was grounded in historical statistical data, which served as the empirical foundation for constructing linear regression models. Optimal parameters were identified through model calibration to ensure accuracy and robustness in the projections. Based on these parameters, socio-economic forecasts for the period 2026–2035 were generated, providing insights into anticipated trends under current developmental trajectories (see Figures 6–8).

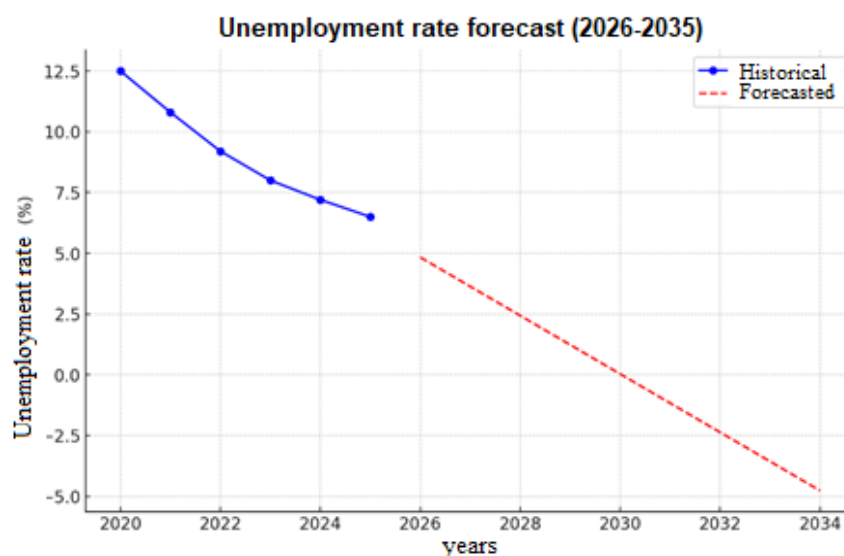


Figure 6. Forecast of unemployment rate for the years 2026-2035.

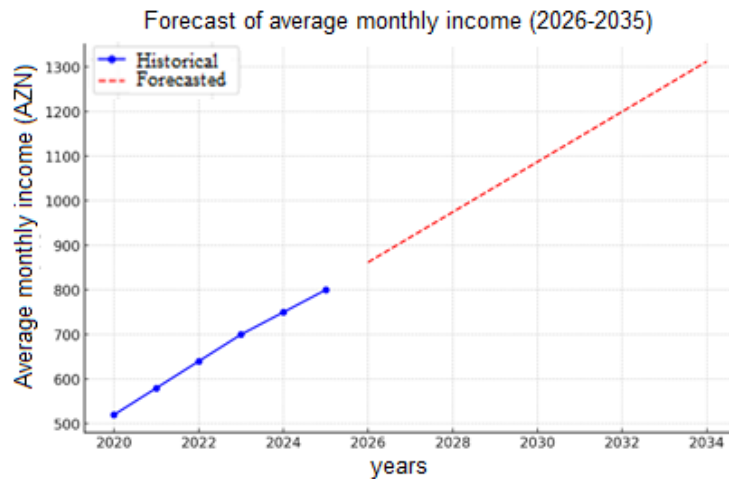


Figure 7. Forecast of average monthly income for the years 2026-2035.

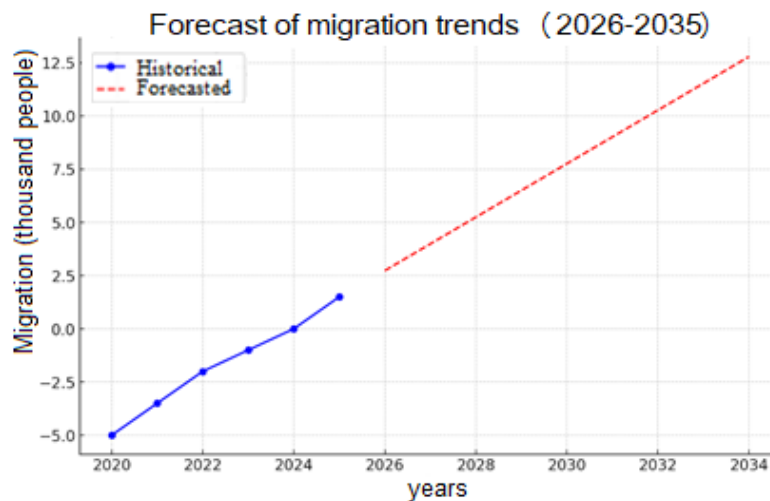


Figure 8. Forecast of migration trends for the years 2026-2035.

The analysis yielded the following key forecasted indicators for the Zangezur Corridor region:

1. **Unemployment Rate Forecast:** Based on current statistical data, the unemployment rate stood at 6.5% in 2025. Projection models suggest a stabilization of this rate between 4% and 5% by 2035. This positive trend is primarily linked to increased regional economic activity and the creation of new employment opportunities across diverse sectors.

2. **Average Monthly Income Growth:** The average monthly income reached approximately 800 AZN in 2025. Forecasts indicate a further rise to between 1,100 and 1,200 AZN by 2035. This income growth is attributable to the expansion of emerging industries, the development of small and medium-sized enterprises (SMEs), and efficiencies gained through reduced logistics costs.

3. **Migration Trends:** Migration analysis reveals an initial population outflow of approximately 5,000 individuals from the region in 2020. However, by 2025, this trend reversed, showing a net inflow of 1,500 people. Projections suggest continued positive net migration through 2035, reflecting an increasing return of residents to the region as socio-economic conditions improve.

Strategic Recommendations:

Enhancing Public-Private Sector Collaboration: Strengthening partnerships between governmental and private actors is critical for sustaining job creation and enhancing the region's economic appeal.

Investments in Social Infrastructure: Targeted improvements in education, healthcare, and public services are essential to support demographic stability and positively influence migration patterns.

Maintaining Ecological Balance: Integrating environmental considerations into development plans is vital to ensure the long-term sustainability of regional growth.

These forecast models offer a comprehensive perspective on the potential socio-economic impacts of the Zangezur Corridor, providing policymakers and economic analysts with actionable insights for strategic planning and evaluation.

Conclusion

This article has examined the socio-economic impact of the Zangezur Corridor on the communities along its route. The research findings reveal several key benefits attributable to the corridor's operation:

1. Employment and Income Growth: A decline in unemployment rates coupled with an enhanced entrepreneurial environment has stimulated economic activity.

2. Advancement of Social Infrastructure: Upgrades to roads, communication networks, healthcare facilities, and educational institutions have contributed significantly to improving residents' quality of life.

3. Regulation of Migration Patterns: The emergence of new job opportunities and improved social services have helped mitigate migration outflows, with some evidence of reverse migration encouraging population retention.

4. Activation of Cultural and Tourism Potential: The promotion of the region's historical and cultural assets, alongside the development of new tourism routes, has diversified local income sources and fostered economic resilience.

Collectively, these findings underscore the Zangezur Corridor as a pivotal catalyst for sustained socio-economic development in the region. To fully realize its potential, it is imperative to emphasize ecological sustainability, social equity, and long-term development planning. The evidence illustrates that the corridor transcends its function as a mere transport artery, positioning itself as a strategic instrument for regional socio-economic advancement. Achieving this vision necessitates robust public-private partnerships and the formulation of comprehensive, forward-looking socio-economic strategies.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

- Abbasov, N. (2024). The potential role of the Zangazur corridor in the development of economic relations between Azerbaijan and the countries of the Turkish World (in the example of Turkey). *Geostrategiya*, pp. 149-153. Available at: <https://www.doi.com/10.30546/3006-0346.2023.6.78.149> (Accessed 10 April 2025).
- Abdirakhimova, M. (2024). *The place of South Caucasus as a part of international corridors*. Presented at the International Conference on South Caucasus in the Context of Modern Global Challenges, Baku, 3 May, pp. 20–21. Available at: <https://au.edu.az/userfiles/uploads/517f08cc736c6b4d2bf63e8f3afaf092.pdf> (Accessed: 28 April, 2025).

- Aliyeva, A., Mammadova, R., Aliyeva, L. (2023). Sustainability of post-conflict recovery strategies: impact to Azerbaijani economy. *Studi di storia medioevale e di diplomatica*, 12(4), pp. 1521–1532. <https://doi.org/10.46932/sfjdv4n4-007> (Accessed: 11 April 2025).
- Azhgaliyeva, D., Mogilevskii, R. & Akbar, R. (eds.) (2024). *Unlocking Transport Connectivity in the Caucasus and Central Asia*. Manila: Asian Development Bank. Available at: <https://chatgpt.com/c/6839505e-a250-8001-adde-53896aa2b41d> (Accessed: 30 May 2025).
- Deen, B., Zweers, W. & Linder, C. (2023). *The EU in the South Caucasus: Navigating a geopolitical labyrinth in turmoil*. Clingendael Institute, March. Available at: <https://www.clingendael.org/sites/default/files/2023-03/the-eu-in-the-south-caucasus.pdf> [Accessed 30 May 2025].
- Frechtling, D.C. & Horváth, E. (1999). Estimating the multiplier effects of tourism expenditures on a local economy through a regional input-output model. *Journal of Travel Research*, 37(4), pp.324–332. <https://doi.org/10.1177/004728759903700402> (Accessed: 22 April 2025).
- Gawliczek, P. & Iskandarov, K. (2023) The Zangezur corridor as part of the global transport route (against the backdrop of power games in the South Caucasus region), *Security and Defence Quarterly*, 41(1), pp. 36–53. <https://doi.org/10.35467/sdq/161993>.
- Hajiyeva, N. (2024). Revitalizing Karabakh: the strategic role of science and education in post-liberation development. *Modern Diplomacy*. Independent European Media LTD. Available at: <https://moderndiplomacy.eu/2024/08/15/revitalizing-karabakh-the-strategic-role-of-science-and-education-in-post-liberation-development/> (Accessed: 28 April 2025).
- Isgandarli, R. (2022). Post-conflict Azerbaijan and development for peace: The role of NGOs. *Handbook of Research on Ethnic, Racial, and Religious Conflicts and Their Impact on State and Social Security*, pp. 121-136. Hershey, Pennsylvania: IGI Global. <https://doi.org/10.4018/978-1-7998-8911-3.ch008> (Accessed: 16 April 2025).
- Iskandarov, K. & Gawliczek, P. (2022) Economic coercion as a means of hybrid warfare: The South Caucasus as a focal point, *Security and Defence Quarterly*, 40(4), pp. 47–57. <https://doi.org/10.35467/sdq/151038>.
- Iskandarov, K., Mahammadali, V. & Gardashkhan, A. (2020). Caspian region: Geopolitical arena. Clash of interests and energy security”, *Civitas Et Lex*, 26(2), pp. 7-22. <https://doi.org/10.31648/cetl.5138> (Accessed: 28 May 2025).
- Iskandarov, K., Mammadzada, V. & Sadiyev, S. (2019). Non-Alliance policy as a principle of shaping the national security with a focus on the case of Azerbaijan, *Journal of Defense Resources Management*, 10:2, pp. 62-72. Available at: <https://www.cceol.com/search/article-detail?id=812186> (Accessed: 28 May 2025).
- Sadiyev, S. & Iskandarov, K. (2018). The evolution of the security environment in the South Caucasus since the end of the Cold War, 17th Workshop of the PfP Consortium Study Group Regional Stability in the South Caucasus, “What a New European Security Deal” could mean for the South Caucasus, 14/2018, pp. 47-53. Available at: https://www.academia.edu/37852657/What_a_New_European_Security_Deal_could_mean_for_the_South_Caucasus (Accessed: 29 May 2025).
- Saqib, N.U. & Naazer, M.A. (2023). Dynamics of regional integration in Central Asia: A case study of Belt and Road Initiative. *Journal of South Asian Studies*, 11(3), pp. 287-298. Available at: <https://www.esciencepress.net/journals/index.php/JSAS/article/view/4981> (Accessed: 28 April 2025).
- Shokri, U. (2024). *Geopolitical Rivalries in the South Caucasus: Evaluating the Aras Corridor as an Alternative to Zangezur*. Trends Research. Available at: <https://trendsresearch.org/insight/geopolitical-rivalries-in-the-south-caucasus-evaluating-the-aras-corridor-as-an-alternative-to-zangezur/> (Accessed: 29 May 2025).

- Stokenberga, A., Morales Sarriera, J., Sekerinska, L., Ferrarini, L.R., Raffo, V.I., Schiro, J., Comini, N., Spinelli, L., Balestro, F. (2024). *Corridors for Development and Growth*. Washington, D.C.: World Bank Group. Available at: <http://documents.worldbank.org/curated/en/099101524184531877> (Accessed: 28 April 2025).
- Talibov, A.M. & Hashimov, E.G. (2024). Vehicle transport cost calculation method. Current directions of development of information and communication technologies and control tools, Proceedings of the 14th International Scientific and Technical Conference, Vol. 2, pp. 3-6.
- Talibov, A.M., Hashimov, E.G., Sabziev, E.N., Pashayev, A.B. (2023). On the optimal placement of logistics centers. *Informatics and Control Problems*, 43(2), pp. 51–58. <https://doi.org/10.54381/icp.2023.2.07> (Accessed: 21 April 2025).
- Talibov, A.M., Sabziev, E.N., Pashayev, A.B. & Hashimov, E.G. (2023). Optimal placement of logistics centers in the Republic of Azerbaijan. *2nd International Conference on Problems of Logistics, Management and Operation in The East-West Transport Corridor (PLMO 2023)*, Baku, 24-26 May 2023. Available at: <https://plmo.cyber.az/2023/papers/20.pdf> (Accessed: 17 March 2025).
- Teo, H.C., Lechner, A.M., Walton, G.W., Chan, F.K.S., Cheshmehzangi, A., Tan-Mullins, M., Chan, H.K., Sternberg, T., Campos-Arceiz, A. (2019). Environmental impacts of infrastructure development under the Belt and Road Initiative. *Environments*, 6(6), p. 72. <https://doi.org/10.3390/environments6060072> (Accessed: 23 March 2025).

Список використаних джерел

- Abbasov, N. (2024). The potential role of the Zangazur corridor in the development of economic relations between Azerbaijan and the countries of the Turkish World (in the example of Turkey). *Geostrategiya*, pp. 149-153. Available at: <https://www.doi.com/10.30546/3006-0346.2023.6.78.149> (Accessed 10 April 2025).
- Abdirakhimova, M. (2024). *The place of South Caucasus as a part of international corridors*. Presented at the International Conference on South Caucasus in the Context of Modern Global Challenges, Baku, 3 May, pp. 20–21. Available at: <https://au.edu.az/userfiles/uploads/517f08cc736c6b4d2bf63e8f3afaf092.pdf> (Accessed: 28 April, 2025).
- Aliyeva, A., Mammadova, R., Aliyeva, L. (2023). Sustainability of post-conflict recovery strategies: impact to Azerbaijani economy. *Studi di storia medioevale e di diplomatica*, 12(4), pp. 1521–1532. <https://doi.org/10.46932/sfidv4n4-007> (Accessed: 11 April 2025).
- Azhgaliyeva, D., Mogilevskii, R. & Akbar, R. (eds.) (2024). *Unlocking Transport Connectivity in the Caucasus and Central Asia*. Manila: Asian Development Bank. Available at: <https://chatgpt.com/c/6839505e-a250-8001-adde-53896aa2b41d> (Accessed: 30 May 2025).
- Deen, B., Zweers, W. & Linder, C. (2023). *The EU in the South Caucasus: Navigating a geopolitical labyrinth in turmoil*. Clingendael Institute, March. Available at: <https://www.clingendael.org/sites/default/files/2023-03/the-eu-in-the-south-caucasus.pdf> [Accessed 30 May 2025].
- Frechtling, D.C. & Horváth, E. (1999). Estimating the multiplier effects of tourism expenditures on a local economy through a regional input-output model. *Journal of Travel Research*, 37(4), pp.324–332. <https://doi.org/10.1177/004728759903700402> (Accessed: 22 April 2025).
- Gawliczek, P. & Iskandarov, K. (2023) The Zangezur corridor as part of the global transport route (against the backdrop of power games in the South Caucasus region), *Security and Defence Quarterly*, 41(1), pp. 36–53. <https://doi.org/10.35467/sdq/161993>.
- Hajiyeva, N. (2024). Revitalizing Karabakh: the strategic role of science and education in post-liberation development. *Modern Diplomacy*. Independent European Media LTD. Available

- at: <https://moderndiplomacy.eu/2024/08/15/revitalizing-karabakh-the-strategic-role-of-science-and-education-in-post-liberation-development/> (Accessed: 28 April 2025).
- Isgandarli, R. (2022). Post-conflict Azerbaijan and development for peace: The role of NGOs. *Handbook of Research on Ethnic, Racial, and Religious Conflicts and Their Impact on State and Social Security*, pp. 121-136. Hershey, Pennsylvania: IGI Global. <https://doi.org/10.4018/978-1-7998-8911-3.ch008> (Accessed: 16 April 2025).
- Iskandarov, K. & Gawliczek, P. (2022) Economic coercion as a means of hybrid warfare: The South Caucasus as a focal point, *Security and Defence Quarterly*, 40(4), pp. 47–57. <https://doi.org/10.35467/sdq/151038>.
- Iskandarov, K., Mahammadali, V. & Gardashkhan, A. (2020). Caspian region: Geopolitical arena. Clash of interests and energy security”, *Civitas Et Lex*, 26(2), pp. 7-22. <https://doi.org/10.31648/cetl.5138> (Accessed: 28 May 2025).
- Iskandarov, K., Mammadzada, V. & Sadiyev, S. (2019). Non-Alliance policy as a principle of shaping the national security with a focus on the case of Azerbaijan, *Journal of Defense Resources Management*, 10:2, pp. 62-72. Available at: <https://www.cceol.com/search/article-detail?id=812186> (Accessed: 28 May 2025).
- Sadiyev, S. & Iskandarov, K. (2018). The evolution of the security environment in the South Caucasus since the end of the Cold War, 17th Workshop of the PfP Consortium Study Group Regional Stability in the South Caucasus, “What a New European Security Deal” could mean for the South Caucasus, 14/2018, pp. 47-53. Available at: https://www.academia.edu/37852657/What_a_New_European_Security_Deal_could_mean_for_the_South_Caucasus (Accessed: 29 May 2025).
- Saqib, N.U. & Naazer, M.A. (2023). Dynamics of regional integration in Central Asia: A case study of Belt and Road Initiative. *Journal of South Asian Studies*, 11(3), pp. 287-298. Available at: <https://www.esciencepress.net/journals/index.php/JSAS/article/view/4981> (Accessed: 28 April 2025).
- Shokri, U. (2024). *Geopolitical Rivalries in the South Caucasus: Evaluating the Aras Corridor as an Alternative to Zangezur*. Trends Research. Available at: <https://trendsresearch.org/insight/geopolitical-rivalries-in-the-south-caucasus-evaluating-the-aras-corridor-as-an-alternative-to-zangezur/> (Accessed: 29 May 2025).
- Stokenberga, A., Morales Sarriera, J., Sekerinska, L., Ferrarini, L.R., Raffo, V.I., Schiro, J., Comini, N., Spinelli, L., Balestro, F. (2024). *Corridors for Development and Growth*. Washington, D.C.: World Bank Group. Available at: <http://documents.worldbank.org/curated/en/099101524184531877> (Accessed: 28 April 2025).
- Talibov, A.M. & Hashimov, E.G. (2024). Vehicle transport cost calculation method. Current directions of development of information and communication technologies and control tools, Proceedings of the 14th International Scientific and Technical Conference, Vol. 2, pp. 3-6.
- Talibov, A.M., Hashimov, E.G., Sabziev, E.N., Pashayev, A.B. (2023). On the optimal placement of logistics centers. *Informatics and Control Problems*, 43(2), pp. 51–58. <https://doi.org/10.54381/icp.2023.2.07> (Accessed: 21 April 2025).
- Talibov, A.M., Sabziev, E.N., Pashayev, A.B. & Hashimov, E.G. (2023). Optimal placement of logistics centers in the Republic of Azerbaijan. *2nd International Conference on Problems of Logistics, Management and Operation in The East-West Transport Corridor (PLMO 2023)*, Baku, 24-26 May 2023. Available at: <https://plmo.cyber.az/2023/papers/20.pdf> (Accessed: 17 March 2025).
- Teo, H.C., Lechner, A.M., Walton, G.W., Chan, F.K.S., Cheshmehzangi, A., Tan-Mullins, M., Chan, H.K., Sternberg, T., Campos-Arceiz, A. (2019). Environmental impacts of infrastructure development under the Belt and Road Initiative. *Environments*, 6(6), p. 72. <https://doi.org/10.3390/environments6060072> (Accessed: 23 March 2025).

Military Operations for Law Enforcement. Joint Operation of the Army Special Forces Command and the Police during the “Nemangkawi” Operation in Papua 2018

Військові операції з підтримання правопорядку. Спільна операція Командування сил спеціального призначення армії та поліції під час операції “Немангкаві” в Папуа, 2018 рік

Mhd. Halkis ^A

Corresponding author: Lecturer, Faculty of Law, e-mail: halkis@unsurya.ac.id

Ida Bagus, Y.S. ^B

Deputy Commander of the Action Task Force during the “Nemangkawi” Operation, e-mail: yusanegara@gmail.com

Мхд. Халкіс ^A

Corresponding author: Викладач, факультет права, e-mail: halkis@unsurya.ac.id

Іда Багус, Ю. С. ^B

Заступник командира оперативної групи дій під час операції “Немангкаві”, e-mail: yusanegara@gmail.com

^A Університет Діргхантари Маршала Сур'ядгарми, Індонезія

^B Deputy Commander of the Action Task Force during the Nemangkawi Operation, Papua

^A Університет Діргхантари Маршала Сур'ядгарми, Індонезія

^B Командування Сил спеціальних операцій армії, Індонезія

Received: July 11, 2025 | Revised: August 09, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.2>

Purpose. to analyze the strategy and tactics of the Indonesian Army Special Forces Command (Kopassus) within the Nemangkawi Task Force during joint operations with the National Police of Indonesia, focusing on counterinsurgency measures against the Papuan separatist armed group (KKSБ).

Method. The research employs a qualitative approach based on a collective case study method. Data sources include official documents, academic publications, interviews with task force members, and analytical materials concerning the activities of KKSБ. The analysis covers the three operational phases of the Nemangkawi Task Force (2018–2022).

Findings. The results demonstrate that KKSБ posed a significant threat to Indonesian sovereignty by employing violent tactics such as killings, ambushes, hostage-taking, and propaganda about alleged human rights violations. Kopassus involvement initially improved operational effectiveness, though results declined as KKSБ adapted its strategies. The dual nature of the operations—military and law enforcement—required high-level coordination between the army and the police. Weaknesses included limited trust from the local population, civilian casualties, and KKSБ's effective international propaganda efforts.

Practical implications. The findings can be applied to improve joint army–police counterinsurgency operations, design personnel training models to minimize losses, and strengthen information policies against separatist propaganda. This case may also serve as a practical model for military education institutions in Indonesia and other countries facing similar challenges.

Originality/value. The article provides one of the few comprehensive examinations of the Nemangkawi Operation as an example of hybrid military–law enforcement activity. It contributes to the understanding of counterinsurgency operations in Southeast Asia and offers new insights into the integration of military and police strategies in combating separatism.

Paper type. Applied nature.

Мета дослідження. аналіз стратегії та тактики Командування сил спеціальних операцій армії Індонезії (Kopassus) у складі оперативної групи «Немангкаві» під час спільних операцій із Національною поліцією, спрямованих на боротьбу з повстанськими угрупованнями (KKSБ) у Папуа.

Метод дослідження. застосовано якісний метод дослідження із використанням підходу колективного *case study*. Джерельну базу становили офіційні документи, наукові публікації, інтерв'ю з учасниками операцій та аналітичні матеріали щодо діяльності KKSБ. Методологія ґрунтувалася на аналізі досвіду проведення трьох фаз операції «Немангкаві» (2018–2022 рр.).

Результати дослідження. Встановлено, що KKSБ становить реальну загрозу суверенітету Індонезії, використовуючи терористичні методи: убивства, напади на військові пости, захоплення заручників, пропаганду про «порушення прав людини». Доведено, що участь Kopassus у складі оперативної групи підвищила ефективність правоохоронних операцій на початкових етапах, але у подальшому результативність знижувалася через адаптацію тактики KKSБ.

Практична цінність дослідження. Результати можуть бути використані: для вдосконалення спільних дій армії та поліції у контрповстанських операціях; для розробки моделей підготовки персоналу та стратегії зменшення втрат; для посилення інформаційної політики проти пропаганди сепаратистів; як практичний кейс для військових навчальних закладів Індонезії та інших країн, що мають подібні виклики.

Цінність дослідження. Стаття є однією з небагатьох робіт, що комплексно описує досвід операції «Немангкаві» як приклад гібридної військово-поліцейської діяльності. Дослідження розширює знання про специфіку контрповстанських операцій у Південно-Східній Азії, які залишаються маловисвітленими в міжнародній літературі.

Тип статті. Прикладного характеру.

Key words: counterinsurgency, Nemangkawi Operation, Kopassus, law enforcement, Papua conflict, hybrid threats.

Ключові слова: боротьба з повстанцями, операція Немангкаві, Копассус, правоохоронні органи, конфлікт у Папуа, гібридні загрози.

Introduction

The Papuan separatist movement, in legal terminology, is referred to as the Armed Criminal Separatist Group (KKSBB Papua). To address the increasing intensity of KKSBB activities in 2018, the Government of Indonesia established a Special Law Enforcement Task Force composed of the Indonesian National Police and the Indonesian National Armed Forces (TNI) (Ikhsal, 2021). Task Force Nemangkawi 1 managed to disrupt KKSBB operations by overrunning seven remote jungle bases, neutralizing several key figures, and seizing weapons. For several months thereafter, the overall security situation in Papua improved. However, KKSBB soon resumed active operations, targeting both security forces and civilians (Gumelar & Nachrawi, 2022), resulting in increased personnel and material losses on the part of the Task Force. The strategy and tactics used by Nemangkawi 1 did not achieve the same level of success in subsequent phases, highlighting the need for more effective strategic adjustments to safeguard the sovereignty of the Republic of Indonesia (NKRI) (Gumelar & Nachrawi, 2022).

KKSBB Papua, also known as the Free Papua Movement (OPM), was formed in 1963 (Febrianti et al., 2019). Its forerunner was the Papua Volunteer Corps (PVC), established by the Dutch to resist Indonesian military operations in West Irian. Trained by the Dutch army, the PVC fought against Indonesia during Operation Trikora (Ervianto, 2019). The PVC, educated and equipped by the Dutch, rejected the results of the Act of Free Choice (Pepera), which had been internationally recognized by the United Nations (Mhd, 2020).

On July 1, 1971, Seth Jafeth Roemkoreem and Jacob Hendrik Prai declared the independence of West Papua, raising the Morning Star flag and singing the anthem "*O my land Papua*" (Herlambang, 2020). On March 26, 1973, the OPM established the West Papua National Liberation Army (TPNPB), and a few years later Goliath Tabuni was appointed Commander-in-Chief with the rank of General. OPM militants repeatedly created security disturbances. In 1976 they threatened PT Freeport Indonesia by cutting slurry and fuel pipelines, disrupting telephone and power lines, and setting fire to warehouses and facilities. In 1982, OPM formed the Revolutionary Council (OPMRC) under Moses Woror, which sought independence through international diplomacy via non-aligned forums, the South Pacific, and ASEAN (Damarjati, 2019). At the political level, OPM was represented abroad by Benny Wenda, who obtained British citizenship and resided in Oxford despite lacking support from the military wing TPNPB.

The coexistence of violent insurgency and political separatist movements poses a real threat to Indonesia's territorial integrity. Such insurgency requires counterinsurgency operations (Wibowo et al., 2011). While the use of the term OPM (Free Papua Organization) carries diplomatic advantages for separatists, the Indonesian authorities sought to diminish its international legitimacy by replacing it with the label Armed Criminal Group (KKB), though this limited TNI's legal scope of involvement.

In 2017, Coordinating Minister for Political, Legal, and Security Affairs Wiranto introduced a new designation: the Armed Criminal Separatist Group (KKSBB) (Putra, 2017). According to Wiranto, this unified terminology replaced the previous labels—Armed Criminal Group (KKB) and Free Papua Organization (OPM). KKSBB refers to groups that commit crimes, terrorize, and harass the population using firearms, thereby engaging in insurgency or separatist activities aimed at secession from Indonesia (Kominfo, 2019). This terminology provided a legal framework for TNI involvement in countering armed violence in Papua.

On August 2018, the TNI Commander and the Chief of Police established a Special Joint Task Force (Satgasus TNI–Polri) named Nemangkawi, with the primary mission of conducting law enforcement, intelligence, and territorial operations. The Task Force operated from July 23, 2018, throughout Papua Province to support law enforcement and safeguard security stability.

As its name suggests, the Task Force consisted of both TNI and Police elements under the

command of the Indonesian National Police Chief. Each element was organized into operational commands comprising several task forces. The organizational structure of the Nemangkawi Task Force is illustrated in the following figure.

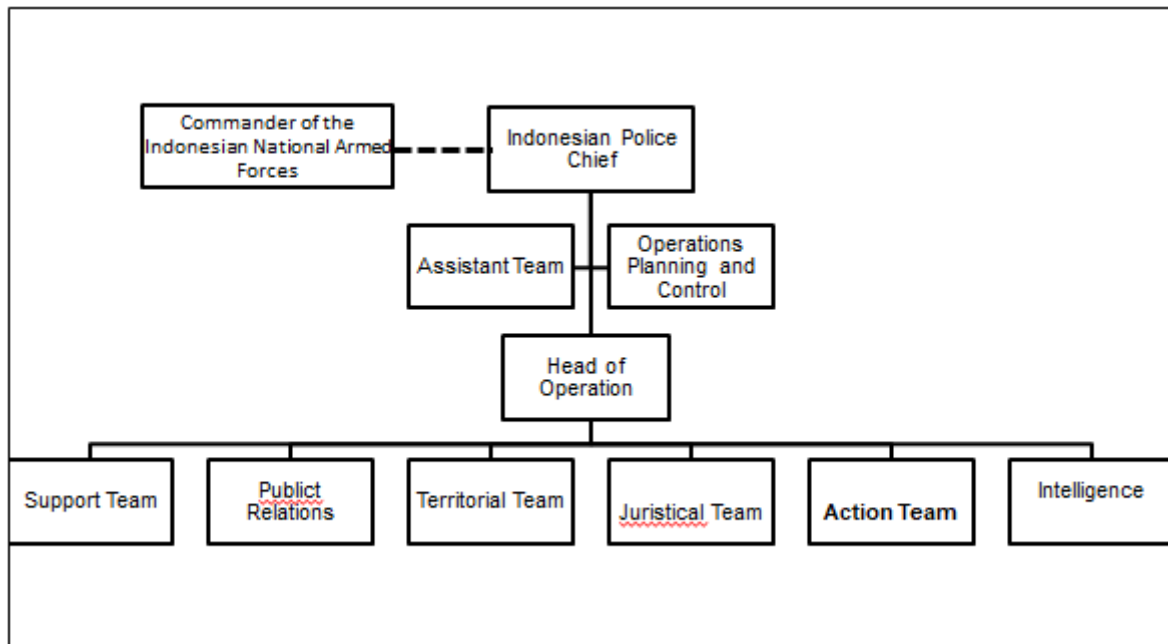


Figure 1 – Structure Organization Nemangkawi

Source: processed by the researcher (2021)

Each operational command (Koops) of both the TNI and the Police has task units such as Task Force Support, Territorial, Public Relations, Legal, Operations, and Intelligence. In carrying out field activities, these units may work jointly or conduct separate operations according to the agreements made in TNI–Polri coordination meetings. Personnel in TNI Koops primarily originate from the Special Forces units. The organizational structure is not fixed; it may be adjusted in response to evolving operational needs. Nemangkawi 1 and Nemangkawi 2 completed their assignments, and as of June 2020, Nemangkawi 3 was conducting its mission in Papua.

Before deployment, personnel assigned to Task Force Nemangkawi underwent several preparatory stages, including selection, organization, and training. During the selection phase, candidates submitted by Special Forces units were evaluated for health, physical fitness, psychological stability, and mental resilience. Personnel deemed fit for duty were classified as ready, while those with limitations were reassigned according to the standards and needs of the Task Force. All personnel were assigned based on their specialization and skills and attended a 12-day training program at the Kopassus Education and Training Center (Pusdiklatpassus) before deployment to Papua.

Theoretical background

Before proceeding further, it is essential to review previous studies of similar incidents conducted in different contexts and time periods. Examining these works enriches understanding and increases the effectiveness of the present research. The results also provide meaningful contributions that can be more widely applied and positively impact the units that rely on such findings.

The first relevant study was conducted by Mohd Farid bin Abd Hamid in 2018, entitled *“Counterinsurgency Operations by the Malaysian Army in Response to Communist Party Threats during the Second Emergency (1968–1989) to Achieve National Security.”* This study analyzed how the Malaysian government confronted the insurgency of the Communist Party of Malaya. The

rebellion employed guerrilla warfare strategies, attempting to compensate for weaknesses by mobilizing resources and local support against the legitimate government. However, Malaysia implemented the KESBAN approach, which successfully countered the insurgency by combining military operations to pursue rebel groups with civic programs aimed at separating insurgents from the population and winning the hearts and minds of the people (Hamid, 2018). This research is relevant to the present study because it provides lessons on how Task Force Nemangkawi established operational success standards and used them to prepare troops for effective missions.

The second study was conducted by Darman Fauzan Dhahir in 2019, entitled *“The Image of Indonesia in OPM Propaganda: Cases of Assaults on Civilians in Nduga Regency.”* This work examined how the Free Papua Movement (OPM) carried out violent attacks against both indigenous Papuans and migrants, as well as security forces, and then manipulated these incidents through propaganda by reversing the facts on the ground (Dhahir, 2019). KKSBB sought to portray the Indonesian government as committing human rights violations by distributing photos of victims of armed violence. They also exploited the misconduct of careless security personnel and used historically symbolic dates to attract public attention. This research is relevant for understanding how the Nemangkawi Task Force anticipated propaganda and patterns of OPM/KKSBB activity, enabling the Task Force to design training and preventive measures (Dhahir, 2019).

The third relevant study was conducted by Georgy Mishael, Joko Setiyono, and Soekotjo Hardiwinoto in 2016, entitled *“The Policy of the Indonesian National Armed Forces in Operations Against the Free Papua Organization from the Perspective of International Humanitarian Law.”* This study examined how Indonesia’s military actions in suppressing OPM armed violence complied with legal frameworks, particularly Law No. 34 of 2004, Article 7(2), concerning the armed resolution of separatist movements (Mishael et al., 2016). The 1949 Geneva Conventions, ratified by Indonesia through Law No. 59 of 1958, provide legal authority for Indonesia to conduct military operations against OPM, while also requiring adherence to humanitarian law. Since the Papuan insurgency is strongly associated with alleged human rights violations, this study is highly relevant to the mental and legal preparedness of soldiers assigned to the Task Force, ensuring that they operate within the law and avoid human rights abuses (Mishael et al., 2016).

Data and methods

According to Sugiyono’s theory (2011), the researchers employed a qualitative research method. One approach within qualitative research is the collective case study, which examines events that occur during specific operations—in this case, the Nemangkawi operation. A case study is defined as a particular event bounded by context, although the distinction between the event and its context is often only partially clear. This study was conducted within the Special Forces Unit, focusing on the personnel and preparation of the Nemangkawi Task Force.

The research subjects were personnel involved in preparing the TNI Operational Command under the Nemangkawi Task Force. The selected informants were task force members who directly participated in field operations and experienced the outcomes of the unit’s activities. These included the Commander of the Operational Command Task Unit of the Nemangkawi Task Force, the Commander of the Field Action Task Force under the TNI Koops Nemangkawi, and the Kopassus Operations Commander, who played a role in planning and preparing the TNI Operational Command integrated into the Nemangkawi Task Force.

Results

1. Actual Threat of KKSBB to the Sovereignty of the Republic of Indonesia (NKRI)

The threats faced today include military, non-military, and hybrid threats that are expected to continue in the coming years, originating both domestically and from abroad (RI, 2015). Among the most significant threats are armed insurgency and armed separatism. An armed insurgency seeks

to oppose or overthrow a legitimate government. In the case of Papua, the persistent actions of KKSB, which repeatedly carry out armed attacks and create public unrest, can even attract international attention. This situation threatens the integrity and sovereignty of the Republic of Indonesia. If the state fails to confront and resolve KKSB actions, it could signal that Indonesia's sovereignty over Papua is weakened, potentially leading to the detachment of Papua from the unitary framework of NKRI.

The threat of armed separatism is closely related to armed rebellion, with the main difference lying in the ultimate goal. Separatist movements aim to break away from the Republic of Indonesia, seeking sovereignty and independence for a particular region or community. Such movements are usually driven by nationalism or religious motivations.

In responding to threats from KKSB, close attention must also be paid to proxy wars, in which external actors may finance and support KKSB activities for their own national interests. Addressing this challenge requires coordinated operations by the security forces as well as the participation of all components of the nation. The roots of separatism stem from racial differences, economic and social disparities, uneven development, and efforts to marginalize or discredit the indigenous population. These factors have fueled the separatist sentiment underlying KKSB's political movement.

Armed violence has persisted for decades. Since Papua's reintegration into Indonesia, KKSB's armed actions have continuously disturbed public order. In 1970, KKSB—also known as the Free Papua Movement (OPM)—formed the National Liberation Army (TPN). Their separatist activities escalated when, on July 1, 1971, they declared the establishment of the Republic of West Papua. They planned to announce this declaration internationally in July 1972, but the attempt failed due to a lack of community support. Subsequently, Martin Tabu, a TPN/OPM figure, launched an attack on a TNI post in Senggigi, resulting in the deaths of one member of Kodim 1701 and two members of Battalion 753, with four weapons seized. In 1973, Marcus Sam led further attacks, followed by Obert Tabuni in Jayapura in 1974, operations in Serui in 1975, and additional sporadic incursions in Jayapura in 1976 under the leadership of Alex Derey and Jelly Ellaby.

Even after the Nemangkawi law enforcement operation was launched in 2018, KKSB's violent actions have not ceased. Numerous armed incidents have caused casualties among both security forces and indigenous Papuan civilians. Several of KKSB's actions following the Nemangkawi operation are summarized in the following table.

Based on the data above, the acts of armed violence carried out by KKSB clearly have both political and psychological objectives. They are intended to weaken the morale of security officers, who are intimidated one by one. From the perspective of the Police, these are criminal acts; however, the broader objective pursued by KKSB directly threatens national sovereignty. Their methods of action are violent, including attacks on officers, the killing of civilians, hostage-taking, and the symbolic raising of the Morning Star flag.

KKSB continuously escalates its activities to demonstrate its existence, while remaining fragmented into groups with differing agendas. With relatively small forces, they attack poorly defended outposts or security personnel caught off guard. They also kill civilians suspected of being spies or undercover officers. Up to the present, KKSB continues to operate by exploiting time in a manner typical of insurgency warfare—deliberately prolonging conflict in order to exhaust security forces and erode their morale. This protracted strategy creates opportunities for soldiers to become negligent, commit mistakes, and suffer declining combat spirit. Prolonged counterinsurgency operations also place a heavy burden on state finances and deplete human resources.

Table 1 – Threat current KKSb post Nemangkawi

#	TIME	THE PLACE	INCIDENT	DESCRIPTION
1	June 22, 2018	Regency Kenya, Papua	KKSb-shot aircraft, Trigana water, and Dimonim water transport bromob	1 pilot was wounded and shot in the back
2	October 2018	Mapenduma, Regency. guess, Papua	16 people hostage, teacher, and a health authority accused of eye Eye	Hostage released after the negation Custom
3	December 1, 2018	Trans-road Papua, Regency Indonesia Nduga,	Massacre of workers at Street Trans Papua PT Istaka site	31 Road Workers Killed Slaughtered KKSb
4	January 18, 2019	District Yambi, Regency Peak Jaya, Papua	Shoot contact TNI/Polri with KKSb group Lekagak Telenggen	1 TNI Fall
5	August 12 2019	Kampung Banish, Kab Peak, Papua	Hostage	1 Police Fall
6	September 16, 2019	Habeme, Jayawijaya Regency , Papua	Attack on member TNI by Group Egianus Kogoya	1 TNI killed
7	Tuesday, September 17 2019	Olenki Village, North Ilaga District, Puncak Regency, Papua	Shooting to Public Ilaga by KKSb	3 inhabitant civil dead
8	December 18, 2019	Intan Jaya, Papua	Contact TNI Police with KKSb	2 TNI Fall
9	September 17, 2020	Hitadipa, district of Intan Jaya Papua	Attack on TNI	2 TNI Fall
10	Friday, 4 June 2021	Nipuralome, District Ilaga, Regency Peak, Papua	Head Village Kago, Denis Wanda, and 9 OAP others report incident shooting against 6 OAP	Three real people dead in Papua
11	December 1, 2021	push, Papua West	Factory Burn P.T. Get up Wood Irian as an action denial development KKSb	nothing victim
12	Thursday, January 27, 2022	Ilaga districts Peak, Papua	Shoot contact TNI/Polri with Numbuk Group Telenggen	2 TNI Fall

Source: processed by the researcher (2011)

2. Threat Potential KKSb to Sovereignty NKRI

The implementation of law enforcement in Papua has not been fully effective because KKSb still retains significant strength and continues to act violently, both militarily and politically. Persistent acts of violence, left unresolved, undermine the authority of the Indonesian government in the eyes of the Papuan population, the wider Indonesian public, and even the international community. The longer the Papua issue remains unaddressed, the greater the threat posed by KKSb becomes. At the same time, KKSb's political wing exploits the government's weaknesses for propaganda to seek foreign support.

According to Yusvitasari (2019), three elements determine whether a separatist group is likely to gain recognition: (1) the existence of a well-organized structure, (2) the use of clear symbolic identifiers, and (3) dominance over a particular territorial area. In this regard, KKSb has established regional war commands (*Kodap*) led by Commander-in-Chief Goliath Tabuni, uses the Morning Star

flag as its symbol, and maintains a presence across almost all regions of Papua.

On the political front, KKSBB consistently maneuvers to exploit weaknesses in Indonesian governance. Public distrust in law enforcement in Papua, persistent economic underdevelopment in the highlands, and ongoing human rights concerns remain potential flashpoints that could one day explode into a major crisis. Declining public confidence in government erodes state authority and threatens national sovereignty. KKSBB's political wing conducts propaganda both domestically and internationally, and this requires continuous monitoring.

Since Papua's transfer to Indonesia by the United Nations Temporary Executive Authority (UNTEA) on May 1, 1963, political turmoil in Papua has never ceased. Numerous organizations emerged, including Genapa (Gerakan Nasionalis Papua), Panapa (Partai Nasional Papua), OPM (Organisasi Papua Merdeka), PPM (Partai Papua Merdeka), GPM (Gerakan Papua Merdeka), IPARI (Ikatan Papua Anti Republik Indonesia), SAMPARI (Semangat Angkatan Muda Papua Anti Republik Indonesia), IRPARI (Ikut Republik Papua Anti Republik Indonesia), and PPGPM (Pimpinan Pusat Gerakan Papua Merdeka).

These organizations maintained activities not only within Papua but also abroad, such as in the Netherlands (Marcus Kaisepo), Senegal (Ben Tanggahama), Papua New Guinea (Eli Mariem), and Sweden (Yakop H. Pray). Their overseas campaigns spread anti-Indonesian propaganda and sought international sympathy by manipulating facts in order to win United Nations support (Operation to Crush the Separatist Movement in Papua 1965–1991, 2018).

Following the reform era of 1998, KKSBB's political activities were increasingly coordinated under Benny Wenda, a convict in the Abepura police station arson case. He later became active under the United Liberation Movement for West Papua (ULMWP). This organization gathers and disseminates reports accusing Indonesia of human rights violations. Benny Wenda originally acted through the *Koteka Community Consultative Council* (Denmak), which advocated for traditional Papuan rights and rejected Indonesia's special autonomy framework.

On June 6, 2002, Wenda was arrested in Jayapura for involvement in the police station attack. On October 27, 2002, he escaped from prison with the help of a European NGO, fled to Papua New Guinea, and eventually obtained political asylum in the United Kingdom with the support of a New Zealand NGO (Catherine Delahunty). In 2011, Indonesia issued a red notice against him, but it was revoked by Interpol after legal intervention from an Australian lawyer.

Wenda's major international initiatives include establishing the *International Parliamentarians for West Papua (IPWP)*, launched in the UK Parliament in London on October 15, 2008, as a cornerstone of global advocacy against Indonesia's sovereignty in Papua. On December 6, 2014, he co-founded the ULMWP, which coordinates anti-Indonesian activities abroad. On February 4, 2015, Wenda registered West Papua with the *Melanesian Spearhead Group (MSG)* and the *African, Caribbean, and Pacific Group of States (ACP)* in hopes of gaining recognition of Papuan sovereignty. In 2017, nine New Zealand parliamentarians supported a petition advocating for West Papua. Domestically, Wenda maintains links with the *Papua National Committee (KNPB)* and the *Federal Republic of West Papua (NFRPB)* to mobilize Papuan support and highlight alleged Indonesian human rights violations.

The diplomatic strategy relies on KNPB and NFRPB to organize illegal referendums and generate human rights narratives, which Wenda then amplifies internationally through IPWP and ULMWP. Through MSG and ACP platforms, he seeks to raise the Papua issue in international forums, including the United Nations. Indonesia's defense diplomacy must therefore remain vigilant in countering these international efforts (Mhd, 2020).

Between 2014 and 2017, several states and organizations voiced support for West Papuan independence. In March 2014, New Zealand Māori women staged a performance entitled "*Oceania Interrupted Action 3: Free West Papua*." In May 2016, the Westminster Declaration was signed during an IPWP session at the UK Parliament. In December 2016, the Prime Minister of Vanuatu

called for an end to human rights violations against indigenous Papuans. In March 2017, seven Pacific states—Vanuatu, Tonga, Palau, Tuvalu, Marshall Islands, Nauru, and Solomon Islands—accused Indonesia of human rights violations at the UN Human Rights Council in Geneva. In May 2017, eleven members of New Zealand's Green Party signed the Westminister Declaration (tiro.id, 2017).

Conclusion

The strategy of the Special Forces in preparing Task Force Nemangkawi for law enforcement operations in Papua is essential for safeguarding Indonesia's sovereignty. KKSBB's actual and potential threats to the sovereignty of the Republic of Indonesia (NKRI) remain evident in Papua. Without proper handling, these threats could seriously endanger national unity and even risk detaching Papua from the NKRI. KKSBB's armed violence against the Papuan community and security apparatus—including murders, robberies, rapes, hostage-taking, and attacks on posts—has caused significant losses for the Indonesian state. Infrastructure development in Papua has been severely hampered, as workers are afraid to continue construction, while completed projects such as buildings, roads, and bridges are often damaged by KKSBB attacks.

At the same time, potential threats persist in the form of declining public trust in law enforcement, deep economic inequality, and recurring allegations of human rights violations, all of which undermine government authority in the eyes of Papuans. Public fear for personal security further fuels KKSBB propaganda, which can be exploited internationally to intensify pressure for Papuan independence.

The strategy for preparing the TNI Operations Command in support of Task Force Nemangkawi to safeguard the sovereignty of NKRI can be analyzed in terms of goals, resources, and methods.

- **Goals (Ends):** To ensure that each replacement of the Task Force can carry out its duties effectively, raise awareness among personnel, and face KKSBB separatist actions with minimal losses among both Task Force members and civilians.
- **Resources (Means):** The Task Force is composed of Kopassus personnel with operational experience and knowledge of Papua. They are equipped with unit-level and individual gear suited to the operational environment, supported by education and training centers, and reinforced by specialized units outside Kopassus.
- **Methods (Ways):** Synchronization of Kopassus training activities with pre-deployment preparation, allowing sufficient time for comprehensive readiness to address all forms of threats in the operational area. This includes careful selection of personnel, determination of operational areas, and provision of intelligence data to be used in practical training.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

- Damarjati, D. (2019). Benny Wenda's trail: Escape from prison, wanted by Interpol, live in England. *Detik News*.
- Dhahir, D. F. (2019). Images of Indonesia in propaganda of Free Papua Movement: Case of attacks on civilians in Nduga Regency. *Journal of Communication Research and Public Opinion*, 23(3), 1–20.
- Ervianto, T. (2019). Measuring the threat strength of KKSBB-OPM (Part-1). *Between Megapolitan*.

- Febrianti, S. W., Arum, A. S., & Dermawan, W. (2019). Resolution of the internal conflict between the Government of Indonesia and the separatism movement in Papua through the horse-trading mechanism. *Journal of the Society*, 7(2), 83–100.
- Gumelar, I., & Nachrawi, G. (2022). Legal protection for TNI members under the human rights law: A case study of the Free Papua Movement separatist organization. *Journal of Social Sciences and Education*, 6(2), 4146–4166.
- Hamid, M. F. bin A. (2018). Operation against insurgency by the Malaysian Army when facing the threat of the Malayan Communist Party in the Second Emergency (1968–1989) in order to achieve national security. *Journal of Defense & National Defense*, 1(1), 1–28.
- Herlambang, A. (2020). *The Papuan conflict* (pp. 1–66). Academia.edu. <https://www.academia.edu/>
- Ikhbal, A. M. (2021). TNI-Polri solid guard the land of Papua from the KKB through the Nemangkawi Task Force. *INewsPapua.id*.
- Kominfo. (2019). Monthly hoax issue report for March 2019. *Directorate of Information Technology Applications, Directorate General of Information Technology Applications*.
- Mhd, H. (2020). The implementation of Penta Helix counterinsurgency (COIN) strategic model in reconstructing special autonomy for Papua. *Society*, 8(1), 234–248. <https://doi.org/10.33019/society.v8i1.182>
- Mishaal, G., Setiyono, J., & Hardiwinoto, S. (2016). Military operations policy of the Indonesian National Armed Forces against Free Papua Organizations in the perspective of international humanitarian law. *Law and Justice*, 5(41), 1–13.
- Putra, P. M. S. (2017). Coordinating Minister for Political, Legal, and Security Affairs changes name of armed group in Papua to KKSBB. *Liputan6.com*.
- Republik Indonesia, Kementerian Pertahanan. (2015). *Defense white paper*.
- Wibowo, E. Y., Hartono, & Purwanto, T. H. (2011). Determining attack paths in operations against insurgency in urban areas using remote sensing data and GIS. *Indonesian Geography Magazine*, 25(1), 15–24.
- Yusvitasari, D. (2019). Analysis of the validity of an international treaty under international law: A case study of the Helsinki Agreement between GAM and Indonesia. *Journal of Pancasila and Citizenship Education Communication Media*, 1(2), 46–62. <https://doi.org/10.23887/jmpppkn.v1i2.46>

Список використаних джерел

- Damarjati, D. (2019). Benny Wenda's trail: Escape from prison, wanted by Interpol, live in England. *Detik News*.
- Dhahir, D. F. (2019). Images of Indonesia in propaganda of Free Papua Movement: Case of attacks on civilians in Nduga Regency. *Journal of Communication Research and Public Opinion*, 23(3), 1–20.
- Ervianto, T. (2019). Measuring the threat strength of KKSBB-OPM (Part-1). *Between Megapolitan*.
- Febrianti, S. W., Arum, A. S., & Dermawan, W. (2019). Resolution of the internal conflict between the Government of Indonesia and the separatism movement in Papua through the horse-trading mechanism. *Journal of the Society*, 7(2), 83–100.
- Gumelar, I., & Nachrawi, G. (2022). Legal protection for TNI members under the human rights law: A case study of the Free Papua Movement separatist organization. *Journal of Social Sciences and Education*, 6(2), 4146–4166.
- Hamid, M. F. bin A. (2018). Operation against insurgency by the Malaysian Army when facing the threat of the Malayan Communist Party in the Second Emergency (1968–1989) in order to achieve national security. *Journal of Defense & National Defense*, 1(1), 1–28.
- Herlambang, A. (2020). *The Papuan conflict* (pp. 1–66). Academia.edu. <https://www.academia.edu/>

- Ikhbal, A. M. (2021). TNI-Polri solid guard the land of Papua from the KKB through the Nemangkawi Task Force. *INewsPapua.id*.
- Kominfo. (2019). Monthly hoax issue report for March 2019. *Directorate of Information Technology Applications, Directorate General of Information Technology Applications*.
- Mhd, H. (2020). The implementation of Penta Helix counterinsurgency (COIN) strategic model in reconstructing special autonomy for Papua. *Society*, 8(1), 234–248. <https://doi.org/10.33019/society.v8i1.182>
- Mishael, G., Setiyono, J., & Hardiwinoto, S. (2016). Military operations policy of the Indonesian National Armed Forces against Free Papua Organizations in the perspective of international humanitarian law. *Law and Justice*, 5(41), 1–13.
- Putra, P. M. S. (2017). Coordinating Minister for Political, Legal, and Security Affairs changes name of armed group in Papua to KKSB. *Liputan6.com*.
- Republik Indonesia, Kementerian Pertahanan. (2015). *Defense white paper*.
- Wibowo, E. Y., Hartono, & Purwanto, T. H. (2011). Determining attack paths in operations against insurgency in urban areas using remote sensing data and GIS. *Indonesian Geography Magazine*, 25(1), 15–24.
- Yusvitasari, D. (2019). Analysis of the validity of an international treaty under international law: A case study of the Helsinki Agreement between GAM and Indonesia. *Journal of Pancasila and Citizenship Education Communication Media*, 1(2), 46–62. <https://doi.org/10.23887/jmpppkn.v1i2.46>

Математична модель максимізації значення інтегрального індексу безпеки державного кордону

Mathematical model of maximizing the value of the integral index of state border security

Владислав Шевчук

Vladyslav Shevchuk

старший викладач кафедри прикордонної служби, e-mail: goal_keeper@ukr.net, ORCID: 0000-0001-5583-2160

Senior Lecturer of the Border Guard Service Department, e-mail: goal_keeper@ukr.net, ORCID: 0000-0001-5583-2160

Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький, Україна

Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine

Received: July 30, 2025 | Revised: August 09, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.3>

Мета роботи. Розробити оптимізаційну математичну модель максимізації значення інтегрального індексу безпеки державного кордону.

Метод дослідження. В основу моделі покладено інтегральний індекс безпеки державного кордону (ІІБ) як цільову функцію, яку необхідно максимізувати. Змінними в моделі виступають не самі показники, а керуючі впливи або ресурси, що спрямовуються на покращення цих показників.

Результати дослідження. Розроблено математичну модель максимізації значення інтегрального індексу безпеки державного кордону та реалізовано її у середовищі Matlab.

Теоретична цінність дослідження. Теоретично методика збагачує область математичного моделювання в системах безпеки, демонструючи, як оціночні індекси можна трансформувати в оптимізаційні задачі.

Оригінальність/Цінність дослідження. Новизна полягає у інтеграції оціночної моделі та агрегації цільової функції до специфічного індексу ІІБ з елементами математичного програмування для оптимального розподілу ресурсів у контексті безпеки державного кордону.

Майбутні дослідження. У ході подальших досліджень доцільно опрацювати вхідні дані та розробити програмний продукт для комп'ютерної підтримки.

Тип статті. Теоретична.

Purpose. To develop an optimization mathematical model for maximizing the value of the integral index of state border security.

Method. The model is based on the integral index of state border security (IBS) as an objective function that needs to be maximized. The variables in the model are not the indicators themselves, but the controlling influences or resources aimed at improving these indicators.

Findings. A mathematical model for maximizing the value of the integral security index of the state border was developed and implemented in the Matlab environment.

Theoretical implications. Theoretically, the methodology enriches the field of mathematical modeling in security systems by demonstrating how evaluation indices can be transformed into optimization problems.

Originality/Value. The novelty lies in the integration of the evaluation model and aggregation of the objective function to a specific IIB index with elements of mathematical programming for optimal resource allocation in the context of state border security.

Future research. In the course of further research, it is advisable to process the input data and develop a software product for computer support.

Paper type. Theoretical.

Ключові слова: управління, планування, прийняття рішення, моделювання, підрозділи охорони державного кордону, органи військового управління, оперативно-службова діяльність.

Key words: management, planning, decision-making, modeling, state border protection units, military command bodies, operational and service activities.

Вступ

Традиційні моделі оцінювання стану безпеки державного кордону, як правило, фокусуються на розрахунку поточного стану (наприклад, через індекси ризиків чи ефективності) та рідко включають динамічну оптимізацію під обмеженнями. У документі модель еволюціонує від статичної оцінки до динамічної оптимізації, що дозволяє не лише діагностувати, а й прогнозувати та коригувати рівень безпеки через керуючі впливи (ресурси (X_k)). Більшість відомих моделей оптимізації безпеки кордонів (наприклад, стратегія оптимізації ресурсів СВР США, яка фокусується на штатному персоналі та інфраструктурі, або multi-objective моделі для патрулювання кордонів з використанням теорії ігор) не інтегрують вагові коефіцієнти з нелінійними функціональними залежностями ресурсів від показників. Запропонована модель вводить саме такі залежності ($(P_i = f(X_k))$), що враховують ефект насичення та базуються на реальних даних чи симуляціях, роблячи її більш гнучкою для нелінійних сценаріїв.

У вітчизняній науковій літературі (Андрощук О., Грінченко В. 2021), (Bratko A. та інші, 2021), (Kosevtsov V. та інші 2020), (Братко А. 2023), (Михайлюк Ю. О., Башнянин О. В. 2024) переважають моделі оцінки ризиків (наприклад, моделі протидії контрабандної діяльності чи нелегальної міграції), але рідко зустрічаються комплексні оптимізуючі моделі для ІІБ. Новизна в тому, що методика поєднує експертні ваги (метод аналізу ієрархій) з обмеженнями ресурсів, адаптуючи загальні принципи математичного моделювання до специфіки прикордонної служби України, де ресурси обмежені через геополітичні виклики.

Гібридний підхід надає можливості поєднання статистичних, експертних і симуляційних методів для побудови залежностей робить модель новаторською порівняно з чисто лінійними моделями (наприклад, в оптимізації екосистемних послуг кордонів чи чергової теорії для імміграційного контролю).

Ця новизна обґрунтована відсутністю прямих аналогів у науковій літературі, де оптимізація часто обмежується окремими аспектами (наприклад, патрулюванням чи наявними ресурсами), а не комплексним індексом безпеки.

Теоретичні основи дослідження

Теоретично методика збагачує область математичного моделювання в системах безпеки, демонструючи, як оціночні індекси можна трансформувати в оптимізуючі задачі. Вона розвиває теорію багатокритеріальної оптимізації, інтегруючи вагові коефіцієнти з нелінійними залежностями, що дозволяє враховувати стратегічні пріоритети та ефекти насичення. Це сприяє розвитку теорії прийняття рішень під невизначеністю, особливо в умовах обмежених ресурсів, і може бути узагальнено на інші сфери (наприклад, фінансову чи економічну безпеку). Методика також підкреслює роль гібридних методів (статистика + експертиза + симуляція) для побудови реалістичних моделей, що є внеском у теорію системного аналізу.

Постановка проблеми

Існує потреба у створенні моделі, яка є інструментом для ефективного управління ресурсами в органах та підрозділах охорони державного кордону, дозволяючи обґрунтувати пріоритети фінансування (наприклад, інвестиції в технічні засоби охорони державного кордону та підготовку особового складу), яка б допомогла мінімізувати ризики порушень державного кордону, підвищити оперативність реагування в умовах ускладнення обстановки та оптимізувати бюджетні витрати.

Результати

На основі методики оцінювання стану обстановки на ділянці відповідальності підрозділів охорони державного кордону в умовах її ускладнення, яка описує порядок оцінки стану безпеки кордону, розроблено оптимізаційну математичну модель, мета якої визначити, як найкраще розподілити ресурси для максимізації значення інтегрального індексу безпеки кордону (ІІБ).

Концепція оптимізаційної моделі.

Оптимізаційна модель використовує розрахований Інтегральний індекс безпеки кордону (ІІБ) як цільову функцію, яку необхідно максимізувати. Змінними в моделі виступають не самі показники, а керуючі впливи або ресурси, що спрямовуються на покращення цих показників.

Мета: максимізувати ІІБ за умов обмежених ресурсів:

$$\text{ІІБ} = w_{\text{упр}} \cdot E_{\text{упр}} + w_{\text{оп}} \cdot E_{\text{оп}} \quad (1)$$

Формулювання оптимізаційної моделі.

1. Цільова функція.

Цільова функція повністю базується на моделі. Ми прагнемо максимізувати зважену суму ефективностей:

$$\max(\PiБ) = w_{\text{упр}} \cdot (\sum_{i=1}^n w_i \cdot P_i^{\text{БН}}) + w_{\text{оп}} \cdot (\sum_{j=1}^m w_j \cdot P_j^{\text{ЗОВН}}), \quad (2)$$

де $\{w_{\text{упр}}, w_{\text{оп}}, w_i, w_j\}$ – вагові коефіцієнти, які вважаються константами на етапі оптимізації. Вони визначаються експертно (наприклад, методом аналізу ієрархій) і відображають стратегічні пріоритети.

2. Змінні (керуючі впливи).

Введемо змінні, що позначають обсяг ресурсів, які виділяються на кожен напрямок діяльності. Наприклад:

X_1 – ресурси (наприклад, людино-години, фінанси), виділені на прискорення процесу прийняття рішень (впливає на P_1);

X_2 – ресурси на підвищення кваліфікації аналітиків та планувальників (впливає на P_2);

X_3 – ресурси на закупівлю та використання технічних засобів спостереження (впливає на P_3);

X_4 – ресурси на оснащення груп швидкого реагування (впливає на P_4).

3. Функціональні залежності.

Це найважливіший крок: необхідно встановити, як виділені ресурси (X_k) впливають на значення часткових показників (P_i). Ці залежності, $P_i = f(X_k)$, є основою моделі і можуть бути визначені на основі: статистичного аналізу попередніх періодів; експертних оцінок; результатів імітаційного моделювання.

Приклади залежностей:

Для P_1 (оперативність прийняття рішення) – збільшення ресурсів X_1 на автоматизацію може скорочувати $T_{\text{факт}}$. Залежність може бути нелінійною (ефект насичення).

$$P_1(X_1) = 1 - \frac{T_{\text{факт базовий}} - \Delta T(X_1)}{T_{\text{норм}}}, \quad (3)$$

де $\Delta T(X_1)$ – скорочення часу завдяки ресурсам X_1 .

Для P_3 (результативність протидії): Збільшення ресурсів X_3 на дрони та камери підвищує кількість виявлених порушень $N_{\text{вияв}}$.

$$P_3(X_3) = \frac{N_{\text{вияв базовий}} + \Delta N(X_3)}{N_{\text{спроб}}}, \quad (4)$$

де $\Delta N(X_3)$ – додаткові виявлення завдяки ресурсам X_3 .

4. Обмеження.

Будь-яка система діє в умовах обмежених ресурсів.

Бюджетне обмеження. Сума всіх виділених ресурсів не може перевищувати загальний бюджет B .

$$\sum_{k=1}^K c_k X_k \leq B, \quad (5)$$

де c_k – вартість одиниці ресурсу X_k .

Обмеження за персоналом. Загальна кількість залучених співробітників не може перевищувати штатну чисельність L .

$$\sum_{k=1}^K l_k X_k \leq L, \quad (6)$$

де l_k – кількість персоналу, необхідна для одиниці ресурсу X_k .

Технологічні обмеження. Наприклад, неможливо закупити більше дронів, ніж доступно на ринку.

Етапи практичної реалізації

1. Ідентифікація показників та ресурсів. Скласти повний перелік часткових показників (P_i), які використовуються в моделі, та визначити, які конкретні ресурси або заходи (X_k) на них впливають.

2. Визначення вагових коефіцієнтів. За допомогою експертних методів (наприклад, метод аналізу ієрархій, як зазначено в документі) встановити всі ваги (w).

3. Побудова функціональних залежностей. Зібрати дані та/або залучити експертів для математичного опису залежностей $P_i = f(X_k)$. Це найскладніший етап, що потребує ретельного аналізу.

4. Формулювання обмежень. Чітко визначити кількісні обмеження (бюджет, наявний персонал, часові рамки).

5. Розв'язання задачі. Використовувати спеціалізоване програмне забезпечення для математичного програмування (лінійного або нелінійного, залежно від виду функцій $f(X_k)$) для знаходження оптимального розподілу ресурсів X_k , що максимізує ІІБ.

Аналіз результатів. Ідентифікація показників і ресурсів, визначення ваг, побудова залежностей, формулювання обмежень, розв'язання задачі (за допомогою ПО для математичного програмування) та аналіз результатів.

6. Проаналізувати отриманий оптимальний план розподілу ресурсів та розробити на його основі конкретні управлінські рішення.

Перевага такого підходу полягає в тому, що він перетворює модель з інструменту оцінки в інструмент підтримки прийняття рішень, дозволяючи об'єктивно та кількісно обґрунтовувати пріоритетність фінансування тих чи інших напрямків для найбільш ефективного підвищення безпеки кордону.

Модель орієнтована на стратегічні пріоритети, дозволяючи об'єктивно обґрунтувати інвестиції в напрямки, що дають максимальний ефект для підвищення безпеки кордону.

Математична модель максимізації значення інтегрального індексу безпеки державного кордону реалізована у середовищі Matlab. Приклади розрахунків наведено на рисунках 1–3.

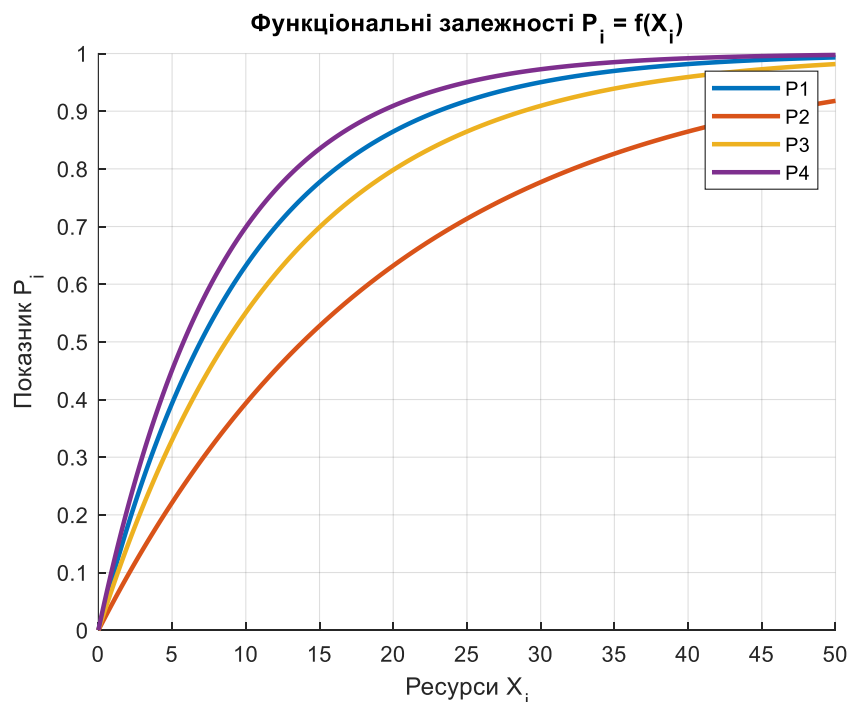


Рисунок 1 – Функціональні залежності показників та ресурсів

Джерело: розроблено автором у Matlab

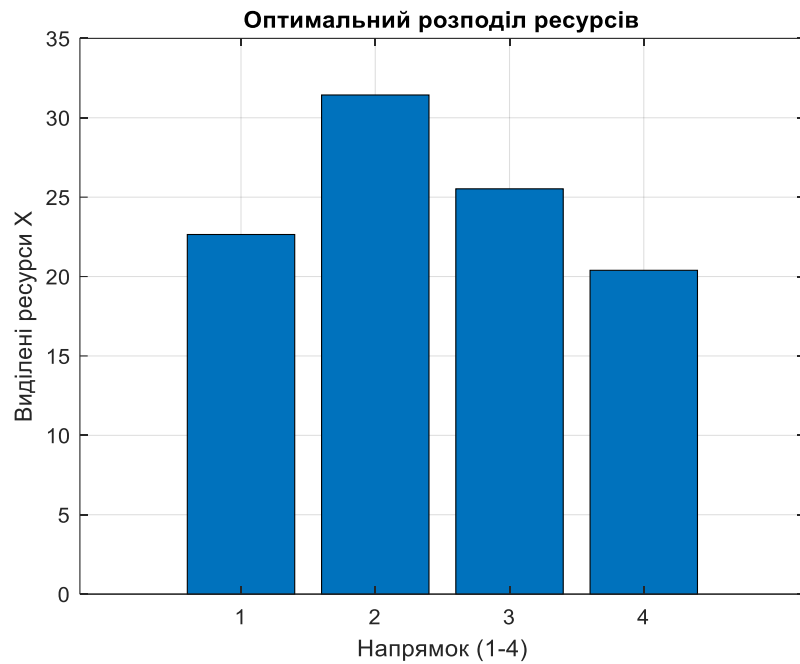


Рисунок 2 – Оптимальний розподіл ресурсів

Джерело: розроблено автором у Matlab

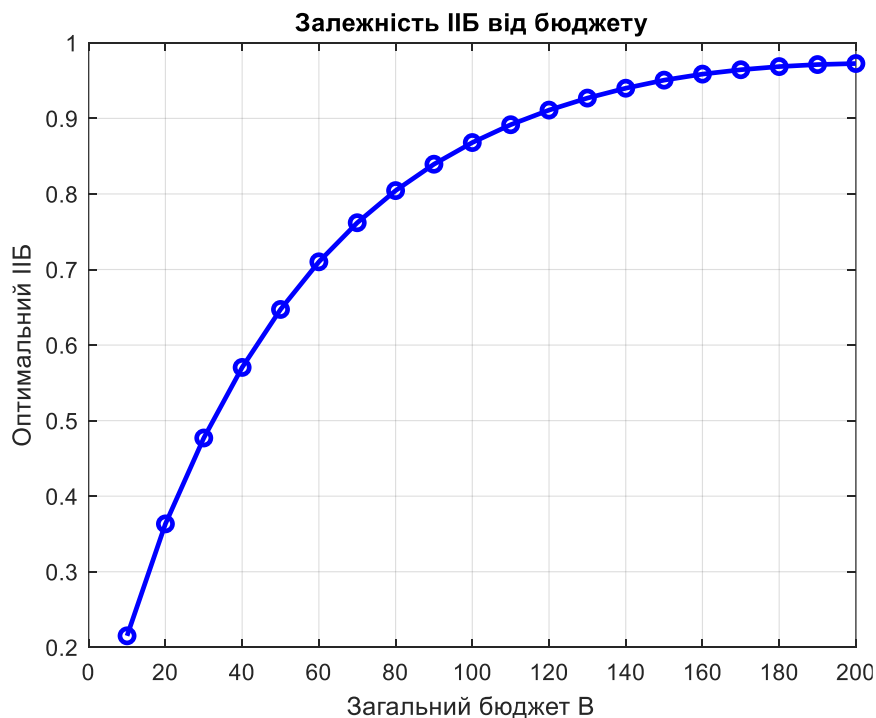


Рисунок 3 – Оптимальний розподіл ресурсів

Джерело: розроблено автором у Matlab

Рекомендації щодо використання.

1. Рекомендується впровадити модель у Державній прикордонній службі України для щорічного планування оперативно-службової діяльності органів та підрозділів охорони державного кордону. Почати з пілотного проекту на конкретній ділянці державного кордону, використовуючи реальні дані для калібрування залежностей $(f(X_k))$.

2. Перед використанням провести статистичний аналіз даних про порушення кордону у минулому та ефективність заходів протидії, а також залучити експертів для визначення ваги і залежностей.

3. Враховувати нелінійність залежностей, тестуючи модель на симуляціях. Якщо обмеження складні, перейти від лінійного до нелінійного програмування.

4. Регулярно оновлювати ваги та залежності на основі нових даних (наприклад, щоквартально). Інтегрувати з GIS-системами для геопросторового аналізу.

5. Проводити тренінги для представників інформаційно-аналітичного забезпечення прикордонної служби з методів оптимізації, щоб забезпечити коректне застосування.

6. Уникати надмірної залежності від експертних оцінок; комбінувати з об'єктивними даними. Якщо ресурси обмежені, почати зі спрощеної версії моделі (лише ключові (X_k)).

Загалом, методика має високий потенціал для підвищення ефективності безпеки державного кордону, але вимагає якісних вхідних даних і комп'ютерної підтримки.

Висновки

Таким чином, розроблена модель є інструментом для ефективного управління ресурсами в органах та підрозділах охорони державного кордону, дозволяючи обґрунтувати пріоритети фінансування (наприклад, інвестиції в технічні засоби охорони державного кордону та підготовку особового складу). Вона допомагає мінімізувати ризики порушень державного кордону, підвищувати оперативність реагування в умовах ускладнення обстановки та оптимізувати бюджет. У контексті України це особливо актуально для посилення безпеки на державному кордоні, в умовах обмеженого фінансування та обмежених ресурсів. Модель надає можливість оптимізувати людські (особового складу) та інженерно-технічні ресурси при проведенні спеціальних заходів (дій) щодо пошуку правопорушників чи плануванні оперативно-службової діяльності у наступному календарному році або іншому періоді). Модель може інтегруватися в системи підтримки прийняття управлінських рішень, зменшуючи суб'єктивність і підвищуючи ефективність на 10–20% (за аналогією з подібними моделями в СППР). Практичне значення також у можливості симуляції сценаріїв (наприклад, що якщо збільшити бюджет на 10%), що полегшує планування. Математична модель є одним із етапів моделі застосування підрозділів охорони державного кордону в умовах ускладнення обстановки.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

- Андрощук О. С., Грінченко В. В. Розробка аналітичного методу аналізу ефективності охорони державного кордону із застосуванням ймовірнісно-статистичного підходу. *Information Processing Systems*. 2021. № 1(164). С. 6–11.
- Bratko A., Bereziuk V., Shevchenko A., Kubetsky Ya., Didyk V., Serkhovets S. Application of simulation modeling means in management decisions-making within the security and defense sector. *Emerging Science Journal*. 2021. Vol. 5, №. 4. P. 521–532. <http://dx.doi.org/10.28991/esj-2021-01294>
- Братко А. В. Методика організації роботи органів управління Державної прикордонної служби України щодо планування оперативно-службової діяльності. *Social development and Security*. 2023. Vol. 13, №. 1. P. 29–37. <https://doi.org/10.33445/sds.2023.13.1.4>

- Kosevtsov V., Telelim M., Lobanov A., Punda Yu. Development and Implementation of the Target Function in the Decision-Making Process in the System of Providing the Military Security of the State. *Eastern-European Journal of Enterprise Technologies*. 2020. № 5 (3(107)). P. 17–23.
- Михайлюк, Ю., & Башнянин, О. (2024). Науково-методичний апарат протидії нелегальній міграції на ділянці відповідальності прикордонного загону. *Social Development and Security*, 14(5), 37-42. <https://doi.org/10.33445/sds.2024.14.5.4>.

References

- Androshchuk O. S., Hrinchenko V. V. Rozrobka analitychnoho metodu analizu efektyvnosti okhorony derzhavnoho kordonu iz zastosuvanniam ymovirnisno-statystychnoho pidkhodu. *Information Processing Systems*. 2021. № 1(164). S. 6–11.
- Bratko A., Bereziuk V., Shevchenko A., Kubetsky Ya., Didyk V., Serkhovets S. Application of simulation modeling means in management decisions-making within the security and defense sector. *Emerging Science Journal*. 2021. Vol. 5, №. 4. R. 521–532. <http://dx.doi.org/10.28991/esj-2021-01294>
- Bratko, A. (2023). The method of organizing the work of the management bodies of the State Border Guard Service of Ukraine regarding the planning of operational and service activities. *Social Development and Security*, 13(1), 29-37. <https://doi.org/10.33445/sds.2023.13.1.4>.
- Kosevtsov V., Telelim M., Lobanov A., Punda Yu. Development and Implementation of the Target Function in the Decision-Making Process in the System of Providing the Military Security of the State. *Eastern-European Journal of Enterprise Technologies*. 2020. № 5 (3(107)). P. 17–23.
- MykhailiukY., & Bashnianyn, O. (2024). The scientific and methodical apparatus for combating illegal migration in the area of responsibility of the border detachment. *Social Development and Security*, 14(5), 37-42. <https://doi.org/10.33445/sds.2024.14.5.4>.

Ключові кроки України в системі воєнної та національної безпеки щодо підвищення когнітивної стійкості (2025-2028 рр.): рекомендації у когнітивній та воєнно-економічній сфері

Key Steps of Ukraine in the Military and National Security System to Increase Cognitive Resilience (2025-2028): Recommendations in the Cognitive and Military-Economic Spheres

Олег Семененко ^A

Corresponding author: д. військ. н., професор, заступник начальника науково-дослідного інституту з наукової роботи, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Олександр Кінь ^B

к. тех. н., старший науковий співробітник, доцент, email: cubalibre1972@ukr.net, ORCID: 0009-0001-2196-7515

Лілія Семененко ^C

старший викладач кафедри іноземних мов, e-mail: selin-ua@ukr.net, ORCID: 0000-0002-5628-3586

Володимир Ремез ^C

доктор філософії, доцент кафедри територіальної оборони, e-mail: remezv93145@gmail.com, ORCID: 0000-0002-2561-1081

Сергій Митченко ^C

доктор філософії, доцент кафедри стратегії національної безпеки та оборони, serhii.mytchenko@gmail.com, ORCID: 0000-0003-3711-2033

Дмитро Рибак ^C

старший викладач кафедри територіальної оборони, e-mail: rybak.dima@ukr.net, ORCID: 0009-0005-4239-2131

Oleh Semenenko ^A

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

Oleksandr Kin ^B

Candidate of Technical Sciences, SENIOR Research Fellow, Associate Professor, email: cubalibre1972@ukr.net, ORCID: 0009-0001-2196-7515

Liliia Semenenko ^C

Senior Lecturer, Department of Foreign Languages, e-mail: selin-ua@ukr.net, ORCID: 0000-0002-5628-3586

Volodymyr Remez ^C

Doctor of Philosophy, Associate Professor of the Department Territorial Defese, e-mail: remezv93145@gmail.com, ORCID: 0000-0002-2561-1081

Serhii Mytchenko ^C

Doctor of Philosophy, Associate Professor of the Department of National Security and Defense Strategy, Kyiv, Ukraine, serhii.mytchenko@gmail.com, ORCID: 0000-0003-3711-2033

Dmytro Rybak ^C

Senior Teacher of the Department of Territorial Defense, e-mail: rybak.dima@ukr.net, ORCID: 0009-0005-4239-2131

^AЦентральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна

^BДипломатична академія України імені Геннадія Удовенка при Міністерстві закордонних справ, м. Київ, Україна

^CНаціональний університет оборони України, Київ, Україна

^ACentral Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

^BHennadiy Udoenko Diplomatic Academy of Ukraine under the Ministry of Foreign Affairs, Kyiv, Ukraine

^CNational Defence University of Ukraine, Kyiv, Ukraine

Received: August 05, 2025 | Revised: August 25, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.4>

Мета роботи. Окреслити ключові кроки України у 2025–2028 рр. у системі воєнної та національної безпеки, спрямовані на підвищення когнітивної стійкості суспільства і сектору оборони, з урахуванням загроз російсько-української війни, глобальних тенденцій інформаційного протистояння та економічних викликів війни.

Метод дослідження. Методи аналізу та синтезу; порівняння; стратегічного аналізу.

Результати дослідження. Визначені ключові кроки України щодо підвищення когнітивної стійкості у 2025–2028 рр. за різними сценаріями розвитку російсько-української війни; сформована система воєнно-економічних наслідків когнітивного впливу; сформовано цілісний опис ключових кроків України на 2025–2028 рр. щодо підвищення власної когнітивної стійкості й водночас системного, правомірного впливу на свідомість росіян – громадян, еліт і цільових груп.

Теоретична цінність дослідження. Результати дослідження можуть використовуватися фахівцями органів військового управління вищого рівня.

Тип статті. Теоретичний.

Purpose. Outline the key steps of Ukraine in 2025–2028 in the military and national security system, aimed at increasing the cognitive resilience of society and the defense sector, taking into account the threats of the Russian-Ukrainian war, global trends in information confrontation, and the economic challenges of the war.

Method. Methods of analysis and synthesis; comparison; strategic analysis.

Findings. Ukraine's key steps to increase cognitive resilience in 2025–2028 were identified under various scenarios of the development of the Russian-Ukrainian war; a system of military-economic consequences of cognitive influence was formed; a holistic description of Ukraine's key steps for 2025–2028 to increase its own cognitive resilience and, at the same time, a systematic, legitimate influence on the consciousness of Russians - citizens, elites and target groups..

Theoretical implications. The results of the study can be used by specialists of higher-level military command bodies to form views on further countering cognitive threats during an ongoing war.

Paper type. Theoretical.

Ключові слова: когнітивні загрози, воєнна та національна безпека, когнітивна стійкість, когнітивний вплив, когнітивна війна, інформаційна безпека, державна стійкість, сценарії продовження російсько-української війни.

Key words: cognitive threats, military and national security, cognitive resilience, cognitive influence, cognitive warfare, information security, state resilience, scenarios for the continuation of the Russian-Ukrainian war.

Вступ

Тривала російсько-українська війна демонструє, що сучасні воєнні конфлікти виходять далеко за межі традиційного збройного протистояння. Вони охоплюють когнітивну, інформаційну та воєнно-економічну сфери, де вирішується не лише доля фронтових операцій, а й довгострокова стійкість держави. Росія, усвідомлюючи не вигідність прямого протистояння з технологічно розвиненим світом, робить ставку на інструменти когнітивного впливу – масовану дезінформацію, пропаганду, маніпулятивні наративи та створення “альтернативної реальності” для власного населення й міжнародної спільноти. Це є черговою спробою агресора уникнути відповідальності, перетворитися в очах світу на “жертву” геополітики та водночас зберегти здатність контролювати свідомість і політичні рішення як всередині країни, так і поза її межами [1–7].

Додатковий виклик становить зміна політичних пріоритетів у США, де президент Дональд Трамп демонструє прагнення “задобрити” росію шляхом пошуку компромісів, що може підважити єдність Заходу та знизити рівень стратегічної підтримки України. У таких умовах росія отримує додаткове вікно можливостей для просування власних наративів у міжнародних інституціях, що створює ризики ревізії санкційної політики й посилення глобальної втоми від війни.

Міжнародний досвід підтверджує, що когнітивна стійкість є критичною складовою національної безпеки [1–20]. НАТО визначає стійкість суспільств як “першу лінію оборони” у гібридних війнах. Країни Балтії [12–14], зокрема Литва та Естонія, зробили ставку на розвиток стратегічних комунікацій, освіти у сфері медіаграмотності та формування довіри до державних інституцій, що дозволяє успішно нейтралізувати російську пропаганду. Ізраїль, перебуваючи у стані постійної воєнної загрози, демонструє приклад інтеграції військово-економічних заходів з когнітивною мобілізацією суспільства — від швидкої адаптації економіки до умов війни до формування колективної психологічної готовності протистояти багатовекторним загрозам [15–16].

Для України на 2025–2028 рр. пріоритетом стає поєднання воєнно-економічної стабільності з когнітивною стійкістю суспільства. З одного боку, необхідно створювати ефективну систему мобілізаційної економіки, здатну забезпечувати Збройні Сили ресурсами для тривалого опору. З іншого, потрібно формувати психологічну й інформаційну витривалість громадян, зміцнювати довіру до держави, захищати національну ідентичність та нейтралізувати інформаційно-психологічні атаки противника.

Таким чином, актуальність дослідження зумовлена потребою у виробленні цілісних рекомендацій у когнітивній та воєнно-економічній сферах, що дозволять Україні зберегти стійкість, зміцнити стратегічну автономію й залишатися активним суб’єктом міжнародної безпеки навіть в умовах змін зовнішньополітичної кон’юнктури [3–12].

Теоретичні основи дослідження

Проведемо аналіз наукових досліджень і публікацій за напрямом когнітивна стійкість, стратегічні комунікації / протидія когнітивному впливу росії, воєнно-економічна стійкість і відбудова [1–12].

1) Когнітивна війна та стійкість суспільства, що відбувається сьогодні:

НАТО трактує когнітивну війну як діяльність, синхронізовану з іншими інструментами сили, спрямовану на вплив на установки та поведінку шляхом захисту / порушення когніції населення; людська свідомість визнається окремим полем протистояння;

концепт “стійкості як першої лінії оборони” закріплений у підходах Альянсу та Стратегічній концепції 2022 р.: суспільна / інфраструктурна готовність критична для всіх базових завдань оборони;

наукові огляди відзначають міждисциплінарність і розмитість дефініцій “когнітивної війни”, але підтверджують її корисність для політичного аналізу та планування стійкості;

Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats – *Європейський центр передового досвіду з протидії гібридним загрозам*) системно описує “гібридні загрози” як скоординовані дії з експлуатацією вразливостей демократичних інститутів; пропонує whole-of-government підхід і навчальні / табличні вправи для відпрацювання стримування. Термін whole-of-government означає підхід, коли усі державні інституції та відомства діють скоординовано та узгоджено задля досягнення спільної стратегічної мети. Основні характеристики: комплексність – замість того, щоб кожне міністерство чи відомство діяло окремо, формується єдина державна політика; синергія – використання ресурсів і компетенцій різних структур (оборона, безпека, економіка, дипломатія, освіта, охорона здоров’я тощо); єдине стратегічне бачення – уряд працює як єдиний організм, а не як сукупність відомчих інтересів; застосування – найчастіше у сфері національної безпеки, кризового управління, боротьби з гібридними загрозами, кібербезпеки, когнітивної безпеки. Приклад: У контексті НАТО чи ЄС whole-of-government approach застосовується для протидії гібридним загрозам: не лише військові, а й дипломатичні, інформаційні, економічні та правові інструменти працюють у комплексі. В Україні це можна уявити як узгоджену взаємодію ЗСУ, СБУ, МЗС, МВС, Мінцифри, МОН та інших відомств у протидії російській агресії.

Фактично, Hybrid CoE – це аналітичний і навчальний хаб, який допомагає країнам розробляти інструменти для боротьби з гібридними війнами, подібними до тієї, яку веде росія проти України та Заходу.

Що це дає для України. Підтвердження потреби інституціоналізувати когнітивну безпеку (постійний урядовий центр / доктрина, міжвідомча координація, вимірювачі впливу) як компоненту нацбезпеки 2025–2028 рр.

Прогалини. Бракує валідованих метрик когнітивної стійкості на рівні громад / галузей; необхідні лонгітюдні панелі для оцінки ефекту втручання (комунікаційних, освітніх, психологічних) у воєнних умовах (Лонгітюдна панель (longitudinal panel) – це група респондентів (людей, сімей, організацій чи навіть цілих спільнот), які опитуються або обстежуються багаторазово протягом певного часу. “Лонгітюдний” означає протяжний у часі (на відміну від одноразового зрізу). “Панель” означає, що досліджується та сама вибірка респондентів у кількох хвилях (раундах).

2) Протидія FIMI / дезінформації та стратегічні комунікації, що відбувається сьогодні (FIMI часто використовується як абревіатура в контексті False Information, Misinformation, Malinformation, and Influence (у деяких джерелах ще включають disinformation. False Information – неправдива інформація (фейки без уточнення мотиву), Misinformation – ненавмисне поширення неправдивих відомостей (людина вірить у фейк і поширює його), Malinformation – “зловмисна інформація” – правдива, але використана у викривленому чи контекстуально маніпулятивному вигляді (наприклад, “зливи” особистих даних), Influence – інформаційний чи когнітивний вплив (маніпулятивні кампанії, психологічні операції)). Протидія FIMI / дезінформації розглядається як: моніторинг і виявлення інформаційних атак; фактчекінг і перевірка джерел; освітні заходи з медіаграмотності; побудова системи стратегічних комунікацій; залучення суспільства до “колективного імунітету” проти маніпуляцій);

ЄС (EEAS StratCom TF, зокрема East StratCom) розвиває інституційні спроможності моніторингу середовища, стратегічних кампаній і підвищення стійкості до FIMI; у звіті-2025 описані тактики державних і квазідержавних акторів та роль офіційних акаунтів як мультіплікаторів;

RAND (2024) узагальнює уроки українського спротиву російській дезінформації: швидкі урядові / волонтерські “факти-чек” екосистеми, наративи про суб’єктність, координація з партнерами, операційна безпека;

освітні втручання з медіаграмотності (IREX Learn to Discern) показали статистично значущі покращення умінь аналізувати новини та відрізняти факти / думки у школярів та дорослих.

Що це дає для України. Емпірична база для масштабування медіаграмотності як елемента нацбезпеки (включно з підготовкою військових / публічних службовців). Підтвердження ефективності єдиного вікна спростувань + мережевих центрів стратегічних комунікацій (Кабінету Міністрів України / Сили оборони України / партнери).

Прогалини. В Україні недостатньо приділяється увазі цьому питанню, достатньо мало робіт, що порівнюють вартість-ефект різних інструментів (фактчек, освітні курси, контр-наративи, бот-виявлення). Потрібні RCT / квазіексперименти на українській вибірці 2025–2028 років.

3) *Военно-економічна стійкість, відбудова та доброчесність, що відбувається сьогодні:*

оновлена RDNA4 (Rapid Damage and Needs Assessment (*швидка оцінка збитків і потреб*)), тобто Уряд України, Світовий банк, ЄК, ООН оцінює потреби відновлення станом на 31.12.2024 у \$524 млрд на десятиріччя; підсвічує пріоритети енергетики, житла, транспорту й посилення інституцій управління проектами. Це ключові рамки для планування 2025–2028 років.

огляди ЄС щодо наближення до *acquis* (огляди ЄС щодо наближення до *acquis* (Звіт-2024) → EU reviews on approximation to the *acquis* (Report-2024), де *acquis* = *acquis communautaire* – сукупність законодавства, рішень, норм та практик Європейського Союзу, які країни-кандидати мають імплементувати) та донорські оцінки (NORAD-2024 → donor assessments (NORAD = Norwegian Agency for Development Cooperation – Норвезьке агентство з питань міжнародного розвитку, яке часто готує незалежні аналітичні оцінки щодо ефективності допомоги та ризиків): цифрові реєстри → digital registries, відкриті дані → open data, незалежний аудит → independent audit, зміцнення наглядових органів → strengthening of oversight bodies) описують корупційні ризики і набір контрзаходів (цифрові реєстри, відкриті дані, незалежний аудит, зміцнення наглядових органів).

Що це дає для України. Обґрунтування включення до стратегії когнітивної стійкості економічних комунікацій: прозорість відбудови знижує вразливість до наративів “крадіжок / неспроможності”, а також підсилює довіру. Використання міжнародних стандартів прозорості як “щеплення” проти FIMI (публічні дашборди, аудит відбудови, реєстри бенефіціарів, відкриті контракти).

Прогалини. Нестача досліджень, що прямо пов’язують прозорість фінансування відбудови й рівень довіри / опірність дезінформації в українському контексті; потрібні змішані методи (панелі громад + контент-аналіз інформаційного середовища).

4) *Україноцентричні уроки і порівняльні кейси, що відбувається сьогодні:*

порівняльні підходи (країни Балтії / Ізраїль / НАТО) наголошують на whole-of-society підході, інтеграції психологічної допомоги, кіберзахисту й стратегічних комунікацій; ключова роль довіри та освіти.

Прогалини. Бракує **адаптаційних моделей** під затяжну війну з регулярними ударами по енергетичній системі (зв’язок між “ритмом ударів” і динамікою морально-психологічного стану населення).

Постановка проблеми

Отже, метою дослідження є окреслити ключові кроки України у 2025–2028 рр. у системі воєнної та національної безпеки, спрямовані на підвищення когнітивної стійкості суспільства і сектору оборони, з урахуванням загроз російсько-української війни, глобальних тенденцій інформаційного протистояння та економічних викликів війни. У роботі ставиться завдання

виробити науково обґрунтовані рекомендації щодо розвитку інституційних, когнітивних та воєнно-економічних механізмів, які дозволять зміцнити здатність держави та суспільства протидіяти когнітивному впливу противника, забезпечувати національну стійкість і створювати підґрунтя для стратегічної переваги України.

Результати

Одним із визначальних чинників стійкості українського суспільства у найближчі роки стане здатність держави та її інституцій забезпечити належний рівень когнітивної безпеки [1–20]. В умовах російсько-української війни противник активно застосовує широкий спектр інформаційно-психологічних операцій, спрямованих на деморалізацію населення, підлив довіри до влади та міжнародних партнерів, а також на спотворення реальної картини війни. Водночас формування цілісної системи когнітивної стійкості вимагає не лише реагування на загрози, а й стратегічного планування, орієнтованого на різні можливі сценарії розвитку ситуації.

Саме тому виникає необхідність визначення ключових кроків, які Україна має реалізувати у період 2025–2028 рр. для посилення когнітивної стійкості суспільства, державних інституцій та сектору безпеки й оборони. Систематизація таких кроків дозволяє окреслити можливості адаптації державної політики під конкретні умови війни або післявоєнного відновлення. Узагальнені орієнтири представлено у табл. 1.

Узагальнимо матеріал табл. 1 за наведеним сценаріями та кроками України щодо підвищення когнітивної стійкості у боротьби з російськими загарбниками.

Таблиця 1 – Ключові кроки України щодо підвищення когнітивної стійкості у 2025–2028 рр. за різними сценаріями розвитку російсько-української війни

Сценарій / Період	Основні заходи когнітивного впливу росії	Необхідні кроки України для підвищення когнітивної стійкості
Сценарій 1. Війна закінчується до кінця 2025 р.		
2025 (кінець війни)	масована кампанія “переможної росії”; дискредитація перемоги України (“це результат Заходу, а не українців”); поширення фейків про нібито “зраду” чи “зміну територій”.	запровадження державної програми стратегічних комунікацій щодо результатів війни; формування нарративу власної перемоги та ролі українців; системна протидія фейкам через єдину цифрову платформу спростувань.
2026–2027 (відновлення)	провокування недовіри до держави через фейки про корупцію у відновленні; розпалювання регіональних протиріч (“хто більше отримує допомоги”).	прозора система контролю відновлення (цифровий аудит, відкриті дані); розвиток громадської участі в ухваленні рішень; освітні програми з медіаграмотності та інформаційної гігієни.
2027–2028 (перехід до мирного життя)	вкиди про “втому від війни” і “непотрібність НАТО”; спроби підірвати віру в інтеграцію України в ЄС та НАТО.	посилення євроатлантичних нарративів через державні та освітні програми; комунікація довгострокових вигод інтеграції; культурні та ціннісні проекти на підтримку ідентичності.
Сценарій 2. Війна триває до кінця 2026 р.		
2025–2026 (активна війна)	дезінформація про “неминучий розпад України”; поширення паніки про виснаження ресурсів; спроби деморалізувати суспільство через втрати.	підвищення рівня стійкості суспільства через національні комунікаційні кампанії (“Україна тримається”); психологічна підтримка військових і цивільних;

Сценарій / Період	Основні заходи когнітивного впливу росії	Необхідні кроки України для підвищення когнітивної стійкості
		розвиток кіберзахисту та платформ для боротьби з фейками.
2027–2028 (важке відновлення)	звинувачення України у “неспроможності відновитися”; поширення нарративу “краще під росією, ніж у бідності”.	державні програми з економічної комунікації (“економіка росте попри війну”); формування довіри до уряду через відкриті механізми відновлення; масштабна підтримка локальних громад як осередків стійкості.
Сценарій 3. Війна триває увесь період (2025–2028 рр.)		
2025–2028 (затяжна війна)	постійна кампанія виснаження: “Захід вас зрадив”, “Ви приречені”, “Україна не існує без росії”; спроби зламати мораль військових та цивільних через щоденний тиск; активне використання когнітивних операцій для розколу в суспільстві та елітах.	інституціоналізація системи когнітивної безпеки (створення Центру когнітивної стійкості в системі нацбезпеки); постійні програми психологічної підтримки населення та військових; синхронізація стратегічних комунікацій з міжнародними партнерами; виховання “суспільства стійкості” через освіту, культуру та медіа.

Сценарій 1. Війна завершується до кінця 2025 року.

У випадку завершення війни до кінця 2025 року Україна опиняється в умовах складного перехідного етапу, коли перемога потребує правильного комунікаційного та когнітивного закріплення. Росія намагатиметься дискредитувати перемогу, поширюючи нарративи про те, що здобутки є виключно результатом допомоги Заходу, а також вигадуючи фейки про “зраду” та “втрату територій”. Основним завданням України у цей період стає формування власного нарративу перемоги, підкреслення ролі українців як центрального суб’єкта опору та створення системної платформи стратегічних комунікацій, яка б одразу спростовувала російські маніпуляції.

У 2026–2027 рр., під час етапу відновлення, російська пропаганда буде спрямована на розпалювання недовіри до української держави через історії про “корупцію у відбудові” та намагання провокувати внутрішні регіональні протиріччя щодо розподілу допомоги. У відповідь Україна має забезпечити максимальну прозорість процесу відновлення, створивши цифрову систему відкритих даних і незалежного контролю. Важливими стануть громадська участь у прийнятті рішень та освітні програми з медіаграмотності, які підвищуватимуть когнітивну стійкість населення.

У 2027–2028 рр., коли відновлення перейде у фазу поступового повернення до мирного життя, основною лінією когнітивного впливу росії стане поширення скепсису щодо вступу України до НАТО та ЄС. Кремль активно просуватиме тези про “непотрібність інтеграції” і “втому від війни”. Українська відповідь має базуватися на широких просвітницьких і культурних програмах, які демонструватимуть вигоди європейської інтеграції та захищатимуть національну ідентичність, закріплюючи стратегічний курс держави.

Сценарій 2. Війна триває до кінця 2026 року.

Якщо війна продовжиться ще протягом двох років, то у 2025–2026 рр. Україна опиниться в умовах виснаження ресурсів та суспільної втоми. Росія намагатиметься поширювати нарративи про “неминучий розпад України”, “вичерпання ресурсів” та “безглуздість опору”. Також активізуються спроби деморалізації населення через інформаційні кампанії про високі втрати. У відповідь Україна повинна проводити національні інформаційні кампанії, спрямовані на консолідацію (“Україна тримається”), а також

розбудовувати систему психологічної підтримки військових і цивільних. Важливим буде й розвиток кіберзахисту та цифрових платформ для спростування дезінформації.

У 2027–2028 рр., коли бойові дії завершаться і розпочнеться відновлення, росія спробує переконати українців і світ у неспроможності України відродитися після війни, просуваючи наративи “краще з росією, ніж у бідності”. Українська відповідь має бути побудована на масштабній комунікації успіхів у відбудові, демонстрації позитивної динаміки економіки та відкритості процесів. Водночас слід підтримувати роль локальних громад як ключових центрів стійкості, оскільки саме вони найменше піддаються централізованим інформаційним маніпуляціям і виступають “фільтрами” проти зовнішнього впливу.

Сценарій 3. Війна триває увесь період (2025–2028 рр.).

У випадку затяжної війни росія застосовуватиме стратегію постійного когнітивного тиску на Україну. Основними напрямками стануть кампанії виснаження, а саме твердження, що “Захід зрадив Україну”, що “ви приречені”, а також намагання підірвати мораль військових та цивільних шляхом щоденних інформаційних атак. Додатковим інструментом буде провокування внутрішніх розколів серед політичних і суспільних еліт з метою створення атмосфери нестабільності та безнадії.

Українська стратегія у цьому сценарії повинна базуватися на інституціоналізації системи когнітивної безпеки, тобто створенні спеціальних державних інституцій (наприклад, Центру когнітивної стійкості) у структурі національної безпеки. Необхідно забезпечити постійні програми психологічної підтримки для військових і цивільних, які допоможуть знизити рівень виснаження. Важливою стане синхронізація стратегічних комунікацій із міжнародними партнерами, щоб протидіяти глобальним маніпуляціям росії. Нарешті, довгостроковою опорою виступатиме виховання “суспільства стійкості” через систему освіти, культуру та медіа, що формуватиме здатність громадян критично мислити та зберігати впевненість у власній державі навіть за умов тривалої війни.

У табл. 2 системно розкрито ключові елементи цього впливу, зокрема: джерела породження наслідків, тобто, через які інструменти, платформи чи когнітивні вектори здійснюється атака; особливості впливу, тобто як саме відбувається втручання в інформаційно-психологічну, економічну або оборонну структуру; конкретні наслідки тобто, які саме дисфункції, втрати чи деформації виникають в економіці, секторі оборони та інших сферах життєдіяльності; а також ступінь впливу на різні виміри національної безпеки, зокрема: ВБ – воєнну безпеку, ЕБ – економічну безпеку, ПБ – політичну безпеку, ІБ – інформаційну безпеку, СБ – соціальну безпеку. Такий підхід дозволяє не лише фіксувати факт негативного впливу, а й визначати критичні вразливості системи та пріоритетні напрями протидії.

Таблиця 2 – Система воєнно-економічних наслідків когнітивного впливу

№ з/п	Наслідок	Джерело породження	Особливості впливу	Конкретні наслідки	Ступінь впливу (ВБ/ЕБ/ПБ/ІБ/СБ)
1	Підрив довіри до інститутів влади та ЗС України	Дезінформаційні кампанії, ІПсО, маніпулятивні наративи	Зменшення суспільної підтримки рішень влади й ЗС України	Демобілізація населення, зниження морального духу військ	ВБ – високий, ПБ – високий, СБ – високий
2	Паніка та деструктивна економічна поведінка	Масоване поширення фейків про критичну інфраструктуру, банківську систему	Створення відчуття катастрофи, обвалу	Виведення капіталу, зняття депозитів, підвищення попиту на готівку, коливання курсу	ЕБ – високий, ІБ – високий

№ з/п	Наслідок	Джерело породження	Особливості впливу	Конкретні наслідки	Ступінь впливу (ВБ/ЕБ/ПБ/ІБ/СБ)
3	Підриг мобілізаційного потенціалу	Когнітивні атаки на патріотизм, спотворення образу війни, знецінення служби	Формування відрази до участі у війні, акцент на втратах, фейкові історії	Зниження кількості добровольців, ухилення від мобілізації, дефіцит кадрів	ВБ – критичний, СБ – середній
4	Руйнування міжнародного іміджу держави	Когнітивні впливи в зарубіжних медіа, дипломатичні ІПСО	Зміна сприйняття міжнародними партнерами	Зниження рівня міжнародної підтримки, санкційне послаблення ворога, зменшення фінансової допомоги	ПБ – високий, ЕБ – високий
5	Розрив інформаційного середовища	Маніпуляція суспільною свідомістю через соцмережі та бот-мережі	Створення поляризації, дезорієнтації	Неможливість вироблення колективної стратегії поведінки в кризі, криза лідерства	ІБ – критичний, ПБ – високий, СБ – високий
6	Економічна демотивація суб'єктів ринку	Прогнозовані або інспіровані повідомлення про майбутній колапс, втрату територій, нестабільність	Очікування краху держави як економічного суб'єкта	Зниження інвестицій, скорочення виробництва, масовий відтік бізнесу	ЕБ – критичний, ВБ – високий
7	Порушення довіри до системи управління обороною	Викриття або створення “викриттів” корупції, некомпетентності в командуванні	Формування образу хаосу в армії	Слабка підтримка військових бюджетів, посилення громадського тиску, політична дестабілізація	ВБ – високий, ПБ – високий
8	Маніпуляція цілями війни та наративами перемоги	Використання когнітивних дисонансів, підміна понять	Розмиття розуміння мети війни у населення	Зниження рівня мобілізації ресурсів і витривалості до тривалої війни	ВБ – високий, СБ – середній
9	Ерозія стратегічної економічної стійкості	Інформаційний вплив на рішення щодо критичних галузей	Втягування у помилкові економічні рішення під тиском страху чи фальшивої інформації	Зміна пріоритетів у державному бюджеті, хибна приватизація, втрати в ОПК	ЕБ – критичний, ВБ – високий

Проведений аналіз даних наведених у табл. 2 показує, що:

критично вразливими до когнітивного впливу є воєнна та економічна безпека держави; основними провідними механізмами є інформаційно-психологічні операції, стратегічні наративи, фейкові кампанії;

до найбільш руйнівних наслідків можна віднести демобілізація, підриг економіки оборони, втрата міжнародної підтримки.

Когнітивний вплив є не лише інформаційною загрозою, а потужним інструментом стратегічного ослаблення держави, який впливає на всі складові її безпеки, а саме: воєнну, економічну, політичну, соціальну та інформаційну.

Сформуємо цілісний опис ключових кроків України на 2025–2028 рр. щодо підвищення власної когнітивної стійкості й водночас системного, правомірного впливу на свідомість росіян – громадян, еліт і цільових груп, за трьома можливими сценаріями розвитку війни. Підхід у всіх сценаріях спирається на правду, доказовість, гуманітарне право, прозорість і відмову від мови ненависті: саме довіра до джерела і моральна перевага є головними “множниками сили” в когнітивній площині.

Сценарій 1: війна завершується до кінця 2025 р., у 2026–2027 триває відновлення, у 2027–2028 — перехід до мирного життя.

У короткому періоді до кінця 2025 року Україна має швидко зафіксувати правду про причини й перебіг війни, показавши російській аудиторії документовані наслідки агресії для самих росіян: реальні втрати, деградацію регіонів, падіння якості послуг і доходів, розрив соціальних ліфтів. Для цього доцільно розгорнути сталу російськомовну стратегічну комунікацію на багатьох платформах, синхронізовану з міжнародними медіа й діаспорами, зробивши акцент на простих для верифікації фактах, цифрових реєстрах руйнувань і відновлення, відкритих судах щодо воєнних злочинів та персоналізованих історіях жертв. Пріоритетом є доступність матеріалів через канали, які росіяни реально споживають: легальні дзеркала, подкасти, довгі інтерв'ю з очевидцями, короткі відеоформати, а також окремі продукти для професійних спільнот (медики, вчителі, водії, IT-фахівці), де показуються альтернативні можливості співпраці з Україною в майбутньому і ціна ізоляції. У фазі відновлення 2026–2027 рр. акцент зміщується на контраст: Україна демонструє темп модернізації, прозорість витрат і антикорупційні запобіжники, порівнюючи їх із закритістю російської системи. Цей “наратив розвитку” має підкріплюватися відкритими дашбордами відбудови, історіями про повернення бізнесу, впровадженням енергетичних і цифрових рішень та партнерств із містами ЄС. Все це подається російською мовою як доказ того, що нормальність, добробут і безпека досяжні поза імперською логікою. У 2027–2028 рр., у перехід до мирного життя, важливо підтримувати довгий “маятник довіри”: росії адресуються культурні та освітні продукти, які розвінчують міфи про “історичне призначення” війни, пояснюють переваги європейської безпеки та економічної взаємодії, і водночас відкривають перспективу поствоєнної регіональної співпраці за умови відмови росії від агресії. Стабільні рубрики про успіхи українських громад, технологічні кластери, університетські програми для іноземців, україноцентричні культурні проєкти й переклади сучасної української літератури російською працюють як “м'який міст” до аудиторії, якій починають бути очевидними власні втрати від війни.

Сценарій 2: війна не завершується до кінця 2026 р., у 2027–2028 — затяжне відновлення.

У 2025–2026 рр. ядро когнітивної стратегії – це систематично вибивати з російського інформаційного поля опору на брехню “про неминучу перемогу та стабільність”. Україна має щоденно, одномовно й багатоканально виводити до росіян правдиві показники війни: кадрові й технічні втрати агресора, факти корупції у постачаннях, реальні вироки й слідчі дії, ефект санкцій на регіональні бюджети, скорочення соціальних програм, демографічні провали. Це подається у форматі серіалізованих розслідувань, коротких інфографік і персоналізованих кейсів, а саме: матерів і дружин мобілізованих, підприємців, що втратили експорт, студентів без перспектив мобільності. Окрема лінія – це робота з “професійними мікроспільнотами” всередині росії (медики, освітяни, енергетики, IT), для яких створюються корисні, прагматичні матеріали: як війна знижує стандарти у їхній сфері, чому “відтік мізків” невідворотний, які дороги до професійної реалізації закриті та як це контрастує з траєкторією України. У 2027–

2028 рр., коли Україна починає важке відновлення, ключовим стає показати росіянам незаперечну різницю траєкторій: відкриті тендери, міжнародні аудити, повернення інвесторів і місцеві історії зростання в Україні проти подальшого згортання конкуренції, військових витрат і “ручного управління” в росії. Зміст залишається неагресивним за формою, але докладним за фактами, з юридично перевіреними доказами і простими метриками, які кожен у росії може співвіднести з власним життям (ціни, черги, зарплати, якість сервісів). Головна мета – це не просто “переконати всіх”, а стабільно розширювати прошарок сумніву, підсвічувати внутрішні суперечності режиму та робити привабливим образ “нормального життя без війни”, який росіянам роками недоступний.

Сценарій 3: війна триває увесь період 2025–2028 рр.

За довготривалої війни стратегія повинна перейти від реактивної до інституціоналізованої. Україна вибудовує постійну систему когнітивної безпеки з функціями моніторингу, швидкого реагування, досліджень і вимірювання ефекту. Для російської аудиторії це означає безперервний, професійний, етичний і технологічно підсилений інформаційний вплив. На змістовому рівні пріоритет – це тримати незмінним “ядро правди”: документування злочинів та наслідків, регулярні оновлення даних про економічну і демографічну ціну агресії, викриття корупції у військово-промисловому комплексі, показ альтернатив, які росіяни втрачають (освіта, кар’єра, подорожі, технологічна кооперація). На рівні аудиторій акцент зсувається з масовості до “сітки ніш”: робота з родинами мобілізованих, ветеранами, місцевими елітами в регіонах-донорах мобресурсу, міськими середніми класами у великих агломераціях, технічними спільнотами та творчими індустріями, де критичне мислення природно вище. На інструментальному рівні потрібні довготривалі продукти з високою довірою: російськомовні аналітичні медіа, канали фактчекінгу з відкритими методиками, платформи для безпечних свідчень, “повільні” формати – це документальні подкасти, серії інтерв’ю, лонгріди, освітні курси, а також культурні колаборації з перекладом сучасної української культури й науки. Технічно це підтримується розробкою легальних маршрутів доступу до контенту в умовах цензури, аналітикою аудиторій, етичним використанням штучного інтелекту для персоналізації повідомлень, системою регулярних опитувань у діаспорах і суміжних просторах (Казахстан, Вірменія, Грузія, Латвія тощо), щоб відстежувати зміни переконань. Головна мета – це не швидка “перемога в головах”, а повільне, але невідворотне накопичення когнітивної втоми від війни, нарощення сумніву в “сакральності” агресії, ослаблення готовності підтримувати мобілізацію та репресивну економіку.

Поперек усіх сценаріїв незмінними лишаються кілька принципів. По-перше, бездоганна доказовість і юридична чистота: кожне твердження має спиратися на перевірені джерела, візуальні докази, відкриті реєстри та рішення судів, а саме: це вибудовує довіру в тих росіян, які вже сумніваються. По-друге, персоналізація і емпатія: мова фактів поєднується з людськими історіями, які дають можливість ідентифікувати себе з жертвою, а не з пропагандистським міфом; звернення не принижують гідність, не узагальнюють і не дегуманізують. По-третє, “контраст траєкторій”: Україна послідовно показує власний курс на відбудову, інтеграцію, інновації й свободу, а не лише критикує російську систему, тобто позитивний образ майбутнього працює сильніше за спростування. По-четверте, технологічна і організаційна сталість: міжвідомчий центр когнітивної безпеки, координація зі стратегічними комунікаціями партнерів, аналітика впливу й етичні стандарти роботи з аудиторіями. Нарешті, безпека своїх громадян і військових – це пріоритет: ніяких закликів до насильства чи нелегітимних дій, суворе дотримання міжнародного права та захист персональних даних.

Такий підхід робить українську когнітивну стратегію не “кампанією на тиждень”, а довгою, послідовною політикою (стратегією), що одночасно підсилює внутрішню стійкість і поступово розмиває готовність російського суспільства підтримувати війну. Це не про

пропаганду, а про системну роботу з правдою, довірою і привабливою альтернативою майбутнього.

Висновки

У статті було обґрунтовано, що підвищення когнітивної стійкості України у 2025–2028 рр. є критичною умовою збереження воєнної та національної безпеки в умовах триваючої російсько-української війни та зростаючого міжнародного тиску, пов'язаного з прагненням росії вибilitи свою роль у світовому співтоваристві. Аналіз сучасних тенденцій засвідчив, що росія продовжує активно застосовувати когнітивні та інформаційні інструменти для впливу на свідомість власного населення, міжнародних лідерів і суспільств, намагаючись уникнути відповідальності та легітимізувати агресію. У цих умовах Україна має діяти асиметрично, поєднуючи когнітивні, інформаційні та воєнно-економічні заходи.

Розроблена матриця сценаріїв дозволила виокремити три можливі траєкторії розвитку подій – ескалацію війни, контрольовану напругу та перехід до переговорного процесу. Для кожного сценарію визначено відповідні ключові кроки України у сфері зміцнення когнітивної стійкості. Показано, що незалежно від перебігу війни держава повинна послідовно розвивати систему стратегічних комунікацій, удосконалювати воєнно-економічну спроможність, забезпечувати підтримку населення через освіту й інформаційну безпеку, а також формувати міжнародні коаліції для протидії російським когнітивним атакам.

Аналіз наукових досліджень і публікацій продемонстрував, що питання когнітивної безпеки розглядається переважно в контексті гібридної війни, інформаційно-психологічних операцій та воєнної економіки, проте системне поєднання когнітивних і воєнно-економічних аспектів ще не отримало достатнього висвітлення у вітчизняній та міжнародній літературі. Це підкреслює наукову новизну та практичну значущість проведеного дослідження.

У 2025–2028 рр. Україна має розбудувати цілісну систему когнітивної стійкості, яка поєднує внутрішню оборону свідомості громадян та стратегічний вплив на російське суспільство. Ефективність такої стратегії полягає у правдивості, доказовості та демонстрації позитивної альтернативи розвитку України, що поступово підриває легітимність російської війни у свідомості її громадян. У результаті когнітивна політика України здатна не лише захистити власний інформаційний простір, а й сприяти послабленню ворожої здатності вести затяжну агресію.

Отже, ключовим висновком є те, що Україна має розглядати когнітивну стійкість як багаторівневу систему, яка інтегрує воєнні, інформаційні, економічні та суспільні ресурси. Її розвиток у найближчі роки дозволить не лише протидіяти російським когнітивним операціям, а й сформувати нову модель безпеки, що стане важливим внеском у зміцнення регіональної та глобальної стабільності.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Deppe, A., & Schaal, K. (2024). *Advancing Towards a Common Understanding of Cognitive Warfare for Science and Technology, and Identifying Future Research Trajectories*. NATO Science & Technology Board. URL : <https://pubmed.ncbi.nlm.nih.gov/39552633/>

2. NATO Allied Command Transformation. ACT develops the Cognitive Warfare Concept to combat disinformation and defend against “cognitive warfare” [Електронний ресурс]. – 03.07.2024. – URL : <https://www.act.nato.int/article/cogwar-concept/>
3. Helmus T. C., Holynska K. Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict. RAND Corporation, 2024. (Research Report No. RR-A2771-1). – URL : https://www.rand.org/pubs/research_reports/RRA2771-1.html
4. EEAS StratCom Task Forces. 3rd Threat Report: Fighting Immunity to Misinformation and Disinformation (FIMI). European External Action Service, 2025. – URL : <https://www.eeas.europa.eu/>
5. IREX. (2024). *Learn to Discern in Schools Evaluation Report*. URL: <https://www.irex.org/sites/default/files/node/resource/evaluation-learn-to-discern-in-schools-ukraine.pdf>
6. Mejova Y., Capozzi A., Monti C., De Francisci Morales G. Narratives of War: Ukrainian Memetic Warfare on Twitter [Електронний ресурс]. – arXiv preprint, 2023. – URL : <https://arxiv.org/abs/2309.08363>
7. Gouliev, Z. (2025). *Propaganda and Information Dissemination in the Russo-Ukrainian War: NLP of Russian and Western Twitter Narratives*. arXiv preprint. URL: <https://arxiv.org/abs/2506.01807>
8. NATO. Coronavirus: Invisible threats and preparing for resilience [Електронний ресурс]. – NATO Review, 20.05.2020. – URL : <https://www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html>
9. Freedman L. NATO’s resilience: the first and last line of defence [Електронний ресурс]. – LSE IDEAS, 2021. – URL : <https://lseideas.medium.com/natos-resilience-the-first-and-last-line-of-defence-89c42ac47eb0>
10. Conley H. A., Mina J. The Future of Hybrid Warfare [Електронний ресурс]. – Center for Strategic and International Studies (CSIS), 2022. – URL : <https://www.csis.org/analysis/future-hybrid-warfare>
11. Jastramskis M., Aleksejeva I. Strategic Communications, Countering Disinformation and Propaganda: Recommendations for State Policy [Електронний ресурс]. – 2023. – URL : https://www.researchgate.net/publication/383993797_Strategic_Communications_Countering_Disinformation_and_Propaganda_Recommendations_for_State_Policy
12. Baltic Centre for Media Excellence (BCME). Media Literacy Sector Mapping in Estonia and Lithuania and the Policy Brief: With Media Literacy Towards Cognitive Resilience [Електронний ресурс]. – 2022. – URL : <https://bcme.eu/en/our-work/research/report-media-literacy-sector-mapping-in-estonia-and-lithuania-and-the-policy-brief-with-media-literacy-towards-cognitive-resilience>
13. Pullella S. Inside Lithuania’s Battle Against Russian Disinformation [Електронний ресурс]. – TIME, 2022. – URL : <https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine>
14. Debunk.org. Wikipedia [Електронний ресурс]. – 2023. – URL : <https://en.wikipedia.org/wiki/Debunk.org>
15. Pierri F., Luceri L., Jindal N., Ferrara E. Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine [Електронний ресурс]. – arXiv preprint, 2022. – URL : <https://arxiv.org/abs/2212.00419>
16. Boháček M., Farid H. Protecting President Zelenskyy against Deep Fakes [Електронний ресурс]. – arXiv preprint, 2022. – URL : <https://arxiv.org/abs/2206.12043>
17. World Bank; Government of Ukraine; European Union; United Nations. Ukraine Fourth Rapid Damage and Needs Assessment (RDNA4), February 2022 – December 2024 [Електронний

- ресурс]. – World Bank, 2025. – URL : <https://documents.worldbank.org/curated/en/099022025114040022>
18. European Commission. Ukraine Report 2024 [Електронний ресурс]. – DG NEAR, 30.10.2024. – URL : https://enlargement.ec.europa.eu/ukraine-report-2024_en
19. Norad Evaluation Department. Ukraine: Corruption Risks and Mitigation Strategies. Report 3/2024 [Електронний ресурс]. – Oslo: NORAD, 2024. – URL : <https://www.norad.no>
20. NATO. Resilience: The First Line of Defence [Електронний ресурс]. – NATO Review, 2019. – URL : <https://www.nato.int/docu/review/articles/2019/03/20/resilience-the-first-line-of-defence/index.html>

References

1. Deppe, A., & Schaal, K. (2024). *Advancing towards a common understanding of cognitive warfare for science and technology, and identifying future research trajectories*. NATO Science & Technology Board. Available from : <https://pubmed.ncbi.nlm.nih.gov/39552633/>
2. NATO Allied Command Transformation. (2024, July 3). *ACT develops the Cognitive Warfare Concept to combat disinformation and defend against “cognitive warfare”*. Available from : <https://www.act.nato.int/article/cogwar-concept/>
3. Helmus, T. C., & Holynska, K. (2024). *Ukrainian resistance to Russian disinformation: Lessons for future conflict* (Report No. RR-A2771-1). RAND Corporation. Available from : https://www.rand.org/pubs/research_reports/RRA2771-1.html
4. EEAS StratCom Task Forces. (2025). *3rd threat report: Fighting immunity to misinformation and disinformation (FIMI)*. European External Action Service. Available from : <https://www.eeas.europa.eu/>
5. IREX. (2024). *Learn to discern in schools evaluation report*. Available from : <https://www.irex.org/sites/default/files/node/resource/evaluation-learn-to-discern-in-schools-ukraine.pdf>
6. Mejova, Y., Capozzi, A., Monti, C., & De Francisci Morales, G. (2023). *Narratives of war: Ukrainian memetic warfare on Twitter*. arXiv. Available from : <https://arxiv.org/abs/2309.08363>
7. Gouliev, Z. (2025). *Propaganda and information dissemination in the Russo-Ukrainian war: NLP of Russian and Western Twitter narratives*. arXiv. <https://arxiv.org/abs/2506.01807>
8. NATO. (2020, May 20). *Coronavirus: Invisible threats and preparing for resilience*. NATO Review. Available from : <https://www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html>
9. Freedman, L. (2021). *NATO’s resilience: The first and last line of defence*. LSE IDEAS. Available from : <https://lseideas.medium.com/natos-resilience-the-first-and-last-line-of-defence-89c42ac47eb0>
10. Conley, H. A., & Mina, J. (2022). *The future of hybrid warfare*. Center for Strategic and International Studies. Available from : <https://www.csis.org/analysis/future-hybrid-warfare>
11. Jastramskis, M., & Aleksejeva, I. (2023). *Strategic communications, countering disinformation and propaganda: Recommendations for state policy*. ResearchGate. Available from : https://www.researchgate.net/publication/383993797_Strategic_Communications_Countering_Disinformation_and_Propaganda_Recommendations_for_State_Policy
12. Baltic Centre for Media Excellence. (2022). *Media literacy sector mapping in Estonia and Lithuania and the policy brief: With media literacy towards cognitive resilience*. Available from : <https://bcme.eu/en/our-work/research/report-media-literacy-sector-mapping-in-estonia-and-lithuania-and-the-policy-brief-with-media-literacy-towards-cognitive-resilience>
13. Pullella, S. (2022). Inside Lithuania’s battle against Russian disinformation. *TIME*. Available from : <https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine>

14. Debunk.org. (2023). *Debunk.org*. In *Wikipedia*. Available from : <https://en.wikipedia.org/wiki/Debunk.org>
15. Pierri, F., Luceri, L., Jindal, N., & Ferrara, E. (2022). *Propaganda and misinformation on Facebook and Twitter during the Russian invasion of Ukraine*. arXiv. Available from : <https://arxiv.org/abs/2212.00419>
16. Boháček, M., & Farid, H. (2022). *Protecting President Zelenskyy against deep fakes*. arXiv. Available from : <https://arxiv.org/abs/2206.12043>
17. World Bank, Government of Ukraine, European Union, & United Nations. (2025). *Ukraine fourth rapid damage and needs assessment (RDNA4), February 2022 – December 2024*. World Bank. Available from : <https://documents.worldbank.org/curated/en/099022025114040022>
18. European Commission. (2024, October 30). *Ukraine report 2024*. DG NEAR. Available from : https://enlargement.ec.europa.eu/ukraine-report-2024_en
19. Norad Evaluation Department. (2024). *Ukraine: Corruption risks and mitigation strategies (Report 3/2024)*. Norad. Available from : <https://www.norad.no>
20. NATO. (2019, March 20). *Resilience: The first line of defence*. NATO Review. Available from : <https://www.nato.int/docu/review/articles/2019/03/20/resilience-the-first-line-of-defence/index.html>

Українська дипломатія безпеки в новій геополітичній реальності: гарантії безпеки для України, ризики та виклики

Ukrainian security diplomacy in the new geopolitical reality: security guarantees for Ukraine, risks and challenges

Володимир Гурковський^A

Corresponding author: доктор наук з державного управління, професор, начальник відділу, e-mail: volodymyr.gurkovskiy@gmail.com; ORCID: 0000-0003-2021-5204

Іван Гаврилюк^A

к.військ. наук, старший дослідник, e-mail: ivan_havryliuk@ukr.net, ORCID: 0000-0002-3514-0738

Юрій Клят^A

к.т.н., доцент, начальник Центрального науково-дослідного інституту Збройних Сил України, e-mail: klyatt@ukr.net, ORCID: 0000-0002-8267-3748

Юзеф Добровольський^B

к.т.н., доцент, заступник начальника, e-mail: kataza@i.ua, ORCID: 0000-0002-1077-1402

Євген Романенко^A

доктор наук з державного управління, професор, начальник управління, e-mail: poboss1978@gmail.com, ORCID: 0000-0003-2285-0543

Сергій Ільницький^A

науковий співробітник, e-mail: anastx85@icloud.com; ORCID: 0009-0009-3000-9034

Volodymyr Gurkovskiy^A

Corresponding author: Dr of Science in Public Administration, professor, Chief of Department, e-mail: volodymyr.gurkovskiy@gmail.com; ORCID: 0000-0003-2021-5204

Ivan Havryliuk^A

Ph.D., Associate Professor, e-mail: ivan_havryliuk@ukr.net, ORCID: 0000-0002-3514-0738

Yurii Kliat^A

Ph.D., Associate Professor, Head of the Central Research Institute of the Armed Forces of Ukraine, e-mail: klyatt@ukr.net, ORCID: 0000-0002-8267-3748

Yuzef Dobrovolskyi^B

Candidate of Technical Sciences, Associate Professor, e-mail: kataza@i.ua, ORCID: 0000-0002-1077-1402

Evgen Romanenko^A

Dr of Science in Public Administration, Professor, e-mail: poboss1978@gmail.com; ORCID: 0000-0003-2285-0543

Serhii Ilnitskyi^A

Research Fellow, e-mail: anastx85@icloud.com, ORCID: 0009-0009-3000-9034

^AЦентральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна

^BКафедра військової підготовки Державного університету "Київський авіаційний університет", м. Київ, Україна

^ACentral Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

^BDepartment of Military Training, State University "Kyiv Aviation University", Kyiv, Ukraine

Received: August 05, 2025 | Revised: August 25, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.5>

Мета роботи. Дослідити ключові тренди дипломатії безпеки України в післявоєнному світі, зокрема багатосторонні гарантії, економічну відбудову, протидію гібридним загрозам, оборонну кооперацію та наукову дипломатію, розробивши рекомендації для посилення ролі України в новій геополітичній реальності.

Метод дослідження. Історико-порівняльний метод.

Результати дослідження: виокремлено п'ять трендів: геополітична роль України, протидія гібридним загрозам, безпекові гарантії, економічна відбудова, наукова дипломатія.

Теоретична цінність дослідження. Формулювання концепції дипломатії стійкості України, що поєднує історичні уроки (Віденський конгрес) із сучасними викликами (переговори 2025 року, гібридні загрози), збагачуючи теорію міжнародних відносин і стратегій безпеки.

Тип статті. Теоретичний.

Purpose. To examine key trends in Ukraine's security diplomacy in the post-war world, including multilateral guarantees, economic reconstruction, countering hybrid threats, defense cooperation, and scientific diplomacy, providing recommendations to strengthen Ukraine's role in the new geopolitical reality.

Method. A historical-comparative method.

Findings. Five trends identified: Ukraine's geopolitical role, countering hybrid threats, security guarantees, economic reconstruction, and scientific diplomacy.

Theoretical implications. Development of Ukraine's resilience diplomacy concept, integrating historical lessons (Congress of Vienna) with modern challenges (2025 negotiations, hybrid threats), enriching theories of international relations and security strategies.

Paper type. Theoretical.

Ключові слова: Україна, дипломатія безпеки, геополітика, післявоєнна відбудова, гібридні загрози, Ініціатива трьох морів, переговори 2025 року, енергетична безпека.

Key words: Ukraine, security diplomacy, geopolitics, post-war reconstruction, hybrid threats, Three Seas Initiative, 2025 negotiations, energy security.

Вступ

Російська агресія проти України, розпочата в 2014 році та ескальована у 2022 році, стала поворотним моментом для глобальної безпеки, черговий раз виявивши неспроможність Ради

Безпеки ООН через право вето росії та підкресливши унікальну роль України як геополітичного опорного пункту, що формує нову безпекову архітектуру в Європі та Євразії [4, 5]. В такому контексті небезпека перемир'я чи миру з росією без гарантій, що здатні переважити, з одного боку, неефективність механізмів ООН та міжнародних договорів, на кшталт Будапештського меморандуму та мотивацію володимира путіна на продовження війни, з метою збереження своєї влади, з іншого. У післявоєнному контексті, на тлі мирних переговорів 2025 року, Україна постає активним суб'єктом, який через багатосторонні гарантії безпеки, економічну відбудову, протидію гібридним загрозам і наукову дипломатію може зміцнити національні інтереси та внести вклад у глобальний порядок. Хоча визначальною лишається загроза, сформульована у відомій, але недостовірно приписуваній Отто фон Бісмарку цитаті: угоди з росією не варті паперу, на якому написані.

Стаття спирається на праці Карла фон Клаузевіца [1], Збігнева Бжезінського [2], Володимира Горбуліна [3], а також звіти провідних аналітичних центрів – Інституту Брукінгса, Фонду Карнегі, Ради з міжнародних відносин (CFR), Центру стратегічних і міжнародних досліджень (CSIS), Корпорації RAND, Atlantic Council за 2022–2025 роки [4–9, 19–22].

Актуальність теми зумовлена потребою України адаптуватися до гібридних загроз, економічних викликів і геополітичної поляризації. Проблематика набуває більшої ваги через низку безуспішних спроб мирних переговорів 2025 року, що з плином часу тільки посилили відчуття дипломатичного песимізму, де вирішальну роль відіграє адміністрація Дональда Трампа, яка на початку серпня 2025 року обіцяла завершити війну за 10–50 днів, але зіткнулася з маніпулятивною поведінкою росії та занепокоєнням України щодо можливого виключення з процесу [10–12, 14]. Історичні паралелі, як-от Віденський конгрес 1815 року, що встановив баланс сил в континентальній Європі з участю Британії, хоча і на короткий термін, та абсолютно не враховував інтереси малих народів, чи стратегії стримування Холодної війни, підкреслюють потенціал України як “наріжного каменя” нової системи безпеки [13]. Спираючись на реалізм Карла фон Клаузевіца [1, с. 87], геостратегічне бачення Збігнева Бжезінського [2, с. 46] та ідеї Володимира Горбуліна про технологічну автономію [3], стаття визначає засадничі орієнтири формування й утвердження суб'єктності України на світовій геополітичній арені, що відповідають принципам міжнародного права, економічної та оборонної взаємозалежності та глобальної безпеки і матимуть шанс на реалізацію в світі постправди за рахунок силового контролю їхнього виконання.

Події серпня 2025 року — зокрема саміт Дональда Трампа та володимира путіна в Алясці 15 серпня, який не привів до домовленості про припинення вогню, а також зустріч Трампа із Зеленським та європейськими лідерами у Білому домі 18 серпня — продемонстрували потребу в єдності союзників і зваженому підході до переговорів.. Саміт на Алясці, проведений на базі Joint Base Elmendorf–Richardson не приніс прориву через тверду позицію росії щодо демілітаризації України, але зустріч в Білому домі продемонструвала підтримку України з боку США та Європи. Ці події вказують на потребу в новій дипломатії, яка враховує геополітичні ризики, як-от російські атаки на азербайджанські нафтові бази SOCAR в Одесі 7-8 серпня 2025 року, що загрожують безпеці регіону [25].

Метою статті є дослідження ключових трендів нової дипломатії безпеки України – від багатосторонніх гарантій безпеки, протидії гібридним загрозам, економічної відбудови, розвитку м'якої сили до наукової дипломатії та розроблення пропозицій для посилення ролі нашої держави в післявоєнному світі. Стаття пропонує рекомендації, які поєднують історичні уроки та сучасні виклики, щоб Україна могла утвердитися як активний учасник глобальної безпеки.

Для розуміння цих викликів, які стоять перед нашою державою, необхідно чітко окреслити проблеми, що формують її післявоєнну дипломатію безпеки, враховуючи як сучасні реалії, так і історичні паралелі.

Теоретичні основи дослідження

Дослідження базується на історико-порівняльному методі, зіставляючи сучасні виклики України з досвідом Віденського конгресу 1815 року та стратегіями Холодної війни [13]. Теоретичний фундамент формують праці Карла фон Клаузевіца про стратегічну невизначеність [1], Збігнєва Бжезінського про геополітичну роль України [2] та Володимира Горбуліна щодо технологічної автономії [3].

Аналітичну основу становлять звіти провідних дослідницьких центрів — Brookings, Carnegie, CFR, CSIS, RAND, Heritage та Atlantic Council за 2022–2025 роки [4–9, 19], а також актуальні матеріали провідних медіа (Reuters, BBC, NPR, *The New York Times*, *The Washington Post*) про мирні переговори 2025 року [10–12, 14, 17, 20–24].

Контент-аналіз офіційних документів (зокрема, комюніке саміту миру в Швейцарії 2024 року [12]), заяв НАТО [15] і Європейської Комісії [16] дозволяє виявити ключові тренди дипломатії безпеки. Оцінювання стратегій відбудови та безпеки здійснюється крізь призму принципів міжнародного права (ст. 2(4) Статуту ООН) і концепції економічної взаємозалежності (Horizon Europe, торгівля ресурсами) [12, 16].

Попри обмеження, пов'язані з мінливим характером переговорів та відсутністю доступу до закритих домовленостей, використання актуальних джерел і історичних паралелей забезпечує наукову достовірність.

Запропонована методологія дозволяє оцінити місце України в новій системі безпеки, враховуючи мирні ініціативи 2025 року, позицію адміністрації Дональда Трампа та глобальний контекст із залученням Китаю та Індії. Аналіз виділяє ключові тенденції безпекової дипломатії України, підкреслюючи її внесок у глобальну стабільність і переговорний процес.

Стаття орієнтована на міжнародних експертів, дослідників у сфері національної безпеки та державного управління й містить рекомендації, спрямовані на захист національних інтересів України в умовах формування нової архітектури безпеки.

Постановка проблеми

Російсько-українська війна оголила кризу глобального врядування, зокрема неспроможність міжнародного співтовариства виконати статтю 2(4) Статуту ООН [4, 5]. Україна стикається з багатошаровими викликами.

По-перше, гібридними загрозами, як-от кібератаки по типу штучних блекаутів енергомережі у 2015 році, спричинених хакерською групою фсб росії “Sandworm” (піщаний хробак) [6, 26], економічною дестабілізацією через блокаду портів 2022 року, яка спричинила глобальну продовольчу кризу, та потребою юридично закріплених гарантій безпеки з можливістю їх примусового контролю союзами країн на кшталт Віденського 1815 року, вірогідно, частково поза межами нинішньої неефективної системи ООН [10, 11].

По-друге, Росія використовує мирні переговори як інструмент маніпуляцій і затягування часу, висувуючи від початку нереалістичні умови. З одного боку, це спрямовано на підрив єдності США, Європи та України, з іншого — виконує роль внутрішнього PR, створюючи образ “сили”, яку нібито визнає й боїться світ. У 2025 році на переговорах у Стамбулі остаточно проявилися глибокі розбіжності: Москва наполягає на вимогах, що суперечать основоположним нормам міжнародного права, зокрема принципу непорушності кордонів (Ст. 2, п. 4 Статуту ООН), Декларації принципів міжнародного права (резолюція ГА ООН 2625 (XXV) від 24 жовтня 1970 р.), Гельсінському заключному акту 1975 р. (п. III “Непорушність кордонів”). Йдеться про вимогу демілітаризації України та визнання анексії Криму. Київ, своєю чергою, наполягає на виведенні російських військ і гарантіях безпеки — через НАТО або двосторонні угоди. Цю позицію ускладнює фактор Дональда Трампа, який демонструє готовність до діалогу з путіним, але натрапляє на відвертий опір Росії [10, 12, 14].

Карл фон Клаузевіц описував “туман війни” як невизначеність, що ускладнює стратегічне планування [1, с. 119]. Сьогодні це проявляється в дезінформаційних кампаніях, кібератаках і геополітичній конкуренції, подібній до Холодної війни, коли Захід стримував СРСР через економічний тиск і альянси [13]. Роль Трампа, який, за джерелами, захоплюється стилем лідерів на кшталт Сі Цзіньпіна й путіна з їхньою концентрацією влади за демократичним фасадом, викликає занепокоєння в Європі щодо можливих компромісів, що можуть не враховувати інтереси України, як це було в минулих переговорах [11, 14, 20]. Водночас економічна безпека, як підкреслює Володимир Горбулін, є основою стійкості, що вимагає регіональної співпраці з Польщею, Литвою, Естонією та залучення не західних партнерів, таких як Індія [3, 18]. Актуальність роботи по напрямку Індії зростає в зв’язку з явним охолодженням Індо-російських стосунків в зв’язку з посиленням осі Китай-росія.

Центральне питання: як Україні, зберігаючи національні інтереси, сформувати дипломатію безпеки в умовах мирних переговорів, де США відіграють провідну роль, а росія зберігає агресивну позицію? Росія, сподіваючись відтворити імперію через захоплення України та створити альянс з Китаєм і КНДР, може схвалити перемир’я лише як паузу для підготовки нового наступу, що підкреслює ризики для глобальної безпеки [4, 11]. Україна повинна протидіяти цьому не тільки через принципи міжнародного права, а і через нові союзи в Балтійсько-Чорноморсько-Адріатичному трикутнику, користуючись економічною дипломатією та враховуючи потенціал впливу на росію через зміну конфігурації сил на Кавказі.

Для вирішення цих проблем необхідний науковий підхід, який поєднує історичний досвід із сучасними аналітичними інструментами, щоб забезпечити достовірність аналізу.

Результати

1. Багатосторонні гарантії безпеки

“Ініціатива трьох морів” (ITM), або Тримор’я, – це платформа 13 країн ЄС (Австрія, Болгарія, Хорватія, Чехія, Естонія, Угорщина, Латвія, Литва, Польща, Румунія, Словаччина, Словенія, Греція) та України як асоційованого члена з 2023 року, спрямована на розвиток енергетики, транспорту й цифрової інфраструктури між Балтійським, Адріатичним і Чорним морями, з інвестиційним фондом до €100 млрд для посилення економічної взаємозалежності та безпеки в регіоні [1, 7, 10]. Для України ITM є інструментом інтеграції до ЄС, залучення інвестицій і співпраці з Польщею, Литвою та Естонією, подібно до коаліцій Холодної війни [10, 18].

Гарантії безпеки можуть бути зміцнені ініціативою протидії росії у військово-стратегічному аспекті, створенням поясу безпеки Балтика–Чорне море (BBM Security Belt) та поступовій інтеграції оборонних систем Польщі, країн Балтії, України, Румунії у єдиний західноцентричний захисний пояс, в перспективі з єдиною військовою доктриною регіону.

Президент США Дональд Трамп 6 серпня 2025 року запропонував тристоронню зустріч із путіним і Зеленським для припинення війни, що свідчить про прагнення до дипломатичного вирішення [8, 15, 17]. Виконання угод, навіть якщо вони будуть досягнуті, залишається в сфері найбільших ризиків.

Російська пропозиція “перемир’я в небі” 2025 року, за даними РБК-Україна та Bloomberg, передбачає припинення повітряних ударів, але брак конкретики вказує на тактику затягування переговорів, як у Стамбулі навесні 2025 року, щоб уникнути санкцій ЄС [13, 17, 20, 21]. CFR і Brookings пропонують юридичні гарантії безпеки, як угоди зі США та Великою Британією 2024 року про військову підтримку й спільне виробництво [5, 7, 15]. Україні слід наполягати на включенні до всіх форматів переговорів, спираючись на статтю 2(4) Статуту ООН про суверенітет [11, 14].

Польща, яка виступає за миротворчі сили НАТО, і Литва через “Ініціативу трьох морів” зміцнюють позиції України [10, 18]. Історичні коаліції Віденського конгресу 1815 року показують, що спільні гарантії сильних країн стримують агресію [13]. Нагадаємо, Віденський

конгрес (вересень 1814 – червень 1815) був міжнародною конференцією провідних європейських держав, скликаною після поразки Наполеона для відновлення політичної стабільності в Європі.

Визначальними рішеннями цієї міжнародної конференції стали:

територіальний перерозподіл: Франція повернулася до кордонів 1792 року; Пруссія отримала частину Саксонії та Рейнську область; Австрія — Ломбардію та Венецію; Росія — більшу частину Польщі (Царство Польське); Велика Британія — нові заморські колонії;

запровадження системи балансів сил: створено *Concert of Europe* — механізм колективного підтримання миру між провідними державами;

відновлення монархій: проголошено принцип легітимізму, який передбачав повернення династій, усунених революціями та Наполеоном.

У підсумку Конгрес заклав “віденську систему” міжнародних відносин, яка забезпечила відносну стабільність у Європі майже на 40 років.

Віденський конгрес 1815 року продемонстрував, що коаліційна дипломатія та баланс сил можуть забезпечити стабільність після масштабних конфліктів. Для України це урок про необхідність створення міцних регіональних і глобальних альянсів, як-от через НАТО чи “Ініціативу трьох морів”, для гарантування безпеки та протидії гібридним загрозам росії в новій геополітичній реальності.

Отже, Україні й далі необхідно разом з міжнародними союзниками домагатися санкцій і юридичних зобов’язань, від партнерів, щоб захистити інтереси та сприяти новій безпековій архітектурі, що характеризується невідворотністю настання наслідків для порушників угод.

2. Відновлення як безпекова дипломатія

За оцінками RAND, відбудова України є інвестицією у стабільність Європи, що потребує системних антикорупційних реформ та інтеграції у глобальні ринки [8]. Володимир Горбулін підкреслює, що економічна стійкість є фундаментом безпеки: зокрема, блокада українських портів у 2022 році спричинила кризу продовольчих ланцюгів у країнах Глобального Півдня [3].

Серед ключових партнерів у процесі відбудови вирізняються Польща, яка у 2024 році інвестувала €2 млрд, та Литва, що розвивають енергетичні проекти в межах “Ініціативи трьох морів” [8, 18]. Подібно до Плану Маршала 1948–1952 років, коли провідні європейські країни координували дії під американським патронатом, сьогодні саме Польща та Литва виступають каталізаторами євроінтеграційних процесів України в межах ЄС та НАТО.

Ця історична паралель між сучасним відновленням України та підтримки цих дружніх країн та “Планом Маршала” після Другої світової війни полягає у спільні логіці: економічна допомога та політичне партнерство розглядаються не лише як акт солідарності, а як інвестиція в безпеку регіону. Як “План Маршала” був елементом стримування СРСР, так і підтримка України є інструментом стримування російської агресії. В обох випадках мета – швидке відновлення економіки та інфраструктури з одночасним укріпленням політичної стабільності. Таким чином, підтримка України Литвою та Польщею є сучасним регіональним аналогом “Плану Маршала”, спрямованим на відновлення економіки та зміцнення безпеки, але реалізується під час війни та акцентом на інтеграцію й колективну оборону.

“План перемоги” президента України Володимира Зеленського 2024 року пропонує використання ресурсів (літій, уран) з ЄС і США, що відповідає економічній взаємозалежності та зміцнює позиції України [12, 21].

“Ініціатива трьох морів” формує альянс, який протидіє впливу росії та Китаю, що постачає їй технології [4, 18]. Україні слід залучати інвестиції через “Ініціативу трьох морів” для зеленої енергетики та інфраструктури, щоб прискорити відновлення та зміцнити роль у глобальній економіці, захищаючи національні інтереси [12]. Необхідно забезпечити економічну відбудову потужності України як основу воєнної спроможності відбити наступний

вірогідний напад росії своїми силами та нанести несумісне з можливостями вести наступальну війну ураження силам вторгнення рф.

3. Інформаційна війна, гібридна війна та війна у кіберпросторі

Гібридні загрози, як кібератака 2015 року на енергомережу України, є потужним викликом, зазначають CSIS і Brookings [6, 7]. Центр протидії дезінформації України (2021) співпрацює з Естонією, яка пережила кібератаки 2007 року, для зміцнення безпеки [14]. Всі пропозиції росії, не охоплюють кібербезпеку, а їх тактичний характер, за РБК-Україна, спрямований на затягування переговорів [13, 17, 20].

Російські плани ракетних ударів по Японії через системи Type 12 і MRC Typhon, оприлюднені Voennaya Khronika, підкреслюють глобальну гібридну війну [23]. Україні слід долучитися до протидії через НАТО та “Ініціативи трьох морів” з Польщею й Литвою [15, 18]. Свого часу Карл фон Клаузевіц описував “фрикцію” війни, що нині проявляється в дезінформації та кібератаках [1, с. 119].

Україна має включити кібербезпеку до мирних угод, використовуючи досвід Естонії та підтримку “Ініціативи трьох морів” [14, 18]. Без санкцій ЄС росія безумовно продовжить гібридну агресію, використовуючи “перемир’я” як маневр [13, 17, 22].

Враховуючи “непереговороспроможну” поведінку росії, одних лише захисних дій не достатньо. Сама по собі тактика оборони – програвша. За влучним виразом Герберта Макмастера: “... для протидії російській дезінформації захисних заходів недостатньо”. “Сполучені Штати, європейські та інші демократичні країни мають визнати, що поборювання “методички Путіна” потребує рішучих колективних дій” [27]. Партнери нашої держави мають не тільки наголошувати про наявність кіберзагроз з боку росії та її союзників, а й напрацювати дієві механізми підтримки кібербезпеки за рахунок атакуювальних дій, коли сама думка нападати у агресора не виникне. Страх перед контрударом коаліції має перевершувати страх ядерної зброї.

Це вимагає активної дипломатії для захисту інтересів і сприяння гарантуванню глобальної безпеки.

4. Оборонно-промислова кооперація

Угода з Lockheed Martin 2024 року щодо дронів зменшує залежність України від зовнішньої допомоги [6, 9, 15]. Володимир Горбулін акцентує на R&D для технологічної автономії [3]. “Ініціативи трьох морів”, через проєкти Польщі та Литви з виробництва боєприпасів, інтегрує Україну до глобальних ланцюгів постачання, як це було в Західній Європі після 1945 року [8, 18].

Російські загрози Японії підкреслюють необхідність оборонної автономії [23]. Тому Україні слід розширити кооперацію з США та “Ініціативи трьох морів”, щоб протидіяти загрозам [15, 18].

“Ініціативи трьох морів” підвищує вагу України в переговорах, демонструючи її внесок у безпеку [18]. Спільне виробництво з партнерами зміцнить роль України в новій безпековій архітектурі, захищаючи її інтереси.

5. Дивергенція західних підходів

Carnegie зазначає розбіжності: Heritage Foundation підтримує ринкові реформи, CFR – санкції та гарантії [4, 5, 9]. США надали \$61 млрд у 2024 році, але дебати в ЄС щодо приватизації гальмують інвестиції [15]. Тристороння пропозиція Трампа зіткнулася з опором росії, яка відкидає миротворчі сили НАТО, запропоновані Францією та Великою Британією [8, 10, 15].

Звичайно російські пропозиції є спробою затягнути переговори, як у Стамбулі навесні 2025 року, щоб уникнути санкцій [13, 17, 20, 22]. Україні слід вести паралельні переговори, як під час Холодної війни, коли Захід координував стримування СРСР [13]. Польща та Литва через “Ініціативи трьох морів” підтримують інтеграцію України до НАТО [18].

Україна має використовувати міжнародне право та “Ініціативи трьох морів”, щоб узгодити західні підходи та забезпечити свою участь у переговорах, захищаючи інтереси [18].

6. Геополітична логіка Збігнева Бжезінського

Бжезінський називав Україну “геополітичним опорним пунктом” Євразії [2, с. 46]. CFR підкреслює її роль у зміцненні флангу НАТО, а тристороння пропозиція Трампа підтверджує її значення [5, 8, 15]. Вплив Китаю, який постачає росії технології, та нейтралітет Індії ускладнюють переговори, тоді як загрози росії Японії розширюють конфлікт [4, 23].

Atlantic Council вважає НАТО інструментом стримування, але без санкцій ЄС росія може ескалувати, використовуючи розмиті пропозиції як маневр, як у Стамбулі [10, 13, 19, 22]. Україні слід зміцнювати альянси з “Ініціативи трьох морів” (Польща, Балтія) і залучати Індію, щоб зменшити вплив Китаю [4, 18], що сприятиме безпековій архітектурі.

Україні необхідно наполягати на своїй ролі в переговорах, спираючись на міжнародне право та “Ініціативи трьох морів”, щоб сприяти безпековій архітектурі та захистити інтереси [18].

У своїх працях Збігнев Бжезінський підкреслював, що незалежна й стабільна Україна є визначальним фактором європейської та глобальної безпеки. Він аргументував, що без України росія зберігає імперський потенціал з Україною, інтегрованою в євроатлантичний простір, континентальна безпекова система стає значно міцнішою. Ця стратегічна логіка прямує корелює з міжнародно-правовим підходом до захисту національних інтересів: участь України у формуванні рішень, що визначають майбутню безпекову архітектуру, є не лише політичним правом, а й юридичною необхідністю, закріпленою принципами Статуту ООН, Гельсінського заключного акту та Віденської конвенції про право міжнародних договорів.

Виходячи з основоположних засад міжнародного права Україна має наполягати на активній і рівноправній ролі у будь-яких переговорах, що стосуються завершення війни та майбутньої безпекової архітектури, з таких причин:

1. Принцип суверенної рівності держав.

Відповідно до ст. 2 п. 1 Статуту ООН, усі держави є рівними в правах і зобов’язані брати участь у вирішенні питань, що безпосередньо зачіпають їхній суверенітет і територіальну цілісність. Ігнорування України у процесі означало б порушення цього фундаментального принципу.

2. Право на самовизначення та недоторканність кордонів.

Закріплене у Гельсінському заключному акті 1975 року та Резолюції ГА ООН 2625 (XXV), право українського народу самостійно визначати своє політичне майбутнє виключає можливість ухвалення рішень без його згоди.

3. Принцип pacta tertiis nec nocent nec prosunt.

Відповідно до Віденської конвенції про право міжнародних договорів 1969 року, міжнародні угоди не можуть покладати права чи обов’язки на третю сторону без її згоди. Тому будь-які домовленості, укладені без участі України, не матимуть для неї юридичної сили.

4. Безпекова архітектура як спільна відповідальність.

Формування нових регіональних або глобальних механізмів безпеки (аналогічно Гельсінському процесу) потребує участі всіх зацікавлених сторін. Україна, як держава, що стала ключовим чинником європейської безпеки, повинна бути співтворцем цих механізмів, щоб гарантувати їхню ефективність та відповідність власним інтересам.

5. Захист національних інтересів через міжнародно-правові гарантії.

Участь у переговорах дозволяє інтегрувати в угоди положення про конкретні гарантії безпеки, відшкодування шкоди та механізми відповідальності агресора, що неможливо забезпечити без прямої присутності України за столом переговорів.

З огляду на це, ігнорування України в мирних чи безпекових переговорах суперечить базовим принципам міжнародного права та знижує легітимність майбутньої безпекової

архітектури. Тому рівноправна участь забезпечить не лише захист національних інтересів, а й стійкість нової системи безпеки в Європі.

7. Наукова дипломатія та технологічна автономія.

Володимир Горбулін підкреслює, що дослідження та розробки (R&D) є фундаментом безпеки, особливо в аерокосмічній сфері [3]. Програма Horizon Europe, яка у 2023 році виділила €100 млн, підтримує розвиток кібербезпеки та зеленої енергетики, виступаючи прикладом наукової дипломатії [16]. Співпраця України з CERN та Індією у високотехнологічних проєктах, за аналогією з Манхеттенським проєктом, спрямована на протидію впливу Китаю [4, 8, 16].

Співробітництво України з CERN та Індією має стратегічний ефект, подібний до ролі Манхеттенського проєкту у зміні балансу сил під час Другої світової війни. Як тоді зосередження наукового потенціалу провідних держав забезпечило технологічний прорив і визначило геополітичну перевагу, так нині спільні науково-технологічні ініціативи з високотехнологічними партнерами здатні створити критичні компетенції, що зменшують залежність від китайських технологій і формують альтернативні центри інноваційної потуги у світі. Це не лише розширює власну науково-промислову базу, а й зміцнює позиції України у глобальній конкуренції за технологічне лідерство.

Російські загрози Японії підкреслюють необхідність технологічної автономії [23]. Фонд Карнегі бачить у науковій дипломатії інструмент врядування [4]. Тому Україна має залучати інвестиції для інновацій, щоб посилити економічну інтеграцію та нову безпекову архітектуру, захищаючи інтереси [18].

8. Ризики та виклики.

Політична нестабільність у США, зокрема зміна пріоритетів адміністрації Трампа, може послабити підтримку, як під час Холодної війни [13]. Корупція в Україні (індекс Transparency International 2024 року – 36/100) ускладнює реформи та відбудову [17]. Вплив Китаю, який постачає росії технології, та нейтралітет Індії створюють дипломатичні виклики [4].

Російські атаки на азербайджанські нафтові бази SOCAR в Одесі 7–8 серпня 2025 року, за допомогою дронів Shahed, є прикладом геополітичної ескалації, що загрожує енергетичній безпеці регіону [24]. Азербайджан засудив удари та розглядає зняття ембарго на постачання зброї Україні, що може посилити напругу на Кавказі [24]. Україні слід протидіяти таким ризикам через “Ініціативи трьох морів” з Польщею та Балтією [18]. Ініціативи РФ, спрямовані на відтермінування санкцій, підкреслюють потребу в санкціях і включенні України до переговорів [10, 13, 22].

Виявлені тренди та ризики підкреслюють важливість м’якої сили та наукової дипломатії для зміцнення ролі України в мирних переговорах і глобальній безпеці.

Висновки

Російсько-українська війна та мирні переговори 2025 року підкреслюють роль України як суб’єкта нової безпекової архітектури. Тренди – багатосторонні гарантії, відбудова, гібридні загрози, оборонна кооперація, дивергенція підходів, геополітична роль, наукова дипломатія – показують її потенціал. Готовність президента США Дональда Трампа вести діалог з путіним свідчать про прагнення до миру, але російський лідер, сподіваючись відтворити імперію через альянс з Китаєм і КНДР, може знову наполягати на перемир’ї як паузу для підготовки, що вимагає обережності [4, 11].

Тристороння пропозиція Трампа для зустрічі з путіним і Зеленським може стати кроком до миру, але вимагає обережності, щоб уникнути ірраціональної віри в швидке вирішення, як у минулих ініціативах.

Історичні уроки, як-от Віденський конгрес, підкреслюють важливість коаліційної дипломатії для стабільності [10,13]. Останні події, як-от відсутність угоди на саміті Трампа та Путіна в Алясці 15 серпня 2025 року та зустріч Трампа з Зеленським і європейськими лідерами

в Білому домі 18 серпня 2025 року, демонструють прогрес у єдності союзників щодо України. [28, 29].

Дискусії щодо нових гарантій безпеки для України від США викликають не лише надію, а й закономірний скептицизм. Український досвід Будапештського меморандуму 1994 року чітко засвідчив, що навіть письмові міжнародні зобов'язання провідних держав світу можуть залишитися декларативними. Тоді обіцянки поважати суверенітет і територіальну цілісність України не завадили росії порушити ці домовленості, спершу анексувавши Крим, а згодом розпочавши повномасштабне вторгнення у 2022 році. Цей факт закономірно породжує занепокоєння: чи не повториться історія, коли безпекові документи залишаться інструментом дипломатії без реальних механізмів стримування агресора?

Рекомендації:

1. **Забезпечити повноцінну участь України в переговорах**, спираючись на принципи суверенітету, закріплені у статті 2(4) Статуту ООН, щоб уникнути небезпечних компромісів, подібних до ситуації на саміті в Алясці [10, 12].

2. **Зміцнювати регіональні альянси** через “Ініціативу трьох морів” у співпраці з Польщею, Литвою та Естонією для поглиблення інтеграції з НАТО та ЄС, а також залучення інвестицій [15, 18].

3. **Посилювати протидію гібридним загрозам і розвивати кібербезпеку** разом з Естонією. Паралельно — створювати власні кіберзасоби стримування у взаємодії з союзниками, аби росія більше остерігалася контрудару, ніж навіть ядерного стримування [14].

4. **Розвивати економічну дипломатію** через використання стратегічних ресурсів (літій, уран) і участь у проєктах Horizon Europe. Важливо залучати Індію як партнера для протидії впливу Китаю, диверсифікації ринків і зменшення технологічної залежності [4, 16].

5. **Просувати реформування ООН та створення дієвих регіональних альянсів**, зокрема “Ініціативи трьох морів”, для стримування Росії, враховуючи ймовірні провокації на Кавказі. Доцільно також формувати воєнно-економічний союз держав “поясу безпеки” проти агресії РФ, розуміючи її непоступливу та “непереговороспроможну” поведінку [4, 18].

На переконання авторів дослідження, Україна має шанс не лише відновитися після війни, але й стати **лідером у формуванні нової архітектури безпеки в Європі та світі**. Подібно до періоду після наполеонівських воєн, коли держави створювали новий порядок, Україна може використати історичні уроки та сучасні можливості з рішучістю та стратегічною мудрістю.

Останні переговори в Алясці, а також зустріч президента України Володимира Зеленського з президентом США Дональдом Трампом та європейськими лідерами у Білому домі, засвідчили потенціал для єдності союзників. Водночас справжнє припинення агресії можливе лише за умови **посилення санкційного тиску**. Складність досягнення миру підкреслює і думка Карла фон Клаузевіца: *“На війні все дуже просто. Але найпростіше виявляється найскладнішим”*.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Клаузевіц К. Про війну / пер. з нім. — Київ : КМ-Букс, 2018. — 432 с.
2. Brzezinski Z. The Grand Chessboard: American Primacy and Its Geostrategic Imperatives. — New York : Basic Books, 1997. — 240 p.

3. Горбулін В. Гібридна війна як виклик національній безпеці України // Національна безпека і оборона. – 2022. – № 1–2. – С. 10–20.
4. Carnegie Endowment for International Peace. Global Security Analysis [Електронний ресурс]. – 2025. – URL : <https://carnegieendowment.org> (дата звернення: 19.08.2025).
5. Council on Foreign Relations. Ukraine and the Future of European Security [Електронний ресурс]. – 2024. – URL : <https://www.cfr.org> (дата звернення: 19.08.2025).
6. Center for Strategic and International Studies. Cyber Threats and Ukraine: Lessons for NATO [Електронний ресурс]. – 2022. – URL : <https://www.csis.org> (дата звернення: 19.08.2025).
7. Brookings Institution. Ukraine's Public Diplomacy in Wartime [Електронний ресурс]. – 2023. – URL : <https://www.brookings.edu> (дата звернення: 19.08.2025).
8. RAND Corporation. Post-War Scenarios for Ukraine [Електронний ресурс]. – 2024. – URL : <https://www.rand.org> (дата звернення: 19.08.2025).
9. Reuters. Trump wants deal to end Russia's war in Ukraine by Aug. 8, US tells UN [Електронний ресурс]. – 2025. – URL : <https://www.reuters.com> (дата звернення: 19.08.2025).
10. Wikipedia. Peace negotiations in the Russian invasion of Ukraine [Електронний ресурс]. – 2025. – URL : <https://en.wikipedia.org> (дата звернення: 19.08.2025).
11. BBC News. Putin not swayed by Trump's Ukraine war ultimatum [Електронний ресурс]. – 2025. – URL : <https://www.bbc.com> (дата звернення: 19.08.2025).
12. NATO. Defence Planning Process [Електронний ресурс]. – 2023. – URL : <https://www.nato.int> (дата звернення: 19.08.2025).
13. European Commission. Horizon Europe: Ukraine's Participation [Електронний ресурс]. – 2023. – URL : <https://ec.europa.eu> (дата звернення: 19.08.2025).
14. Transparency International. Corruption Perceptions Index [Електронний ресурс]. – 2024. – URL : <https://www.transparency.org> (дата звернення: 19.08.2025).
15. National Security and Defense Council of Ukraine. Center for Countering Disinformation [Електронний ресурс]. – 2021. – URL : <https://www.rnbo.gov.ua> (дата звернення: 19.08.2025).
16. Polish Ministry of Foreign Affairs. Poland's Support for Ukraine's Reconstruction [Електронний ресурс]. – 2024. – URL : <https://www.gov.pl> (дата звернення: 19.08.2025).
17. Atlantic Council. A Plan for Peace Through Strength in Ukraine [Електронний ресурс]. – 2025. – URL : <https://www.atlanticcouncil.org> (дата звернення: 19.08.2025).
18. The New York Times. Trump's Envoy Is Expected to Visit Russia as U.S. Pushes for Peace Deal in Ukraine [Електронний ресурс]. – 2025. – URL : <https://www.nytimes.com> (дата звернення: 19.08.2025).
19. NPR. Trump slams Zelenskyy over Russia-Ukraine peace terms [Електронний ресурс]. – 2025. – URL : <https://www.npr.org> (дата звернення: 19.08.2025).
20. Reuters. Trump officials eye a longer road to Ukraine peace as frustration mounts [Електронний ресурс]. – 2025. – URL : <https://www.reuters.com> (дата звернення: 19.08.2025).
21. Voennaya Khronika. Russian military analysts examine missile strike options against Japan [Електронний ресурс]. – 2025. – URL : <https://voenkhronika.ru> (дата звернення: 19.08.2025).
22. The Washington Post. Trump's Admiration for Authoritarian Leaders and Its Impact on U.S. Diplomacy [Електронний ресурс]. – 2025. – URL : <https://www.washingtonpost.com> (дата звернення: 19.08.2025).
23. Foreign Policy. Putin's Strategy to Rebuild the Russian Empire Through Alliances with China and North Korea [Електронний ресурс]. – 2025. – URL : <https://foreignpolicy.com> (дата звернення: 19.08.2025).
24. Politico. Europe's Nervousness Over Potential U.S. Compromises in Ukraine Talks [Електронний ресурс]. – 2025. – URL : <https://www.politico.com> (дата звернення: 19.08.2025).

25. Al Jazeera. Russian Drone Attacks on Azerbaijan's SOCAR Facilities in Odesa [Електронний ресурс]. – 2025. – URL : <https://www.aljazeera.com/news/2025/8/8/russia-drone-attacks-azerbaijan-socar-facilities-odesa-ukraine> (дата звернення: 19.08.2025).
26. Greenberg A. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. – New York : Knopf Doubleday Publishing Group, 2019. – 368 p. – ISBN 978-0-385-54440-5.
27. Макмастер Г. Поля битв. Борьба за захист вільного світу / пер. з англ. Н. Коваль. – Київ : Наш Формат, 2023. – 58 с. – ISBN 978-617-8120-15-3.
28. The New York Times. Trump Returns to Washington After Putin Talks Yield No Ukraine Deal [Електронний ресурс]. – 2025. – URL : <https://www.nytimes.com/2025/08/18/trump-putin-ukraine-talks-alaska.html> (дата звернення: 19.08.2025).
29. Reuters. Trump officials eye a longer road to Ukraine peace as frustration mounts [Електронний ресурс]. – 2025. – URL : <https://www.reuters.com> (дата звернення: 19.08.2025).

References

1. Clausewitz, C. von. (2018). *On war* (Ukrainian transl.). Kyiv: KM-Books.
2. Brzezinski, Z. (1997). *The grand chessboard: American primacy and its geostrategic imperatives*. New York: Basic Books.
3. Horbulin, V. (2022). Hybrid war as a challenge to Ukraine's national security. *National Security and Defense*, 1–2, 10–20.
4. Carnegie Endowment for International Peace. (2025). *Global security analysis*. Available from : <https://carnegieendowment.org>
5. Council on Foreign Relations. (2024). *Ukraine and the future of European security*. Available from : <https://www.cfr.org>
6. Center for Strategic and International Studies. (2022). *Cyber threats and Ukraine: Lessons for NATO*. Available from : <https://www.csis.org>
7. Brookings Institution. (2023). *Ukraine's public diplomacy in wartime*. Available from : <https://www.brookings.edu>
8. RAND Corporation. (2024). *Post-war scenarios for Ukraine*. Available from : <https://www.rand.org>
9. Reuters. (2025, August). Trump wants deal to end Russia's war in Ukraine by Aug. 8, US tells UN. Available from : <https://www.reuters.com>
10. Wikipedia. (2025). *Peace negotiations in the Russian invasion of Ukraine*. Available from : <https://en.wikipedia.org>
11. BBC News. (2025, August). Putin not swayed by Trump's Ukraine war ultimatum. Available from : <https://www.bbc.com>
12. NATO. (2023). *Defence planning process*. Available from : <https://www.nato.int>
13. European Commission. (2023). *Horizon Europe: Ukraine's participation*. Available from : <https://ec.europa.eu>
14. Transparency International. (2024). *Corruption perceptions index*. Available from : <https://www.transparency.org>
15. National Security and Defense Council of Ukraine. (2021). *Center for countering disinformation*. Available from : <https://www.rnbo.gov.ua>
16. Polish Ministry of Foreign Affairs. (2024). *Poland's support for Ukraine's reconstruction*. Available from : <https://www.gov.pl>
17. Atlantic Council. (2025). *A plan for peace through strength in Ukraine*. Available from : <https://www.atlanticcouncil.org>
18. The New York Times. (2025, August). Trump's envoy is expected to visit Russia as U.S. pushes for peace deal in Ukraine. Available from : <https://www.nytimes.com>

19. NPR. (2025, August). Trump slams Zelenskyy over Russia-Ukraine peace terms. Available from : <https://www.npr.org>
20. Reuters. (2025, August). Trump officials eye a longer road to Ukraine peace as frustration mounts. Available from : <https://www.reuters.com>
21. Voennaya Khronika. (2025). Russian military analysts examine missile strike options against Japan. Available from : <https://voenkhronika.ru>
22. The Washington Post. (2025, August). Trump's admiration for authoritarian leaders and its impact on U.S. diplomacy. Available from : <https://www.washingtonpost.com>
23. Foreign Policy. (2025, August). Putin's strategy to rebuild the Russian empire through alliances with China and North Korea. Available from : <https://foreignpolicy.com>
24. Politico. (2025, August). Europe's nervousness over potential U.S. compromises in Ukraine talks. Available from : <https://www.politico.com>
25. Al Jazeera. (2025, August 8). Russian drone attacks on Azerbaijan's SOCAR facilities in Odesa. Available from : <https://www.aljazeera.com/news/2025/8/8/russia-drone-attacks-azerbaijan-socar-facilities-odesa-ukraine>
26. Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. New York: Knopf Doubleday Publishing Group. ISBN 978-0-385-54440-5.
27. McMaster, H. R. (2023). *Battlegrounds: The fight to defend the free world* (N. Koval, Trans.). Kyiv: Nash Format. ISBN 978-617-8120-15-3.
28. The New York Times. (2025, August 18). Trump returns to Washington after Putin talks yield no Ukraine deal. Available from : <https://www.nytimes.com/2025/08/18/trump-putin-ukraine-talks-alaska.html>
29. Reuters. (2025, August). Trump officials eye a longer road to Ukraine peace as frustration mounts. Available from : <https://www.reuters.com>

The Generational Division of Warfare and Controversial Issues

Класифікація воєн за поколіннями та дискусійні аспекти

Zafar Nuri Najafov

PhD in National Security and Military Sciences, e-mail: zafarnajafov@yahoo.com, ORCID: 0000-0002-1392-9359

National Defence University, Republic of Azerbaijan

Зафар Нури Наджафов

Доктор філософії з національної безпеки та військових наук, e-mail: zafarnajafov@yahoo.com, ORCID: 0000-0002-1392-9359

Національний університет оборони, Азербайджан

Received: August 17, 2025 | Revised: August 30, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.6>

Purpose. To identify the transformational trends and controversial points of the changing face of military violence in the context of the concept of “Generations of warfare”.

Method. Historical, comparative analysis, systematic approach, and structural analysis methods.

Findings. Although the concept of “Generations of warfare” allows for a systematic study of the transformations from the classical to the hybrid form of military violence, and for the identification of the specific developmental determinants of different conflict generations, it should not be considered perfect. The incompleteness of generations of warfare, the lack of fundamental differences between some generations, is considered a new challenge to this concept.

Theoretical implications. The concept of “Generations of warfare”, put forward by Lind in 1989, does not keep pace with modern military developments and armed conflicts, the concept of “generations of warfare” is not defined by clear boundaries. This theory is unable to explain the subsequent transformation of methods and means of military operations, the decisive impact of non-kinetic means – drones, artificial intelligence and cyberattacks – on military skill, as well as the essence of technology-based cyberwarfare and hybrid wars. This gap has been filled in the study of 5th generation warfare.

Practical implications. The concept of “Generations of warfare” has had a significant impact on the improvement of combat equipment, the emergence of new tactics, and the transformation of military skills. With the help of the concept of “Generations of warfare”, practitioners can study the dynamics of military and military-practical transformations that have marked a huge period in human history, from the classical form of military violence to the hybrid form and become familiar with the shortcomings in this direction.

Value. This article aims to study the dominant strategies and technologies of each generation of warfare in the context of the concept of “Generations of Warfare”, to explain the problematic aspects and to improve it in accordance with the requirements of new transformations.

Paper type. theoretical.

Мета дослідження. Визначити трансформаційні тенденції та дискусійні аспекти змінюваного обличчя воєнного насильства в контексті концепції “поколінь війни”.

Метод дослідження. методи історичного, порівняльного аналізу, системного підходу та структурного аналізу.

Результати дослідження. Хоча концепція “поколінь війни” дозволяє системно досліджувати трансформації від класичної до гібридної форми воєнного насильства та виявляти специфічні детермінанти розвитку різних поколінь конфліктів, її не слід вважати досконалою. Незавершеність теорії поколінь війни, відсутність фундаментальних відмінностей між деякими поколіннями розглядається як новий виклик цій концепції.

Теоретична цінність дослідження. Концепція “поколінь війни”, висунута Ліндом у 1989 році, не встигає за сучасними військовими трансформаціями та збройними конфліктами, оскільки не визначена чіткими межами. Ця теорія не здатна пояснити подальшу еволюцію методів і засобів воєнних дій, вирішальний вплив некінетичних засобів — дронів, штучного інтелекту та кібератак — на військову майстерність, а також сутність технологічно обумовленої кібер- та гібридної війни. Цю прогалину частково заповнює вивчення війни п'ятого покоління.

Практична цінність дослідження. Концепція “поколінь війни” суттєво вплинула на вдосконалення бойового оснащення, появу нових тактик та трансформацію військової майстерності. За її допомогою практики можуть досліджувати динаміку воєнних і воєнно-практичних трансформацій, що охопили значний період в історії людства — від класичної форми воєнного насильства до гібридної, — а також ознайомитися з її недоліками у цьому напрямі.

Цінність дослідження. Стаття має на меті дослідити домінантні стратегії та технології кожного покоління війни в контексті концепції “поколінь війни”, пояснити проблемні аспекти та вдосконалити її відповідно до вимог нових трансформацій.

Тип статті. теоретичний.

Key words: generations of warfare, transformation, linear strategy, hybrid warfare, blitzkrieg.

Ключові слова: покоління війни, трансформація, лінійна стратегія, гібридна війна, блицкриг.

Introduction

Human history is the history of warfares. Military violence has played a unique role in the formation of this history. On the one hand, war is associated with bloody events – mass murder of people as a result of the collapse of states, enslavement, the spread of infectious diseases, on the other hand,

it is marked by the emergence of new states and empires, new rules of governance, anti-violent theories and views, a set of laws aimed at saving civilians from the pain and suffering of war.

Thus, in the history of mankind, warfare has both a negative image and positive consequences. The study of the paradoxical image and dynamics of military conflicts is extremely important in terms of studying the changing faces of wars.

Theoretical Background

The concept of “Four generations of war” was developed in the 1980s by authors such as historian William S. Lind and Lieutenant Colonel Thomas H. Hammes. According to these authors, the four generations of war began with the Peace Treaty of Westphalia (1648), which established the state’s monopoly on warfare. The qualitative evolution of warfare, described as “generations,” is largely due to technological factors, as well as political, social, and economic factors that shape society both domestically and internationally [1].

Although the concept of “generations of war” was introduced into science in 1989, it is still a subject of scholarly debate. Some researchers describe this process as the transformation of military conflicts, while others describe it as the “history of a revolution in military affairs”. In general, this is a broad issue. “The concept of generations of warfare reflects the evolution of humanity’s approach to conflict. From the mass armies of the first generation to the industrial weapons of the second generation, war has continuously adapted to technological and social changes. Today, war blurs the boundaries between traditional warfare, asymmetric strategies, cyber tactics, and information warfare. As conflicts become more complex, countries are forced to rethink traditional methods [2].

Problem Statement

The study of generations of war, the place of military violence in human society and the system of interstate relations, its formalization as a tool for ensuring national interests, its negative and positive function, the improvement of the rules and tools for conducting military operations, the reaction of the international community, and other issues have played an important role in the evolution of this concept. Today, this concept is still relevant and has a questionable fate. On the one hand, questions about the exact historical cycle of generations of military violence await their answers, and on the other hand, there are not a few who are not satisfied with the number of generations of warfare, but rather voice the possibility of its decline. In addition, within each generation, there are disagreements regarding the perpetrators, the structure of the warfare and the means of conducting it. It is also extremely controversial to determine the exact time boundaries between some generations.

Results

An analysis of the history of wars and military conflicts shows that in the pre-nuclear era, the alternation of war and peace was a natural and initial state on Earth. Wars have never stopped, but have continued to develop: from ancient times to the present day, at least five generations of wars and military conflicts have undergone changes. The main stages of such generational change mainly coincide with historically significant qualitative leaps in the development of human society, which led to the emergence of fundamentally new means of destruction and laid the foundation for the emergence of new forms and methods of waging war [3, pp. 75-80].

First Generation Wars (1st GW)

Since the Peace of Westphalia in 1648, the concept of war has moved from the mass use of manpower (1st GW), to the concentration of firepower (2nd GW), to maneuver warfare (3rd GW), to insurgency and terrorism (4th GW), and more recently to contactless and unrestricted warfare (5th GW).

History shows that 1st GW existed from the mid-17th century to the mid-19th century. 1st GW was characterized by positional warfare between large centralized forces (referring to the early stages of organized warfare with armed forces under state control) and went down in history under the terms “massive warfare” or “warfare of lines and columns” (the emphasis in these periods was on linear and column tactics). The forms and methods of waging this generation of wars were determined by the revolution in military affairs inherent in the transition from feudalism to capitalism. The initial stage of this revolution is considered to be the emergence of gunpowder and smooth-bore weapons and cannons. At this stage, new methods of armed struggle on a tactical scale of divisions, units and formations appeared, and linear tactics were used [3, pp. 75-80].

Battles were usually fought on a single battlefield, which limited the mobility of forces and resources. Wars attributed to this period include the Anglo-Spanish War, the Seven Years’ War, the US War of Independence, the Napoleonic Wars, etc. The First War Generation reached its peak in 1914-1918, during the First World War.

The main features of this class of warfare are:

Historically, first-generation wars have acted as a way to resolve conflicts and have political (crown conflicts, territorial claims, and dynastic change, etc.) content.

These wars were fought at the tactical level by organized armed forces of states. Armed battles were conducted exclusively by manpower – infantry and cavalry equipped with cold weapons, and numerous forces were deployed in battle lines and columns;

In the final stages of the 1st generation of warfare, weapons of war – swords and shields, bows and arrows, spears and bayonets – were replaced by rifles, hand grenades, machine guns, cannons, and artillery.

Among the generations of warfare, the 1st GW has the longest history. During this period, the means of warfare and combat tactics did not undergo rapid transformation, but rather continued to develop very slowly. The war did not go beyond a specific and limited geographical space and was not prone to expansion. First-generation warfare can be described as “ancient and post-classical wars with a tendency to inertia.” However, this generation of warfare was characterized by a number of innovations in terms of theoretical and practical activities.

Cardinal changes began to manifest themselves only towards the end of this generation of warfare. In particular, the idea of national state sovereignty, put forward after the Peace of Westphalia (1648), paved the way for the transfer of the army to state control, military culture began to develop, military training began to improve, a conscription system was created, and the pace of warfare increased. In the Napoleonic Wars, for the first time, control over the dissemination of information was applied, and the tactic of economic warfare – counterfeit banknotes were issued in order to weaken the enemy’s economy [4].

This generation of warfare is also remembered for its positive impact on the improvement and development of a number of progressive documents (Vigayet (1280), the Vienna Convention (1864) and the Liber Code (1863), etc.), which existed to improve preventive measures – to improve the rules of battle, to prevent the sick, wounded, children and women from becoming victims of war.

Second Generation of Warfare (2nd GW)

The period from the mid-19th century to the early 20th century (1840s to 1918) can be attributed to the second generation of warfare. During this period, warfare tactics changed dramatically with the advent of mass production, railroads, and the telegraph. This period is notable for the use of mass-produced weapons and their improvements. Machine guns and rapid-fire artillery are just a few examples of technological advances in this war, which contributed to the development of trench warfare, combat techniques, and strategies of attrition. This period can be broadly described as the era of industrial warfare, as for the first time it became easier than ever to attack a foreign country and inflict mass destruction.

Generally, 2nd GW is defined by the terms “trench warfare” or “linear fire and movement warfare” and benefited from the successes of the industrial age. New technological advances have increased the individual maneuverability of small groups, reduced the concentration of casualties, and developed cover and camouflage to gain an advantage.

This generation of warfare has responded to technological advances by developing “position warfare”, artillery support, more sophisticated reconnaissance methods, the widespread use of camouflage uniforms, radio communications, and fire team maneuvers.

World War I (1914–1918) was a war between coalitions of European states, which used a wide range of weapons and equipment, mainly artillery and machine guns, to destroy enemy forces and seize territory, establishing the dominance of more powerful states. The presence of armored fleets in technologically advanced states was an important tool in their struggle for world domination.

2nd GW can also be characterized as the emergence of “Blitzkrieg”. Within the framework of blitzkrieg tactics, the evolution and improvement of 2nd GW can be seen in its emphasis on speed, maneuverability, and the integration of air power on the battlefield. Although related to blitzkrieg, 2nd GW refers to a broader historical period characterized by the development of industrial warfare, including trench warfare, artillery support, and the use of reconnaissance and radio communications. The Civil War in the United States, the Crimean War, and World War I are included in this division.

2nd GW developed until World War II. The main characteristics of this type of warfare were: fighting continued by organized armed forces of nation states;

warfare increasingly relied on firepower and maneuver, coordinated movements from closed firing positions to ensure progress on the front, and cavalry maneuvers;

armored vehicles and aviation developed, which determined rapid movements in the theater of military operations and required mobile warfare;

industrial warfare paved the way for the formation and further development of the “Blitzkrieg” tactic and brought the end of linear strategies closer.

Third Generation of Warfare (3rd GW)

3rd GW is known as “maneuver warfare”, a continuation of the “Blitzkrieg” philosophy of World War II. This generation of warfare continued until the Korean and Vietnam wars.

3rd GW relied on the use of speed and surprise to overwhelm enemy positions and defeat their forces in the rear (rear line). It was essentially the end of linear warfare at the tactical level. In this, units sought to outmaneuver each other to gain maximum advantage rather than simply confronting each other.

The well-known characteristics of this theoretical class of warfare are maneuver warfare (aimed at destroying enemy manpower, military resources, and fighting spirit), adaptation to changing battlefield conditions, joint operations, and the use of indirect firepower.

This generation of warfare emphasizes the transition to mechanized warfare and the integration of air forces. This refers to rapid, joint operations and the concept of “Blitzkrieg”. These tactics were best exemplified by the “blitzkrieg” tactics of Nazi Germany in World War II. The main goal of this tactic was to neutralize the enemy with relatively small attacks before launching a decisive offensive.

Tanks, aircraft and highly mobile infantry allowed them to advance rapidly and encircle the enemy. As a result, the enemy suffered serious losses of resources, which undermined his will to continue the fight. One of the main advantages of this generation of tactics was the blurring of the front line.

3rd GW is a concept in military theory that, rather than traditional tactics of attrition, uses maneuver warfare, speed and surprise to outmaneuver and change the enemy’s direction. It involves moving from linear frontline battles to more complex, non-linear operations, using

technology and new strategies to control and defeat enemy forces from the rear. Maneuver warfare, speed and surprise, non-linear operations, technological advances, and decentralized command are considered to be the hallmarks of this generation of warfare. In principle, Third Generation warfare represents a shift from static, outdated warfare to a more dynamic, maneuverable approach that uses technology and speed to achieve decisive results.

With the end of linear warfare, new methods of moving more quickly began to emerge, the development of helicopters allowed landings in enemy territory, and advanced missile technology allowed troops to bypass enemy defenses and strike targets from greater distances. The speed inherent in these methods required greater independence for units on the front line. Small units were given greater freedom and flexibility to make decisions in response to changing conditions on the ground, while also carrying out decisions made by commanders far from the front. This began to erode the culture of military command and discipline (subordination).

The main characteristics of this generation of warfare can be summarized as follows:

Fighting is carried out by organized armed forces of nation states;

Maneuverability at sea, on land, and in the air is further improved through mechanization and new technological capabilities: at sea – ships; on land – tanks, trucks, jeeps, etc.; in the air – airplanes, helicopters, jets, etc.;

Military doctrine develops in the direction of new tactics such as attacking the enemy from the rear and bypassing the front line.

Fourth Generation of Warfare (4th GW)

4th GW is defined by the terms “insurgency warfare”, “asymmetric warfare” or even “unconventional warfare”, are attributed to the era of information and high technology, are characterized by the disappearance of the distinction between war and politics, between combatants and civilians. They are presented as a return to a decentralized form of warfare. This type of generation marks the loss of the monopoly of nation-states over the Armed Forces, a return to the conflict regimes common in pre-modern times, and is becoming a war in which violent non-state actors (non-state actors such as terrorist groups, insurgents and transnational networks) are among the main participants. Classic examples of conflicts belonging to this generation are, for example, the slave revolt during the Spartacus era, and modern examples are the activities of ISIS and Al-Qaeda.

4th GW is characterized by the following elements: the nature of warfare as complex and long-term, highly decentralized, low-intensity, and non-hierarchical conflicts; the direct attack on the enemy's culture, including the commission of acts of genocide against civilians; the use of all available means of coercion – political, economic, social, and military; the use of insurgency tactics as subversion, terror, and guerrilla tactics; and so on. In 4th GW, the battlefield may be fragmented and there are no defined front lines; conflicts often occur in urban environments and in everyday life. Al-Qaeda is often cited as a prominent example of 4th GW practitioners who use advanced technology and media to spread their ideology and influence. This model of warfare reflects a shift toward protracted warfare in which success is measured not by military victories but by the ability to undermine the opponent's resolve and legitimacy [5].

The most important characteristics of this type of warfare are:

the decline in the participation of nation-states and the emergence of non-state actors for the first time, indicating that one of the warring parties does not include the organized armed forces of the state;

the use of asymmetric tactics, methods and procedures to reduce the advantage and power of the enemy so that he cannot win using traditional methods (increased low-intensity conflicts, the use of insurgency and terror tactics);

the use of cyberattacks to disrupt critical infrastructure, spread disinformation and undermine public trust;

influencing decision-makers to change their political positions in their favor and undermine the fighting spirit and morale of enemy troops. Experts believe that individual concepts of the 4th GW can be found in the 1930s, during the Chinese Civil War. The essence of Mao Zedong's strategy was to avoid military operations when the balance of forces was unfavorable and to choose forms of military operations that would lead to the defeat of enemy forces. According to some experts, 4th GW is the only type of war in which a major power has been defeated: the United States in the Vietnam War and the USSR in the Afghan campaign.

These wars challenge classical concepts, demonstrate the increasing role of information and influence, and indicate the need for a multifaceted approach to conflict resolution.

At the same time, 4th GW is developing in the context of the "technology-ideology conflict". Thus, non-Western countries, such as Islamic and Asian countries, are playing the idea card against technology, which is a powerful weapon of the West, and are reflected in terrorism. Therefore, this type of warfare is considered a large and unlimited front opened against non-Western countries, in addition to being a product of non-Western countries [5]. ISIS's plan to create a Caliphate is the most successful example that meets this classification.

Scholarly debates around 4th GW continue. In his article "Fourth Generation Warfare and Other Myths," Antulio J. Echevarria II, a writer at the Strategic Studies Institute and professor at the U.S. Army War College, criticized the "generational model" as an ineffective way to describe changes in warfare and dismissed the violence of that generation as mere insurgencies [6].

Lieutenant General Kenneth F. McKenzie of the U.S. Marine Corps has stated that the methods of fourth generation warfare are unclear, its facts controversial, and its relevance questionable [7].

Fifth Generation of Warfare (5th GW)

This type of warfare conducted primarily through non-kinetic warfare, such as social engineering, disinformation, cyberattacks, artificial intelligence, and emerging technologies with fully autonomous systems. This generation of warfare has been described by Daniel Abbott as "information and perception" warfare [8], but has been criticized by William S. Linde, the author of the "4 Generations of Warfare" concept.

5th GW is characterized by the use of a "ubiquitous battlefield" or a mix of kinetic and non-kinetic forces rather than absolute military power. The book "Unrestricted Warfare" by People's Liberation Army Colonels Qiao Liang and Wang Xiangsui notes that while conventional military violence has declined in the years following the 1991 Gulf War, there has been a notable increase in "political, economic, and technological violence" that is no less destructive [9].

5th GW is a type of warfare unlike anything experienced before. In past wars, armies fought on identifiable battlefields. They fought in trenches, jungles, or in the skies with guns, tanks, and bombs. 5th GW, on the other hand, is a war of cyberattacks, disinformation campaigns, and economic manipulations to destabilize societies. It seems that this war is not only being waged on the battlefield, but also in the digital world, in financial systems, and even in people's minds. It was not a war to conquer territory, but to break trust, destabilize, and create chaos [10].

Such type of warfare has serious global implications. First and foremost, it challenges the very concept of national sovereignty. 5th GW is a scenario in which a hacker from one country can damage infrastructure in another without crossing borders. A fully-organized fake news campaign could undermine a democracy halfway around the world.

This type of warfare refers to terms such as "unrestricted warfare", "complex warfare", or "unlawful warfare".

Unrestricted warfare is a type of warfare in which one side uses all available means to compel an enemy to act in its own best interests.

Complex warfare is the simultaneous use of regular or main forces and irregular or guerrilla forces against the enemy. In other words, military effectiveness is enhanced by the simultaneous use of both conventional and unconventional forces.

Unlawful warfare is a relentless struggle between state and non-state actors for legitimacy and influence over the relevant population. This type of warfare favors indirect and asymmetric approaches, although it may use all military and other capabilities to undermine the power, influence, and will of the enemy. It presupposes the emergence of powerful individuals or groups with access to advanced knowledge, technology, and resources to wage such modern warfare. These actors prefer asymmetric and hybrid actions to advance their interests.

According to experts, the most important characteristics of 5th generation warfare are as follows:

It is a war against non-state actors, where there is no massed force or clear “center of gravity” to strike.

It represents a continuation of asymmetric and insurgent warfare, in which the adversary employs both conventional and unconventional means.

It is driven by political, religious, and social motives.

It involves spontaneous and anonymous terrorist attacks against random targets (both civilians and military personnel) with the aim of generating confusion and fear.

It includes non-lethal actions in the form of global strategic information operations (conducted via the Internet and continuous news broadcasts).

It can be conducted by either organized or unorganized groups.

It may be directed by a nation-state or a non-state entity seeking to undermine or neutralize the adversary’s advantages in order to advance its own interests.

This concept is not yet fully developed, but it is clearly a product of new technologies and the current stage of a revolution in military affairs.

Table – Generations of Warfare

Generation	Period	Key Determinants	Actors	Strategy, Tactics and Technology
1 GW	1648-mid 19th century	Classical, post-classical warfare (conventional)	State Army	Flank, column, straight line, Linear strategy
2 GW	mid 19th century – early 20th century	Trench warfare (conventional)	State Army	Revolution in military affairs and industrial warfare, Development of blitzkrieg, Positional warfare, Linear strategy
3 GW	mid 20th century – end of Cold war	Maneuver warfare (conventional)	State Army	Failure of linear strategy, Blitzkrieg
4 GW	Late 20th century – early 21st century	Insurgent warfare (non-conventional)	Non-state actor	Terror and insurgency tactics, guerrilla, psychological and low-intensity warfare
5 GW	Late 20th century – early 21st century	Unrestricted warfare (non-conventional)	State and non-state actors	Hybrid, asymmetric, network-centric warfare

Controversial points.

Although the concept of “generations of warfare” was first introduced in 1989, it is reasonable to assume that intense debates surrounding it will persist. These scholarly discussions can be justified by several factors:

1. It is quite difficult to determine the specific historical framework for the beginning and end of each war generation. There are contradictory views in this direction. For example, the question of how long the 1st generation of warfare lasted remains controversial. Some note that this date lasted until the middle of the 19th century, while others note that it lasted until 1914-1918.

Although the concept of “Generations of warfare” in the West is associated with the concept of sovereignty, religious, territorial, power and dynastic wars took place before that, and various military strategies were implemented. In this case, it is not true to say that the concept of war generations has developed since the mid-17th century and creates a basis for the theoretical and practical activities related to armed violence that occurred in the centuries before that to be left out of the study.

In fact, if we take into account the similarity between the tactics used until the first generation of wars, the types of weapons, and the goals of the wars, the beginning of that generation of wars can be extended to the slavery period, or the first generation of wars can be classified into early, classical, and postclassical divisions. Early wars include wars between tribes and tribes, classical wars include wars between religious, territorial, dynastic, and knightly orders covering the slavery and feudalism periods, and postclassical wars include conflicts that arose after Westphalia and emerged between sovereign states.

2. There is polarization in views on the concept of generations of warfare. Currently, the Western-centered perspective is hegemonic in this direction and does not include non-Western countries. For example, while in Western scientific circles 5 generations of warfare are indicated, Russian scientists note 6 generations of military violence. In their periodization, generations of warfare is analyzed from ancient times – from the tribal, clan and family-patriarchal stage of human society, to the fifth generation of “hybrid warfare”.

3. While technology is indicated as the main determinant in the concept of generations of warfare, social, political and cultural factors are not given much serious attention. This division emphasizes the Western ideological approach more. It is as if generations of warfare are explained from the point of view of Westernization. But should conflicts that occurred in the non-Western, especially in the Islamic world, be excluded from the study?

4. The presentation of 5th generation of warfare as a separate category still raises questions. Academic research in this direction is weak.

5. Since some wars combine elements of several “generations”, this leads to inaccuracy in the generational division. As an example, we can cite the similarities between the 4th and 5th generations: the persistence of non-state actors and the tactics they implement (asymmetric), the use of cyberattacks to disrupt the functioning of critical infrastructures, and even the use of all means of pressure (kinetic and non-kinetic capabilities) as a means of struggle, the “delegation” of the use of military force to non-state actors (conducting military operations through proxies), etc.

Conclusion

1. The concept of “Generations of warfare” determined the dynamics of military-theoretical and military-practical transformations that marked a huge period in human history, from the classical form of military violence to the hybrid form. Each generation of warfare had its positive impact on the historical development of military conflictology in general.

2. The concept of “Generations of warfare”, considered the result of the continuous development of the “revolution in military affairs”, had a serious impact on the improvement of combat equipment, the emergence of new tactics and the transformation of military skill.

3. 3rd GW has led to fundamental changes in the military culture and society’s view of war, the culture of war has become more organized, the number of war victims has increased and the conditions of war have become more difficult, and anti-war sentiments have been strengthened in societies and internationally (humanization of military operations – Hague Convention 1899-1907).

4. Modern wars have become uncontrolled, autonomous, decentralized military-political processes, the Hague system (jus ad bellum) has been enriched and improved by new means and methods of armed struggle, and the Geneva system (jus in bello) has undergone a radical transformation due to new actors.

5. 4th GW is characterized as a “stateless/decentralized war” for the first time in human history. Its main participants are considered to be violent non-state actors who challenge national state institutions. These actors have put an end to the hegemony of the “Clausewitz’s legacy” that lasted for more than a century.

This type of warfare has further complicated legal and ethical issues. The laws of war and international law have become more difficult to apply outside traditional battlefields and in conflicts with non-state actors. This has also resulted in the disappearance of the distinction between combatants and civilians. Battlefields are now not only physical, but also virtual, and cyberattacks and information protection have played an important role. These types of warfares often took the form of internal conflicts, but later gave rise to the intervention of international coalitions.

6. 5th GW can be described as a continuation of the previous generation of wars in a more sophisticated form, or even as a “state takeover and development” of the tactics of war used by non-state actors. The absence of obvious actors in this type of warfare, the shift of direct military force to non-kinetic capabilities, are considered the main distinguishing determinants, and it has become the ideal blend of conventional and unconventional conflicts. This type of violence, which gives the impression of a “masked” and “borderless” generation of warfare, ensures victory over the enemy by capturing not the opponent’s territory, but public opinion, cyberspace and social media.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

1. Maria do Céu Pinto Arena. The evolution of conflict: Fourth-generation warfare. Available from : <https://fibrenamics.com/index.php/en/news/the-evolution-of-conflict-fourth-generation-warfare>
2. Fiza Bibi Ameen. Five Generations of Warfare: The Evolution of Military Landscape. Available from : <https://www.paradigmshift.com.pk/warfare-generations/>.
3. Makarenko, S. I., Ivanov, M. S. Network-centric warfare – principles, technologies, examples and prospects. Monograph. – St. Petersburg: Science-intensive technologies, 2018. – 898 p.
4. Andrew Marshall. What are the generations of war / Boot camp and military fitness institute, 14.07.22. Available from : <https://bootcampmilitaryfitnessinstitute.com/2022/07/14/what-are-the-generations-of-warfare/>
5. Fourth-generation warfare (4 GW). Available from : <https://www.ebsco.com/research-starters/history/fourth-generation-warfare-4gw>).
6. Echevarria, J. A. Fourth Generation War and Other Myths Archived 2018-04-22 at the Wayback Machine, Strategic Studies Institute, November 2005.
7. Global Insurgency and the Future of Armed Conflict: Debating Fourth-generation Warfare, edited by Terry Terriff, Aaron Karp and Regina Karp. New York: Routledge, 2008, p. 68.
8. Abbott, Daniel (2010). The Handbook of Fifth-Generation Warfare. Nimble Books. p. 20.
9. Michael, George (2012). Lone Wolf Terror and the Rise of Leaderless Resistance. Vanderbilt University Press. p. 157.

10. Hafsa Nawaz. 5th Generation War: A War Without Borders and its Impact on Global Security / Modern diplomacy. November 25, 2024. Available from : <https://moderndiplomacy.eu/2024/11/25/5th-generation-war-a-war-without-borders-and-its-impact-on-global-security>

Список використаних джерел

1. Maria do Céu Pinto Arena. The evolution of conflict: Fourth-generation warfare. Available from : <https://fibrenamics.com/index.php/en/news/the-evolution-of-conflict-fourth-generation-warfare>
2. Fiza Bibi Ameen. Five Generations of Warfare: The Evolution of Military Landscape. Available from : <https://www.paradigmshift.com.pk/warfare-generations/>.
3. Makarenko, S. I., Ivanov, M. S. Network-centric warfare – principles, technologies, examples and prospects. Monograph. – St. Petersburg: Science-intensive technologies, 2018. – 898 p.
4. Andrew Marshall. What are the generations of war / Boot camp and military fitness institute, 14.07.22. Available from : <https://bootcampmilitaryfitnessinstitute.com/2022/07/14/what-are-the-generations-of-warfare/>
5. Fourth-generation warfare (4 GW). Available from : <https://www.ebsco.com/research-starters/history/fourth-generation-warfare-4gw>).
6. Echevarria, J. A. Fourth Generation War and Other Myths Archived 2018-04-22 at the Wayback Machine, Strategic Studies Institute, November 2005.
7. Global Insurgency and the Future of Armed Conflict: Debating Fourth-generation Warfare, edited by Terry Terriff, Aaron Karp and Regina Karp. New York: Routledge, 2008, p. 68.
8. Abbott, Daniel (2010). The Handbook of Fifth-Generation Warfare. Nimble Books. p. 20.
9. Michael, George (2012). Lone Wolf Terror and the Rise of Leaderless Resistance. Vanderbilt University Press. p. 157.
10. Hafsa Nawaz. 5th Generation War: A War Without Borders and its Impact on Global Security / Modern diplomacy. November 25, 2024. Available from : <https://moderndiplomacy.eu/2024/11/25/5th-generation-war-a-war-without-borders-and-its-impact-on-global-security>

New Approaches in Military Personnel Training: a Pedagogical Evaluation of Teaching Methods

Нові підходи до підготовки військових кадрів: педагогічна оцінка методів навчання

Mujkan Mammadzada

PhD in Pedagogy, e-mail: mujkanmemmedzade@gmail.com, ORCID: 0000-0001-5693-3748

Military Scientific Research Institute of the National Defense University, Baku, Azerbaijan

Муджкан Маммадзада

доктор у галузі педагогіки, e-mail: mujkanmemmedzade@gmail.com, ORCID: 0000-0001-5693-3748

Військовий науково-дослідний інститут Національного університету оборони, Баку, Азербайджан

Received: July 30, 2025 | Revised: August 11, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.7>

Purpose. The purpose is to scientifically analyze and evaluate the pedagogical effectiveness of new teaching methods applied in modern military personnel training.

Method. A comparison has been made between various pedagogical approaches, international military education practices, and the methods applied within the Azerbaijani military education system, and their effectiveness has been evaluated from both theoretical and practical perspectives.

Theoretical implications. The research revealed that the integration of modern teaching methods into military education significantly contributes to enhancing pedagogical quality in officer training. Problem-based learning, simulation, and interactive methods strengthen cadets' analytical thinking, decision-making, and leadership skills. The systematic and continuous application of these approaches can ensure the development of the Azerbaijani military education system in alignment with international standards.

Practical implications. The implementation of problem-based learning models in military education institutions enables cadets to prepare for real combat scenarios. The use of simulation and technological training tools facilitates the practical development of decision-making, coordination, and operational planning skills. Organizing professional development programs for instructors on interactive teaching methods enhances the overall effectiveness of instruction. Integrating subjects that develop leadership and socio-emotional competencies into curricula strengthens cadets' ability to work in teams and improves their psychological resilience. Reinforcing a student-centered approach within the teaching process increases cadet motivation and active engagement in learning.

Value. This article provides a scientific justification for the application of pedagogical innovations in the modern military education system and analyzes the practical impact of new teaching methods, identifying realistic and purposeful directions for aligning the development of Azerbaijan's military education with international best practices.

Paper type. Empirical.

Мета дослідження. Проаналізувати та оцінити педагогічну ефективність нових методів навчання, що застосовуються в сучасній підготовці військовослужбовців.

Метод дослідження: Зроблено порівняння між різними педагогічними підходами, міжнародними практиками військової освіти та методами, що застосовуються в азербайджанській системі військової освіти, та оцінено їх ефективність з теоретичної та практичної точок зору.

Теоретична цінність дослідження. Дослідження показало, що інтеграція сучасних методів навчання у військову освіту значно сприяє підвищенню педагогічної якості підготовки офіцерів. Проблемно-орієнтоване навчання, моделювання та інтерактивні методи зміцнюють аналітичне мислення, навички прийняття рішень та лідерські якості курсантів. Систематичне та безперервне застосування цих підходів може забезпечити розвиток азербайджанської системи військової освіти у відповідності до міжнародних стандартів.

Практична цінність дослідження. Впровадження моделей проблемно-орієнтованого навчання у військових навчальних закладах дозволяє курсантам готуватися до реальних бойових сценаріїв. Використання моделювання та технологічних навчальних інструментів сприяє практичному розвитку навичок прийняття рішень, координації та оперативного планування. Організація програм підвищення кваліфікації для викладачів з інтерактивних методів навчання підвищує загальну ефективність навчання. Інтеграція предметів, що розвивають лідерські та соціально-емоційні компетенції, в навчальні програми зміцнює здатність курсантів працювати в командах та покращує їх психологічну стійкість. Посилення орієнтованого на студента підходу в навчальному процесі підвищує мотивацію курсантів та активну залученість до навчання.

Цінність дослідження. Ця стаття надає наукове обґрунтування застосування педагогічних інновацій у сучасній системі військової освіти та аналізує практичний вплив нових методів навчання, визначаючи реалістичні та цілеспрямовані напрями узгодження розвитку військової освіти Азербайджану з міжнародними найкращими практиками.

Тип статті. Емпірична.

Key words: military education, pedagogical approaches, problem-based learning, simulation, interactive methods.

Ключові слова: військова освіта, педагогічні підходи, проблемно-орієнтоване навчання, моделювання, інтерактивні методи.

Introduction

The changing geopolitical realities and technological advancements of the 21st century have introduced new demands for modern military education. Contemporary warfare is no longer confined to physical battlefields; it now spans information, psychological, and technological domains. Under such conditions, the training of military personnel must go beyond technical and

tactical knowledge and focus on developing analytical thinking, agile decision-making, leadership, and communication skills. This necessitates a fundamental transformation of the instructional process from both pedagogical and methodological perspectives, requiring the integration of new training technologies and modern learning models into military education.

In Azerbaijan, as part of ongoing military reform initiatives, the modernization of military education in terms of both content and structure has become a key national priority. Officers must be equipped not only with technical competence but also with moral, intellectual, and social preparedness, which is of strategic importance for national security. Therefore, the selection of teaching methods based on scientific evidence and their pedagogical evaluation is a highly relevant issue in military personnel training.

The aim of this article is to analyze the new pedagogical approaches and instructional methods used in military education and to assess their impact on the professional, psychological, and leadership development of cadets. Drawing on international experience, practical case studies, and relevant pedagogical theories, the study systematically investigates the effectiveness of problem-based learning, simulation, social-emotional learning, and interactive teaching methods.

The significance of this research also stems from the limited number of scientific studies in this field within Azerbaijan and the lack of systematic analysis regarding the practical implementation of pedagogical approaches. The findings and recommendations presented in this article may serve as a practical foundation for improving the quality of instruction within the military education system and for the effective application of new teaching methodologies in officer training.

Theoretical background

Pedagogical approaches applied in the modern military education system are based on constructivist, interactive, and practice-oriented learning models. Traditional lecture-based instruction is gradually being replaced by problem-based learning, simulation, and group-centered activities. These approaches foster the development of analytical thinking, agile decision-making, and leadership skills among cadets. From a pedagogical perspective, the primary objective is to train military personnel not only as knowledgeable individuals but also as professionals equipped with practical competencies and a high level of moral and motivational readiness.

Problem Statement

In the modern era, the dynamic and complex nature of military operations demonstrates that traditional instructional formats alone are no longer sufficient for officer training. The global security environment, rapid technological advancement, and the proliferation of hybrid warfare forms necessitate the adoption of flexible, practice-oriented, and interactive teaching methods in military education. However, in many cases, outdated lecture-based approaches still dominate the instructional process, which limits cadets' ability to adapt to real combat conditions and make effective decisions. Moreover, the lack of systematic pedagogical evaluation of the implementation of new teaching methods creates challenges in measuring their effectiveness and ensuring sustainable development in this area. Therefore, the scientific and pedagogical analysis of modern instructional methods applied in military training, as well as the assessment of their practical impact, constitutes a timely and significant research problem.

Results

Problem-Based Learning (PBL) and the Military Environment

Problem-Based Learning is one of the core active learning methods in modern pedagogy and has increasingly been adopted in military education in recent years. The central principle of this approach is that cadets confront real or simulated problems and acquire knowledge through self-

directed learning and collaborative problem-solving within group settings. In the military context, this approach fosters not only theoretical knowledge but also the development of situational decision-making, analytical thinking, and leadership skills.

During the implementation of the PBL method, cadets work through scenarios that closely resemble real combat situations. They analyze the core aspects of a given problem using various sources of information and seek strategic solutions. This process supports the formation of critical thinking and operational decision-making skills, while also promoting essential qualities such as teamwork, responsibility, and adaptability to changing environments [1, pp. 235].

The application of PBL in military education is especially widespread in NATO countries' military academies. Research shows that cadets trained through PBL demonstrate higher levels of motivation, retain learned material for longer periods, and respond more flexibly in practical situations [2, pp. 732-741]. The NATO Defence Education Enhancement Programme (DEEP) has also recommended the integration of PBL as a key innovation in modern officer education [3].

Overall, the PBL approach facilitates a shift from passive learning models to active, application-oriented learning within military education. This approach is particularly valuable in preparing officers who are capable of demonstrating leadership, rapid adaptation, and analytical reasoning in situations of conflict and crisis.

Simulation Technologies and Leadership Training in Military Education

The application of simulation technologies in modern military education significantly enhances the practicality and effectiveness of the instructional process. Simulation-based training enables cadets to develop decision-making and operational planning skills in environments that closely resemble real combat situations, yet remain safe and controlled. Through command staff simulations, virtual wargaming, and tactical simulators, cadets engage in strategic decision-making, resource allocation, and scenario analysis [4].

Simulations are particularly valuable for developing military leadership skills. Leadership in military contexts goes beyond issuing orders—it involves situational analysis, motivating subordinates, and assessing risks. Simulation environments allow cadets to practice and refine these competencies in realistic conditions. Research indicates that cadets participating in simulation-based training demonstrate higher levels of strategic thinking, psychological resilience, and decision-making under stress [5, pp. 197].

In addition, leadership training and elements of social-emotional learning (SEL) are increasingly integrated into modern military education programs. Developing soft skills such as self-regulation, empathy, effective communication within teams, and conflict resolution is as vital as technical proficiency on the battlefield. Daniel Goleman's theory of social intelligence provides a foundational theoretical framework in this area, emphasizing the direct relationship between emotional intelligence and effective leadership [6].

Therefore, leadership training complemented by simulation technologies equips officers not only with technical expertise but also with the psychological, decision-making, and interpersonal skills required for complex military operations. This holistic approach is now considered a core requirement of modern military models.

Interactive Teaching Methods and Pedagogical Effectiveness in Military Training

In modern pedagogy, interactive teaching methods emphasize the active involvement of learners in the educational process. This approach is particularly relevant and necessary in military education, where officer training requires not only the acquisition of knowledge but also its practical application, discussion, and analysis. Traditional lecture-based and passive listening methods no longer meet the demands of dynamic and complex military operations. Instead, methods such as simulation, debate, role play, case studies, group tasks, and game-based learning have demonstrated greater pedagogical effectiveness [7].

Interactive methods enhance cadets' critical thinking, analytical reasoning, collaboration, communication, and problem-solving skills. In particular, group-based tasks play a vital role in fostering values essential to the military context, such as team spirit, mutual trust, and collective responsibility. Role-playing and tactical simulation activities allow officers to experiment with different behavioral models in various scenarios, evaluate alternative decision paths, and learn from their mistakes [8].

Studies have shown that interactive learning environments significantly increase student engagement and positively influence learning outcomes. For instance, research by Prince (2004) demonstrated that students in active learning settings achieved higher retention and understanding compared to those in traditional classrooms. Similar outcomes have been observed in pilot studies conducted within military education institutions [3].

There is a growing tendency to implement interactive methods in Azerbaijan's military education system. In recent years, pedagogical training sessions and curriculum reforms have included workshops on the application of these methods for teaching staff. Standard instructional models now include "decision-making under pressure" simulations, group-based tactical planning exercises, and open discussion sessions, especially in institutions like the Military Academy and the Higher Military School [9].

However, the successful application of interactive methods requires several foundational conditions: adequate pedagogical training for instructors, availability of teaching resources, alignment of cadets with the methodology, and properly structured assessment mechanisms. If these components are systematically ensured, the pedagogical effectiveness of interactive methods in military education can be significantly enhanced, contributing to the development of not only professional competence but also social and emotional skills among cadets.

Implementation Experience and Challenges in Azerbaijan

In recent years, the modernization of Azerbaijan's military education system has become one of the key components of broader reforms in defense sector development. Following the 44-day Patriotic War, improving the quality of military personnel training and integrating modern instructional methods were identified as national priorities. Within this framework, the Ministry of Defense of the Republic of Azerbaijan and other relevant institutions have initiated curriculum reforms, pedagogical training programs, and the implementation of simulation-based learning models in higher military institutions [9].

One of the modern instructional methods introduced in Azerbaijan is PBL and interactive training sessions. At the Azerbaijan Higher Military School and Military Academy, cadets participate in sessions based on real or simulated scenarios, where they develop skills such as decision-making, leadership, coordination, and operational analysis. Courses such as "tactical situation analysis", "team-based decision-making", "leadership tasks" and "behavior under dangerous conditions" have been introduced. Additionally, virtual battle simulators have been deployed, and some courses are being offered in distance or hybrid formats as part of pilot initiatives.

As part of instructor professional development, cooperation has been established with NATO's Defence Education Enhancement Programme (DEEP), providing Azerbaijani military educators with training in modern teaching methodology and instructional technologies [3]. These programs have played a critical role in aligning Azerbaijan's military education institutions with international standards and promoting methodological modernization.

However, several challenges persist in the large-scale implementation of modern teaching methods in Azerbaijan:

1. Lack of methodological readiness: Many instructors and officers are accustomed to traditional lecture-based systems, which hinders the transition to interactive and problem-based approaches. Continuous pedagogical training and methodological workshops are necessary for effective implementation [10].

2. Limited teaching resources: In some higher military schools, the absence of simulation technologies and instructional equipment restricts the broad application of these methods. Strengthening technological infrastructure and developing virtual training laboratories are essential steps in this area.

3. Weak assessment mechanisms: Appropriate evaluation tools and performance indicators for assessing learning outcomes in line with new instructional methods have yet to be fully developed. Traditional testing and oral examinations do not adequately reflect the effectiveness of innovative teaching practices.

4. Lack of pedagogical research: There is a notable shortage of systematic studies and empirical research on the outcomes of instructional methods used in military education in Azerbaijan. This hampers the objective evaluation and improvement of new approaches.

Despite these challenges, ongoing educational reforms and internationally supported initiatives provide a foundation for the development of a more flexible, modern, and pedagogically sound military education system in the near future. The expanded application of interactive methods that enhance cadets' practical skills and strategic thinking abilities may mark a qualitative shift in officer training in Azerbaijan.

Recommendations and Development Perspectives

While the steps taken toward the modernization of military education in Azerbaijan have yielded significant results, achieving greater effectiveness and alignment with international standards requires a comprehensive and integrated approach. Based on existing practices and challenges, the following recommendations and development directions may be considered:

1. Systematic professional development for pedagogical staff: The effective implementation of modern instructional methods depends on the pedagogical and methodological readiness of teaching personnel. Long-term training and certification programs should be organized in collaboration with international initiatives such as NATO DEEP, TIKa, and others. Teachers' methodological skills must be regularly updated to align with evolving educational standards [3].

2. Expansion of simulation and digital training technologies: To enhance the practical dimension of military training, military educational institutions should be equipped with advanced simulation platforms, virtual laboratories, and interactive classrooms. This infrastructure will also support remote learning opportunities and ensure operational flexibility in emergency situations [11].

3. Implementation of assessment and outcome-based learning models: In order to measure the effectiveness of new teaching methods, outcome-based learning (OBL) approaches should be applied. Rubrics, performance-based assessments, and practical tasks should be developed to evaluate not only knowledge but also skills and behavioral competencies of cadets [12].

4. Mutual integration of civilian and military pedagogy: Military higher education institutions should cooperate with pedagogical faculties of civilian universities to organize joint seminars, research initiatives, and experience-sharing programs. Such collaboration can facilitate the flexible and effective integration of educational innovations into military training.

5. Strengthening the scientific research base: Systematic studies should be conducted to analyze the pedagogical and psychological effects of military training methods. The scientific activity of military educators should be encouraged, and military research institutions and academies should evaluate pilot applications of new instructional methods and publish their findings in academic journals.

6. Productive international cooperation and regional knowledge exchange: Comparative studies should be carried out with military education models in countries such as Türkiye, Kazakhstan, and Ukraine, and best practices should be adapted and localized accordingly. In particular, collaboration with Türkiye's National Defence University can offer practical examples and valuable perspectives for implementation.

The overarching goal of these recommendations is to enhance the quality of instruction within Azerbaijan's military education system, ensure the systematic implementation of modern

teaching approaches, and prepare professional officers equipped with strong leadership capabilities. These reforms should be viewed not only as an element of higher education policy but also as an integral part of the country's national security strategy.

Conclusion

The conducted research has revealed that the application of modern pedagogical approaches in military officer training—particularly PBL, simulation technologies, interactive methods, and social-emotional learning strategies—plays a critical role in enhancing cadets' professional competence and fostering leadership and strategic thinking skills. Traditional lecture-based methods are no longer sufficiently effective in the context of contemporary warfare and security challenges, making the transition to practice-oriented and applied learning models a necessity.

The international experience analyzed in the study demonstrates that in NATO member states and other advanced military education systems, interactive and learner-centered teaching models have become standard, emphasizing realistic operational training for future officers. The adaptation of these models to Azerbaijan's context and their integration into the local military education environment constitutes an essential part of ongoing educational reforms.

According to the research findings, although there has been progress in implementing modern instructional methods in Azerbaijan, several challenges persist—including uneven levels of methodological preparedness, limited access to simulation technologies, a lack of pedagogical research, and underdeveloped assessment mechanisms. These factors continue to hinder the full and effective realization of innovative training processes.

Nevertheless, with systematic pedagogical advancement, expanded international collaboration, and increased utilization of digital resources, Azerbaijan's military education system has the potential to evolve into a flexible, high-tech, and leadership-oriented model of officer preparation. Such an approach will not only enhance the capabilities of the armed forces but also contribute significantly to strengthening national security and strategic management capacity.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

1. Hmelo-Silver, C. E. (2004). Problem-based learning: What and how do students learn? *Educational Psychology Review*, 16(3). <https://doi.org/10.1023/B:EDPR.0000034022.16470.f3>
2. Dolmans, D. H., De Grave, W., Wolfhagen, I. H., & Van der Vleuten, C. P. (2005). Problem-based learning: Future challenges for educational practice and research. *Medical Education*, 39(7). <https://doi.org/10.1111/j.1365-2929.2005.02205.x>
3. NATO DEEP. (2021). *Defence Education Enhancement Programme (DEEP): Annual Report*. Available from : https://www.nato.int/cps/en/natolive/topics_139182.htm
4. Alexander, A. L., Brunyé, T., Sidman, J., & Weil, S. A. (2005). From gaming to training: A review of studies on fidelity, immersion, presence, and buy-in and their effects on transfer in PC-based simulations and games. *DARWARS Training Impact Group*. Available from : <https://apps.dtic.mil/sti/pdfs/ADA457861.pdf>
5. Salas, E., Bowers, C. A., & Rhodenizer, L. (2009). It is not how much you have but how you use it: Toward a rational use of simulation to support aviation training. *The International Journal of Aviation Psychology*, 8(3). https://doi.org/10.1207/s15327108ijap0803_2

6. Goleman, D. (2006). *Social Intelligence: The New Science of Human Relationships*. Bantam Books. Available from : <https://danielgoleman.info/topics/social-intelligence/>
7. Prince, M. (2004). Does active learning work? A review of the research. *Journal of Engineering Education*, 93(3), 223–231. <https://doi.org/10.1002/j.2168-9830.2004.tb00809.x>
8. Bonwell, C. C., & Eison, J. A. (1991). *Active Learning: Creating Excitement in the Classroom*. ASHE-ERIC Higher Education Report No. 1. Available from : <https://files.eric.ed.gov/fulltext/ED336049.pdf>
9. Ministry of Defense of the Republic of Azerbaijan. (2022). *Official Reports on Educational Reforms*. Available from : <https://mod.gov.az>
10. UNESCO IBE. (2017). *Training Tools for Curriculum Development: A Resource Pack*. Available from : <https://www.ibe.unesco.org/en/resources/training-tools>
11. OECD. (2020). *The Impact of COVID-19 on Education: Insights from Education at a Glance 2020*. Available from : <https://www.oecd.org/education>
12. Biggs, J., & Tang, C. (2011). *Teaching for Quality Learning at University* (4th ed.). Open University Press. Available from : <https://www.mheducation.co.uk/teaching-for-quality-learning-at-university-9780335242757-emea-group>

Список використаних джерел

1. Hmelo-Silver, C. E. (2004). Problem-based learning: What and how do students learn? *Educational Psychology Review*, 16(3). <https://doi.org/10.1023/B:EDPR.0000034022.16470.f3>
2. Dolmans, D. H., De Grave, W., Wolfhagen, I. H., & Van der Vleuten, C. P. (2005). Problem-based learning: Future challenges for educational practice and research. *Medical Education*, 39(7). <https://doi.org/10.1111/j.1365-2929.2005.02205.x>
3. NATO DEEP. (2021). *Defence Education Enhancement Programme (DEEP): Annual Report*. Available from : https://www.nato.int/cps/en/natolive/topics_139182.htm
4. Alexander, A. L., Brunyé, T., Sidman, J., & Weil, S. A. (2005). From gaming to training: A review of studies on fidelity, immersion, presence, and buy-in and their effects on transfer in PC-based simulations and games. *DARWARS Training Impact Group*. Available from : <https://apps.dtic.mil/sti/pdfs/ADA457861.pdf>
5. Salas, E., Bowers, C. A., & Rhodenizer, L. (2009). It is not how much you have but how you use it: Toward a rational use of simulation to support aviation training. *The International Journal of Aviation Psychology*, 8(3). https://doi.org/10.1207/s15327108ijap0803_2
6. Goleman, D. (2006). *Social Intelligence: The New Science of Human Relationships*. Bantam Books. Available from : <https://danielgoleman.info/topics/social-intelligence/>
7. Prince, M. (2004). Does active learning work? A review of the research. *Journal of Engineering Education*, 93(3), 223–231. <https://doi.org/10.1002/j.2168-9830.2004.tb00809.x>
8. Bonwell, C. C., & Eison, J. A. (1991). *Active Learning: Creating Excitement in the Classroom*. ASHE-ERIC Higher Education Report No. 1. Available from : <https://files.eric.ed.gov/fulltext/ED336049.pdf>
9. Ministry of Defense of the Republic of Azerbaijan. (2022). *Official Reports on Educational Reforms*. Available from : <https://mod.gov.az>
10. UNESCO IBE. (2017). *Training Tools for Curriculum Development: A Resource Pack*. Available from : <https://www.ibe.unesco.org/en/resources/training-tools>
11. OECD. (2020). *The Impact of COVID-19 on Education: Insights from Education at a Glance 2020*. Available from : <https://www.oecd.org/education>
12. Biggs, J., & Tang, C. (2011). *Teaching for Quality Learning at University* (4th ed.). Open University Press. Available from : <https://www.mheducation.co.uk/teaching-for-quality-learning-at-university-9780335242757-emea-group>

Сторітелінг в оборонному секторі

Storytelling in the Defense Sector

Костянтин Ніжейко ^A

Corresponding author: доктор філософії з міжнародних економічних відносин, старший викладач, e-mail: k.nizheyko@knute.edu.ua, ORCID: 0000-0002-2925-1140

Kostyantyn Nizheiko ^A

Corresponding author: PhD in International Economic Relations, Senior Lecturer, e-mail: k.nizheyko@knute.edu.ua, ORCID: 0000-0002-2925-1140

Олександра Лендел ^A

здобувач ОС “Марістр”, e-mail: o.lendel_fmtp_4m_24_m_z@knute.edu.ua, ORCID: 0009-0005-9774-5272

Oleksandra Lendel ^A

Master's degree student, e-mail: o.lendel_fmtp_4m_24_m_z@knute.edu.ua, ORCID: 0009-0005-9774-5272

^A Державний торговельно-економічний університет, м. Київ, Україна

^A State University Of Trade And Economics, Kyiv, Ukraine

Received: July 30, 2025 | Revised: August 11, 2025 | Accepted: August 31, 2025

JEL Classification: D91, F52, E65, M33.

DOI: 10.33445/sds.2025.15.4.2

Мета роботи: Ідентифікація комунікативних та інформаційно-психологічних аспектів застосування сторітелінгу як інструменту впливу у військово-промисловій сфері та сфері національної безпеки.

Результати дослідження: Подано загальне визначення сторітелінгу, його функції та роль у формуванні емоційного зв'язку між аудиторією та комунікатором. Особливу увагу приділено аналізу оборонної діяльності в контексті сучасної інформаційної війни, де сторітелінг використовується як ефективний засіб психологічного впливу, мобілізації підтримки та формування позитивного іміджу військових структур. Окреслено актуальні тенденції застосування сторітелінгу у військових комунікаціях, зокрема в межах стратегічних комунікацій, інформаційних кампаній та операцій впливу. Досліджено типові тематики військових наративів: героїзм, жертвність, братерство, боротьба за незалежність, захист цінностей. Визначено особливості військового сторітелінгу, такі як емоційна насиченість, апеляція до національної ідентичності, візуально-звукова виразність і адаптація до різних платформ (соціальні мережі, відео, блоги, документальні формати тощо).

Оригінальність: Систематизовано сторітелінг як цілісний комунікаційний інструмент в оборонному секторі, що поєднує психологічний, маркетинговий та стратегічний виміри. Запропоновано структурований механізм використання сторітелінгу для впливу на публічну думку, державні рішення та позиціонування продукції ВПК у міжнародному середовищі. Обґрунтовані основні кроки для практичного впровадження сторітелінгу у стратегії українських компаній оборонного сектору.

Тип статті: концептуальний.

Purpose: To identify the communicative and informational-psychological aspects of storytelling as a tool of influence in the military-industrial sphere and national security.

Findings: A general definition of storytelling, its functions, and role in forming an emotional connection between the audience and the communicator are provided. Particular attention is paid to the analysis of defense activities in the context of modern information warfare, where storytelling is used as an effective means of psychological influence, mobilization of support, and formation of a positive image of military structures. Current trends in the use of storytelling in military communications, particularly in strategic communications, information campaigns, and influence operations, are outlined. Typical themes of military narratives are explored: heroism, sacrifice, brotherhood, struggle for independence, and defense of values. The features of military storytelling are identified, such as emotional intensity, appeal to national identity, visual and audio expressiveness, and adaptation to various platforms (social networks, video, blogs, documentary formats, etc.).

Originality: The study presents in a systematized storytelling as a comprehensive communication tool in the defense sector, combining psychological, marketing, and strategic dimensions. It proposes a structured mechanism for using storytelling to influence public opinion, government decisions, and the positioning of defense industry products in the international environment. The main steps for the practical implementation of storytelling in the strategies of Ukrainian defense sector companies are substantiated.

Paper type: conceptual.

Ключові слова: сторітелінг, національна безпека, військова комунікація, інформаційна війна, стратегічні наративи, оборонний сектор.

Key words: storytelling, national security, military communication, information warfare, strategic narratives, defense sector.

Вступ

У умовах стрімкого розвитку інформаційних технологій та цифрової комунікації сторітелінг, тобто мистецтво передавання інформації через історії, набуває особливої актуальності навіть у таких специфічних і традиційно закритих сферах, як оборонний сектор. Застосування сторітелінгу в цій сфері обумовлено необхідністю досягнення низки важливих цілей національної безпеки держави, серед яких — формування національних оборонних наративів, побудова довіри до виробників озброєння, посилення морально-психологічної стійкості військових, ефективна комунікація із зовнішніми партнерами та просування продукції на міжнародному ринку.

В умовах війни нового типу, коли бойові дії супроводжуються потужними інформаційними кампаніями, розповіді про реальне застосування озброєння, його ефективність у конкретних бойових ситуаціях та історії військовослужбовців, які завдяки цій техніці змогли виконати завдання або врятувати життя, мають надзвичайне значення. Вони не лише мотивують особовий склад і зміцнюють бойовий дух, а й слугують вагомим аргументом для міжнародних партнерів, демонструючи спроможність держави захищатися і водночас раціонально використовувати надану допомогу. Крім того, у глобальній конкуренції на ринку озброєнь важливу роль відіграє здатність країни або компанії презентувати свою продукцію не лише через технічні характеристики, а й через переконливі історії успішного бойового застосування. Такі історії допомагають створити унікальний бренд вітчизняної продукції військового призначення, підвищують її привабливість для потенційних замовників і можуть бути вирішальними при укладанні контрактів. Водночас сторітелінг є ефективним інструментом публічної дипломатії, оскільки дозволяє доносити до міжнародної спільноти правдиву, емоційно наповнену інформацію про оборонний сектор, цінності, які захищає держава, і потреби, що обґрунтовані реальними історіями. Усе це свідчить про те, що сторітелінг в оборонному секторі є не просто елементом комунікації, а стратегічним інструментом інформаційної та безпекової політики, який допомагає в створенні сильного емоційного зв'язку між брендом та її цільовою аудиторією. В контексті функціонування військово-промислового комплексу, сторітелінг використовується як інструмент маркетингу B2G% має вплив на формування іміджу компаній, просування нових зразків озброєння, а також впливу на громадську думку – як урядів різних країн, потенційних партнерів, так і військових та цивільних.

Теоретичні основи дослідження

Тема сторітелінгу в оборонному секторі наразі не є широко дослідженою, проте вона висвітлюється у працях з інформаційної війни, комунікаційних стратегій у сфері безпеки, а також у контексті військової пропаганди та стратегічних наративів. Так наявні публікації підтверджують, що стратегічні наративи активно інтегрують у військову стратегію, оскільки вони формують зв'язок між намірами, діями й сприйняттям громадськості. Зокрема, Блас у статті “Beyond Storytelling” наголошує, що стратегічні наративи стають обов'язковими в умовах геополітичних конфліктів (як-от російсько-українська війна), оскільки вони допомагають пояснювати зміст операцій і зміцнювати легітимність збройних дій (Blas, 2023).

Інший важливий напрям — FICINT (fictional intelligence або “useful fiction”), що поєднує наукову аналітику та художнє оповідання. Цей підхід отримав популярність завдяки авторам типу О. Коула та П.В. Сінгера, які створюють сценарії майбутніх війн, що стимулюють уяву військових та політиків (Singer & Cole, 2020). Слід зазначити практика FICINT активно розвиваються останні три роки: науковці й практики США й Австралії використовують цей метод для навчання військових та трансляції складних технологічних ідей через захопливі історії (National Defence, 2025). Крім того, дослідження НАТО (2024) свідчать про еволюцію наративів від описових до стратегічних, які стали невід'ємною частиною тактики й операцій – особливо в контексті когнітивного виміру війни (Saari, et al., 2024).

Що стосується української наукової спільноти, то з початком збройної агресії російської федерації проти України у 2014 році, включно з анексією Криму та бойовими діями на Сході країни, зросла увага до питань інформаційного супроводу оборонних процесів, зокрема – комунікаційних стратегій та наративів у сфері ВПК. Але не зважаючи на це в українській науковій спільноті майже відсутні дослідження, присвячених питанням трансформації публічного образу оборонної промисловості, ролі сторітелінгу у просуванні українських оборонних технологій на зовнішні ринки, а також впливу стратегічних наративів на розвиток військово-технічної співпраці з партнерами з ЄС та НАТО. Серед наявних публікацій можна відзначити лише напрацювання

Г. Охріменко та І. Приходько (Охріменко та Приходько, 2023), а також О. Скрыбіна, І. Євсєєва, К. Халіманенко, В. Дембіцького (Скрыбін та ін., 2024).

Постановка проблеми

Сучасний оборонний сектор усе активніше застосовує сторітелінг як інструмент формування стратегічних наративів, здатних впливати на громадську думку, легітимізувати військові рішення та підвищувати довіру до інновацій у сфері безпеки. Це зумовлює необхідність дослідження особливостей сторітелінгу в оборонному секторі як нового елементу безпекового дискурсу та публічної взаємодії. Тому метою дослідження є ідентифікація комунікативних та інформаційно-психологічних аспектів застосування сторітелінгу як інструменту впливу у військово-промисловій сфері та сфері національної безпеки.

Результати

У сучасному світі інформація є важливим чинником впливу. У області озброєння, де зазвичай домінують технічні якості та стратегічні розрахунки, все більшого значення набуває сторітелінг – мистецтво створення та розповідей історій. На перший погляд, поєднання такої практичної сфери з емоційним засобом наративу може виглядати неочевидним. Але правильне використання розповіді у області озброєння має великий потенціал для досягнення різних цілей: від формування думки людей до отримання інвестицій й впливу на міжнародні зв'язки.

Сторітелінг — це метод передачі інформації у вигляді зв'язної та емоційно забарвленої історії. Його мета — не тільки інформувати, а й викликати емоції: співпереживання, довіру або мотивацію. Історія може стати сильнішою за сухі факти, оскільки вона впливає на підсвідомий рівень і активізує емоційне мислення аудиторії.

Військова діяльність є занадто складною та прихованою, оскільки інформація, що пов'язана з виробництвом, використанням та продажом зброї, часто вважається конфіденційною, проте оточується дискусіями. У цьому контексті сторітелінг допомагає донести складні ідеї в легко запам'ятовуючій форму, що надає йому особливого значення.

Спосіб комунікації оборонної промисловості значно змінився за останні 15 років. Зокрема, спостерігалось значне зростання використання сторітелінгу як інструменту впливу на громадську думку, залучення нових співробітників, просування технологічних рішень і формування лояльності до бренду. В таблиці нижче представлена умовна динаміка зростання кількості рекламних роликів, публікацій у соцмережах, фільмів, презентацій тощо, створених або на замовлення оборонних компаній з 2010 по 2025 роки.

Таблиця 1 – Тенденції використання сторітелінгу в оборонному секторі

2010-2015 роки: Початковий етап цифрової трансформації	2016-2020 роки: Поширення цифрового контент-маркетингу	2021-2025 роки: Залучення новітніх технологій
Оборонні компанії традиційно використовують закриті канали комунікації, орієнтуючись на урядових замовників та військових. Зростаюча роль цифрових платформ почала впливати на стратегії комунікації.	Основними інструментами комунікації стають соціальні мережі, відео, блоги, інфографіка тощо. Компанії, такі як Raytheon Technologies і Northrop Grumman, активно використовують сторітелінг для демонстрації технологічних досягнень і залучення громадськості.	Популярним стає використання штучного інтелекту, доповненої реальності для створення персоналізованого контенту. Активно застосовуються соціальні мережі для взаємодії з громадськістю та підвищення прозорості діяльності.

Джерело: складено авторами за відкритими даними

Дані показують, що сторітелінг поступово зріс у першій половині 2010-х років, швидко розвивався після 2016 року на тлі загострення геополітичних конфліктів і активізувався після 2020 року, коли цифрова трансформація набула чинності. До 2025 року сторітелінг стане одним із ключових інструментів публічної комунікації в секторі безпеки та оборони.

Однією з головних особливостей сторітелінгу в сфері озброєння виступає мета у формуванні певного наративу. В залежності від цілей, історії можуть привертати увагу та наголошувати на наступних ідеях:

1. Потреба модернізації та оновленні армії (історії про наявне застаріле та невідповідне обладнання та озброєння, в порівнянні з успішними прикладами сучасних розробок, що можуть переконати державні органи та громадськість у потребі інвестицій у нові технології).

2. Пріоритети наявності та використання конкретних видів озброєння (успішні історії про використання певної зброї та досягнення певних цілей в реальних ситуаціях можуть підвищити інтерес для її придбання потенційними покупцями).

3. Мужність, хоробрість та відвага військовослужбовців (історії про військову службу, підготовку на високому рівні, готовність до будь-якого супротиву, формують позитивні враження про стійкий характер військових, що має вплив на зміцнення зв'язку між армією та громадським населенням, підвищуючи авторитет військової діяльності).

4. Забезпечення національної безпеки (історії про потенційні загрози для держави та суспільства, ефективність використання всього або певного виду озброєння для їх подолання чи недопущення, мають на меті обґрунтування витрат на оборону та військово-промисловий комплекс, оскільки дані витрати є інвестицією у власну безпеку).

Виходячи з аналізу тенденцій за 2024 рік, в тому числі в контексті війни в Україні, зростання оборонних витрат у Європі та США, а також впливу новітніх технологій на комунікаційні стратегії, можна виділити співвідношення ключових тем, які найчастіше зустрічаються у військовому сторітелінгу. Найбільшу частку займають теми героїзму та патріотизму — вони забезпечують глибокий емоційний зв'язок із аудиторією та стимулюють лояльність до військових структур. Також помітну частину займають наративи загрози, що підсилюють відчуття небезпеки та потреби в захисті. Технічні теми, як-от інновації або безпека, менш емоційні, але виконують раціональну функцію переконання (рис. 1).

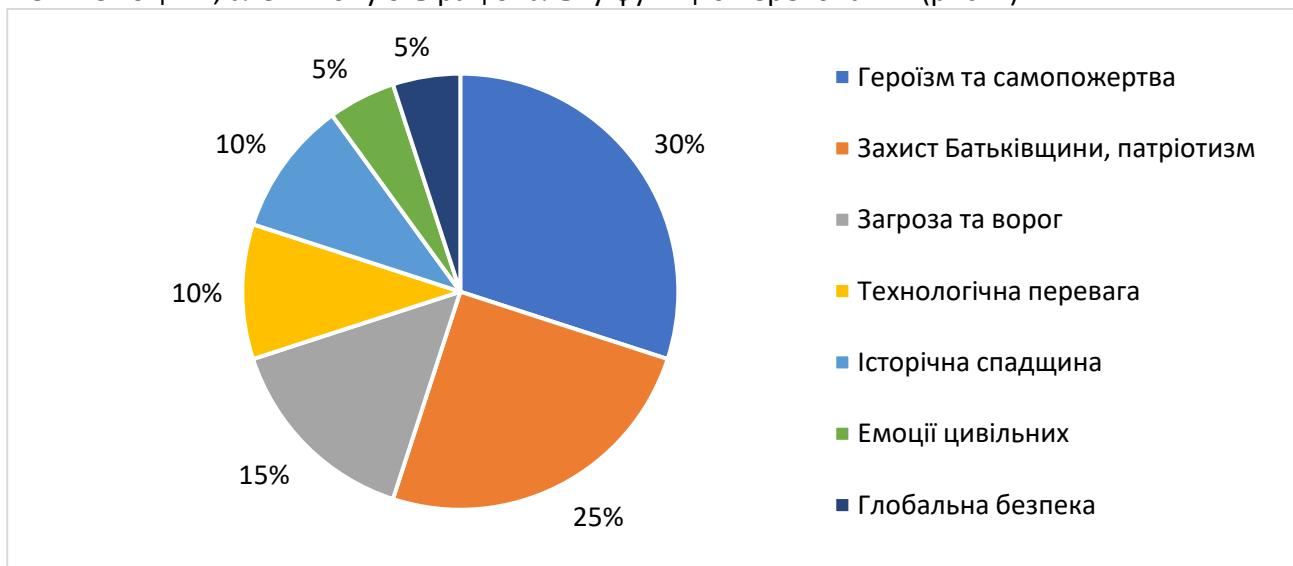


Рисунок 1 – Співвідношення тематик у військових наративах

Джерело: складено авторами

Сторітелінг у військовій сфері вважається досить складним явищем, яке вимагає глибокого розуміння теми, дотримання вимог безпеки, врахування етичних норм та

відповідного використання емоційної сили наративу. Оскільки кожна історія може бути як позитивно, так і негативно вплинула на суспільну думку, політичні рішення та навіть хід війни. Виходячи з цього, військових сторітелінг має свої унікальні та специфічні риси для його використання (табл. 2).

Таблиця 2 – Особливості військового сторітелінгу

Ознака	Його характеристика
Співвідношення між правдою та пропагандою	Не в залежності від того, що історії мають нести емоційне, мотивуюче забарвлення, бути переконливими, вони в першу чергу мають бути правдоподібними. Перебільшення пропаганди може викликати недовіру, маючи зворотній ефект.
Дотримання конфіденційності	У використанні військового сторітелінгу важливо уникати витоку інформації. Історії, що подаються суспільству, мають бути узгоджені для забезпечення безпеки. Не можна зазначати місця розташування військових, назви та місця важливо стратегічних об'єктів або деталі операцій. Дані обмеження вказують на головній цілі – зосередження на людському аспекті історії.
Емоційний та моральний вплив на суспільство	Історії про війну завжди дуже емоційні, вони мають втрати, біль, страх, надію та героїзм. Військові історії можуть як надихати, так і бути психологічно важко сприйнятими. Саме тому важливо донести інформацію правильно, щоб ні в якому разі не романтизувати війну, не знецінювати страждання, не перетворювати біду на сенсацію.
Зв'язок з національною ідентичністю	Військовий сторітелінг має відповідати національному контексту (захист Батьківщини, використання національних символів – прапору, гімну, гербу, зв'язок з історією та подіями минулого). Це домагає створювати великі наративи, будуючи загальну історію боротьби за незалежність та свободу і захисту країни.
Використання візуальних засобів	Візуальний контент допомагає в збереженні довіри глядача. Відеоматеріал, фотографії можуть мати набагато більший вплив та переконливість історій про озброєння. Окрім цього вони додають більшого емоційного забарвлення кожній історії.
Націленість на певну цільову аудиторію	Військові історії мають різну мету, в залежності від їхніх слухачів, відповідно мають адаптуватися: посилення мотивації та важливості підтримки армії для громадян, підтримка бойового духу, відчуття єдності з народом для військових, демонстрація героїзму військових та переконання у правильності дій з боку держави для іноземної аудиторії.

Джерело: складено авторами

В сучасний період сторітелінг активно використовується у різних аспектах, пов'язаних з військовою діяльністю, оборонною промисловістю та озброєння. Найпоширеніший приклад, з яким стикається нині кожен, це історії в соціальних мережах та медіа про бойові дії, військових, їхніх побратимів, особисті переживання, втрати та перемоги, озброєння, яке допомогло видити (наприклад, історія в Facebook від командира підрозділу про український БТР, який витримав пряме влучання, що зберегло життя всім військовим). Також в мережі Інтернет та на телебаченні з'явилася велика кількість військових фільмів та роликів про військові підрозділи, життя військових, їхній шлях та досягнення (наприклад, відео, які показують, як звичайна людина, фахівець в своїй справі, кардинально змінює сферу, вступивши до лав Збройних Сил України). Активно використовують сторітелінг і військові частини для формування іміджу армії та рекрутингу. Історії про військових, їхнє життя до та після, переваги певної бригади, використовують для залучення нових людей в команду. Щодо зв'язку з військовою технікою, наразі існує велика кількість експозицій та виставок у військових музеях і не тільки. Окрім технічного опису озброєння, згадується також хто створив цю техніку, як вона працювала під час бойових дій і як допомогла армії забезпечити перевагу чи навіть

врятувати життя. Самі виробники військової техніки залучають сторітелінг для зовнішньої комунікації. Наприклад, оборонні компанії “Укроборонпром”, “Baykar”, “Rheinmetall” публікують не лише характеристики озброєння, вони також публікують особисті історії виробників та випробувачів, відеоролики створення техніки від перших кроків до використання в бойових діях, показують історії збереження життя військових за їх допомогою (див. наприклад (Baykar, 2022; NEW EASTERN EUROPE, 2025).

На рисунку 2 представлено механізм використання сторітелінгу в оборонному секторі, який ілюструє ключові етапи — від формування наративів до досягнення стратегічних цілей.

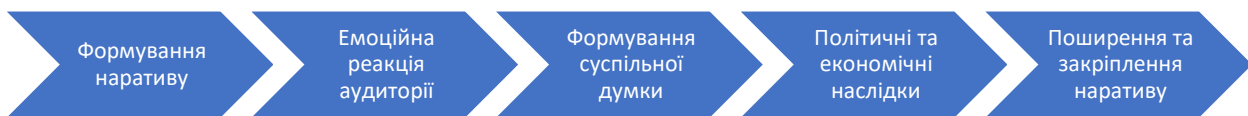


Рисунок 2 – Механізм використання сторітелінгу в оборонному секторі

Джерело: розроблено авторами

Центральним елементом цього процесу є змістовне та емоційне відображення реальних історій, здатних викликати цільову емоційну реакцію в аудиторії. Такі наративи виконують роль каталізаторів інформаційного впливу, оскільки не лише передають фактичні відомості про події, продукцію або дії військових структур, а й забезпечують глибоке залучення, емпатію та ідентифікацію з образами героїв, технологій або ідей.

Емоційний вплив на аудиторії забезпечує трансформацію окремого наративу в засіб формування колективної думки в сфері національної безпеки. В умовах російсько-української війни саме суспільна думка має стати фундаментом політичних рішень щодо розподілу бюджетних ресурсів, пріоритетів державного оборонного замовлення або легітимації стратегічних альянсів. Таким чином, сторітелінг в оборонному секторі виконує функцію не лише комунікаційного інструменту, а й непрямого важеля впливу на прийняття рішень у сфері безпеки та оборони.

Крім того, закріплення військових наративів у масовій культурі — через фільми, документалістику, соціальні мережі або навіть ігрову індустрію — сприяє формуванню стійких образів, що резонують з архетипами сили, захисту, технологічної переваги. Такий наративний контент часто набуває вірусного характеру, повторюється, варіюється та вбудовується в ширший інформаційний простір, створюючи ефект позитивного зворотного зв'язку. У результаті сторітелінг перетворюється на потужний мультиплатформенний інструмент стратегічних комунікацій, що здатний забезпечити довготривалий емоційний і політичний резонанс для формування ідеології національної єдності, підтримки вітчизняних оборонних стратегій та посилення міжнародного позиціонування українських оборонних компаній.

Висновки

Отже сторітелінг — це не лише спосіб подачі певної інформації, це повноцінний інструмент формування свідомості та впливу, особливо в сфері військової діяльності. Через правдиві, емоційні розповіді формується не тільки ставлення до війни, армії або техніки, а також цінності суспільства, моральна готовність та віра у перемогу. Відповідно у часи війни правильно побудована історія може не тільки зачепити слухача, вона здатна мобілізувати, навчити, об'єднати та врятувати.

Сторітелінг в оборонному секторі поступово трансформується зі звичайного інструменту комунікації у стратегічний ресурс впливу, що охоплює водночас емоційну, інституційну та економічну площини. Його ефективне використання дозволяє створювати символічний капітал військової та оборонної продукції, посилюючи суб'єктивне сприйняття її цінності як на внутрішньому, так і на зовнішньому рівні. Наративи, що народжуються з реального бойового

досвіду, персональних історій військовослужбовців або виробників, стають не просто засобом інформування, а цілісною системою передачі значень, яка формує довіру, мобілізує підтримку, створює репутаційні переваги та в цілому посилює національну безпеку.

В умовах інформаційно-психологічної війни, у якій Україна перебуває з 2014 року, сторітелінг стає не лише інструментом переконання або маркетингу, а засобом відстоювання суб'єктності держави в глобальному безпековому середовищі. Історії, які демонструють ефективність озброєння, моральну перевагу воїнів чи адаптивність оборонної промисловості, формують впізнавану візуальну та змістову ідентичність українського ВПК, сприяючи його просуванню на міжнародних ринках і підвищенню переговорної сили у сфері військово-технічного міжнародного співробітництва.

Крім того, наративи, що ґрунтуються на реальному бойовому досвіді, не лише сприяють формуванню іміджу окремих компаній або технологій, але й підсилюють загально-національний бренд безпеки та оборони. Саме тому сторітелінг доцільно розглядати як інструмент національної безпеки – такий, що поєднує медійні технології, цільову психологічну дію, маркетингову логіку та політичну прагматику.

В контексті розвитку українського оборонного сектору в умовах російсько-української війни важливо не лише технологічне нарощування потенціалу, а й вміння супроводжувати це розвитком ефективних стратегічних наративів. Це вимагає підготовки фахівців, здатних мислити як інженери, так і комунікатори, а також формування інституційної культури комунікації в оборонному секторі, орієнтованої на відкритість, репутаційну відповідальність і цілеспрямовану побудову національної безпекової ідентичності. Отже відповідно до отриманих результатів дослідження нами запропоновано основні кроки для практичного впровадження сторітелінгу у стратегії українських компаній оборонного сектору:

- обов'язкова розробка внутрішнього протоколу перевірки контенту на предмет витоку чутливої інформації (місця, об'єкти, технічні характеристики);

- проведення тренінгів з етичного сторітелінгу для PR-фахівців та контент-мейкерів компанії - щоб уникнути маніпуляцій, романтизації війни, пропаганди;

- систематизація реальних історій бойового застосування техніки, її ролі у збереженні життя, успішному виконанні місій;

- використання досвіду користувачів техніки (user experience) – історії від військових, інженерів, інструкторів (із дотриманням заходів безпеки та конфіденційності);

- побудова презентацій та публічних виступів у форматі “реальний виклик – наше рішення – доказ ефективності”;

- вбудовування сторітелінгу в корпоративні стенди на виставках: стенди повинні розповідати історію, а не просто демонструвати ТТХ;

- активне використання соціальних мереж: LinkedIn, X (ex-Twitter), YouTube, Instagram – для створення коротких історій, серій, реактивних постів;

- просування українського оборонного сектору як ціннісного бренду, що боронить не лише Україну, а й принципи свободи та партнерства в регіоні.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

Blas, N. (2023). Beyond storytelling. *Æther: A Journal of Strategic Airpower & Spacepower*, 2(1), 46-57. Available from : [https://www.airuniversity.af.edu/Portals/10/ÆtherJournal/Journals/Volume-2 Number-1/Blas-Beyond-Storytelling.pdf](https://www.airuniversity.af.edu/Portals/10/ÆtherJournal/Journals/Volume-2%20Number-1/Blas-Beyond-Storytelling.pdf)

- Singer, P. W., & Cole, A. (2020). *Burn-in: A Novel of the Real Robotic Revolution*. Mariner Books.
- National Defence (2025). Startup Helps Officers Explain Future Warfare Through Storytelling. Available from : <https://www.nationaldefensemagazine.org/articles/2022/12/16/startup-helps-officers-explain-future-warfare-through-storytelling>
- Saari, D., Häkkinen, T., & Moilanen, P. (2024). A Comprehensive Analysis of Narratives within NATO's Doctrines. In *Proceedings of the European Conference on Cyber Warfare and Security* (Vol. 23, No. 1). Academic Conferences International Ltd. Available from : <https://pdfs.semanticscholar.org/781a/d69e9845867a1f550861f71bf0fa685954f4.pdf>
- Охріменко, Г. В., & Приходько, І. П. (2023). Digital-сторітелінг на теренах медійного простору: аналіз контентоутворення. *Інформація та соціум*, 58-60. Available from : <https://ijas.donnu.edu.ua/article/view/14559>
- Скрябін, О., Євсєєв, І., Халіманенко, К., & Дембіцький, В. (2024). Використання радянською пропагандою комунікативно-пропагандистських технологій впливу для формування "образу США" під час холодної війни. *Вісник Національного університету оборони України*, 141-151. <https://doi.org/10.33099/2617-6858-2024-82-6-141-151>.
- Baykar (2022). Turkish drones have become a symbol of the Ukrainian resistance. Available from : <https://baykartech.com/en/press/turkish-drones-have-become-a-symbol-of-the-ukrainian-resistance/>
- New Eastern Europe (2025) Securing stability: powering Ukraine's defence production surge. Available from : <https://neweasterneurope.eu/2024/07/26/securing-stability-powering-ukraines-defence-production-surge/>

References

- Blas, N. (2023). Beyond storytelling. *Æther: A Journal of Strategic Airpower & Spacepower*, 2(1), 46-57. Available from : [https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-2 Number-1/Blas-Beyond-Storytelling.pdf](https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-2%20Number-1/Blas-Beyond-Storytelling.pdf)
- Singer, P. W., & Cole, A. (2020). *Burn-in: A Novel of the Real Robotic Revolution*. Mariner Books.
- National Defence (2025). Startup Helps Officers Explain Future Warfare Through Storytelling. Available from : <https://www.nationaldefensemagazine.org/articles/2022/12/16/startup-helps-officers-explain-future-warfare-through-storytelling>
- Saari, D., Häkkinen, T., & Moilanen, P. (2024). A Comprehensive Analysis of Narratives within NATO's Doctrines. In *Proceedings of the European Conference on Cyber Warfare and Security* (Vol. 23, No. 1). Academic Conferences International Ltd. Available from : <https://pdfs.semanticscholar.org/781a/d69e9845867a1f550861f71bf0fa685954f4.pdf>
- Okhrymenko, H. V., & Prykhodko, I. P. (2023). Digital storytelling in the media space: An analysis of content creation. *Informatsiia ta Sotsium*, 58-60. Available from : <https://ijas.donnu.edu.ua/article/view/14559>.
- Skriabin, O., Yevsieiev, I., Khalimanenko, K., & Dembitskyi, V. (2024). The use of communicative and propaganda technologies of influence by Soviet propaganda to form the "image of the USA" during the Cold War. *Visnyk Natsionalnoho Universytetu Oborony Ukrainy*, 141-151. <https://doi.org/10.33099/2617-6858-2024-82-6-141-151>.
- Baykar (2022). Turkish drones have become a symbol of the Ukrainian resistance. Available from : <https://baykartech.com/en/press/turkish-drones-have-become-a-symbol-of-the-ukrainian-resistance/>
- New Eastern Europe (2025) Securing stability: powering Ukraine's defence production surge. Available from : <https://neweasterneurope.eu/2024/07/26/securing-stability-powering-ukraines-defence-production-surge/>

Формування моделей оцінки ефективності стрільби зенітними керованими ракетами з урахуванням ймовірностей ураження повітряних цілей

Development of Evaluation Models for Surface-to-Air Missile Firing Effectiveness with Consideration of Air Target Kill Probabilities

Павло Опенько ^A

Corresponding author: к.т.н. старший дослідник, Заслужений винахідник України, начальник кафедри, e-mail: pavel.openko@ukr.net, ORCID: 0000-0001-7777-5101

Олександр П'явчук ^A

доктор філософії, старший викладач кафедри, e-mail: pjawa0905@gmail.com, ORCID: 0000-0002-5623-1866

Юрій Целіщев ^A

к.т.н., доцент, доцент кафедри, e-mail: pjawa0905@gmail.com, ORCID: 0000-0002-3739-9567

Віктор Кудряшов ^B

к.т.н., старший науковий співробітник, старший науковий співробітник відділу нелінійної динаміки електронних систем інституту, e-mail: victor.e.kudryashov@gmail.com, ORCID: 0000-0002-7055-5357

Олексій Коломійцев ^C

д.т.н., професор, Заслужений винахідник України, професор кафедри комп'ютерної інженерії та програмування, e-mail: alexus_k@ukr.net, ORCID: 0000-0001-8228-8404

Валерій Воїнов ^D

к.т.н., доцент, заступник начальника факультету з навчальної та наукової роботи, e-mail: Vvoinov80@gmail.com, ORCID: 0000-0002-5732-5960

Pavlo Openko ^A

Corresponding author: Candidate of Technical Sciences, Senior Research Fellow, Honored Inventor of Ukraine, Head of the Department, e-mail: pavel.openko@ukr.net, ORCID: 0000-0001-7777-5101

Oleksandr Piavchuk ^A

PhD, Senior Lecturer of the Department, e-mail: pjawa0905@gmail.com, ORCID: 0000-0002-5623-1866

Yurii Tselishev ^A

Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department, e-mail: pjawa0905@gmail.com, ORCID: 0000-0002-3739-9567

Viktor Kudriashov ^B

Candidate of Technical Sciences, Senior Research Fellow, Senior Research Fellow Department, e-mail: victor.e.kudryashov@gmail.com, ORCID: 0000-0002-7055-5357

Oleksii Kolomiitsev ^C

Dr of Engineering Science, Professor, Professor of the Department, e-mail: alexus_k@ukr.net, ORCID: 0000-0001-8228-8404

Voinov Valerii ^D

Candidate of Technical Sciences, Associate Professor, Deputy Dean of Army Air Defence Faculty, e-mail: Vvoinov80@gmail.com, ORCID: 0000-0002-5732-5960

^A Національний університет оборони України, м. Київ, Україна

^B Інститут радіофізики та електроніки НАН України ім. О. Я. Усікова, м. Харків, Україна

^C Національний технічний університет "Харківський політехнічний інститут", м. Харків, Україна

^D Харківський національний університет Повітряних Сил ім. І. Кожедуба, м. Харків, Україна

^A National Defence University of Ukraine, Kyiv, Ukraine

^B O.Ya. Usikov Institute for Radiophysics and Electronics of the National Academy of Sciences of Ukraine, Kharkiv, Ukraine

^C National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

^D Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

Received: August 7, 2025 | Revised: August 19, 2025 | Accepted: August 31, 2025

УДК: 519.2-623.1/.7

DOI: <https://doi.org/10.33445/sds.2025.15.4.8>

Мета роботи. Розробити часткову модель для розрахунку значень умовних ймовірностей ураження цілі, для формування найкращих варіантів відбиття удару повітряного противника, а також обґрунтування загальних напрямків удосконалення елементів системи управління вогнем.

Метод. основними методами дослідження є: статистичного аналізу, чисельний метод, порівняльного аналізу.

Результати дослідження. В цілому приведена залежність величин умовних ймовірностей ураження цілей від дев'яти основних параметрів, які описують стрільбу зенітними керованими ракетами та управління вогнем. Отримані практичні результати часткової моделі необхідні для ефективного застосування озброєння за призначенням.

Теоретична цінність дослідження. В статті приведено розрахунки, які дозволяють завчасно розробити декілька варіантів дій самохідних вогневих одиниць (бойових машин), підрозділів при відбитті повітряного удару противника.

Purpose. To develop a partial model for calculating the values of conditional probabilities of target engagement, to generate optimal options for countering enemy air strikes, and to justify the general directions for improving elements of the fire control system.

Method. The main research methods are: statistical analysis, numerical methods, and comparative analysis.

Findings. A relationship is presented between the values of conditional probabilities of target engagement and nine key parameters that characterize surface-to-air missile firing and fire control. The practical results obtained from the partial model are essential for the effective employment of weapon systems as intended.

Theoretical implications. The article provides calculations that make it possible to pre-plan several courses of action for self-propelled fire units (combat vehicles) and subunits in repelling enemy air strikes. The model takes into account the

При цьому враховано параметри удару повітряного противника по бойових порядках військ (сил). У теперішній час відсутня часткова модель, яка визначить значення ефективності стрільби з врахуванням ймовірностей входу повітряних цілей в зону цілерозподілу. Також проведена оцінка ймовірності не виходу повітряних цілей з зони пуску та зони ураження зенітного ракетного комплексу, після пуску зенітних керованих ракет, при цьому враховано вплив ефективної поверхні розсіювання цілей, рівень перешкод і перевантажень цілі, при її маневруванні. Тому задача розробки варіантів дій самохідних вогневих одиниць (бойових машин), підрозділів при відбитті удару противника є важливою та актуальною.

Тип статті. Науково-практична.

parameters of the enemy air strike against the combat formations of friendly forces. Currently, there is no existing partial model that determines the effectiveness of missile firing while considering the probabilities of air targets entering the target allocation zone. The study also includes an assessment of the probability that air targets will not exit the missile launch and engagement zones of the surface-to-air missile system after launch. This assessment considers factors such as the effective radar cross-section (RCS) of targets, the level of jamming, and target overload during maneuvering. Therefore, the task of developing response options for self-propelled fire units and subunits in countering enemy strikes is both important and timely.

Paper type. Scientific and practical.

Ключові слова: відношення сигнал-шум, ймовірності вірного виявлення, ймовірності входу цілей у зони цілерозподілу, ймовірності не виходу цілей з зон пуску (ураження) комплексу, параметри першого та другого родів стрільби ракетами, умовні ймовірності ураження цілей, цілерозподіл.

Key words: signal-to-noise ratio, probabilities of correct detection, probabilities of target entry into target allocation zones, probabilities of target retention within missile launch (engagement) zones, first- and second-type missile firing parameters, conditional probabilities of target engagement, target allocation.

Вступ

Управління вогнем (УВ) підрозділів протиповітряної оборони (ППО) передбачає завчасно розробку декількох варіантів дій самохідних вогневих одиниць (бойових машин), підрозділів (батареї) при відбитті удару повітряного противника. При цьому необхідно враховувати параметри удару повітряного противника по бойових порядках військ (сил) [1-5]. У теперішній час відсутня часткова модель, яка визначить значення ефективності стрільби з врахуванням ймовірностей входу цілей в зону цілерозподілу (ЦР). Також потрібно оцінювати ймовірності не виходу цілей з зони пуску (ЗПу) та зони ураження (ЗУ) зенітного ракетного комплексу, після пуску зенітних керованих ракет. Необхідно враховувати вплив ефективної поверхні розсіювання (ЕПР) цілей, рівень перешкод і перевантажень цілі, при її маневруванні. Тому задача розробки варіантів дій самохідних вогневих одиниць (бойових машин), підрозділів (батареї) при відбитті удару противника є важливою та актуальною. В якості показника ефективності УВ застосовуємо значення умовних ймовірностей ураження цілей [1-3].

Теоретичні основи дослідження

Відомо, що УВ підрозділами військ ППО полягає у цілеспрямованій діяльності командирів (начальників), штабів, бойових розрахунків сумісних командних пунктів авіації і протиповітряної оборони (СКП А і ППО), командних пунктів (КП), пунктів управління (ПУ) по підтримці бойової готовності військових частин (підрозділів) ППО, підготовці бойових дій (операцій) і управління ними при відбитті ударів засобів повітряного нападу (ЗПН) противника. Метою УВ підрозділами військ ППО є повне використання вогневих можливостей підрозділів військ ППО для надійного прикриття та захисту підрозділів (угруповань) військ та інших об'єктів від ударів ЗПН противника, для знищення засобів повітряної розвідки, носіїв високоточної зброї, повітряних десантів та повітрянодесантних військ противника в повітрі.

На сьогодні основними видами цілерозподілу (ЦР) є: централізований, децентралізований, автономний та змішаний ЦР повітряних цілей (ПЦ). Взагалі, ЦР ПЦ між вогневими засобами підрозділів (угруповання) військ ППО, які прикривають підрозділи (угруповання) військ та інші об'єкти з повітря, вимагає витрати часу, пов'язаного з обробкою інформації про повітряну обстановку. Автоматизація даного процесу прямо пов'язана з необхідністю вдосконалення цього елемента контуру управління, завдяки впровадженню методу ефективного ЦР при УВ підрозділу. Вибір методу дає можливість прискорити прийняття рішення командиром будь-якої ланки по ефективному розподілу цілей при УВ підрозділу і уникнути збитки об'єктам, які прикриваються.

Проблема вдосконалювання УВ підрозділами військ ППО полягає у вирішенні протиріччя між вже досягнутими та всезростаючими можливостями вогневих засобів з одного боку, та, з іншого – з можливостями системи управління по використанню вогню зенітних засобів для надійного прикриття та захисту підрозділів (угруповань) та об'єктів. Проведений для цього аналіз публікацій, котрі представлені у літературі [1-6] не дають можливості визначати показники ефективності стрільби по різних цілях, в умовах протидії противника, та в відповідності до технічних характеристик елементів схеми УВ. В вказаній літературі приведені загальні підходи до рішення даної задачі.

Постановка проблеми

На підставі вищевикладеного, можливо стверджувати, що пошук рішення для отримання централізації та децентралізації функцій управління КП і ПУ різних рівнів для використання достоїнств кожного з видів ЦР, установлення залежності ефективності застосування самохідних вогневих одиниць (бойових машин), підрозділів (батареї) від цього співвідношення та на даній основі – розробка оптимальних управляючих алгоритмів та визначення напрямків удосконалювання технічних засобів і структури системи УВ – одне з найважливіших завдань теорії і практики УВ підрозділами (угрупованнями) військ ППО при веденні бойових дій (операцій). Удосконалення управління самохідними вогневими одиницями (бойовими машинами), підрозділами (угрупованнями) військ ППО та його найважливішої складової частини – УВ, поряд з якісним удосконалюванням зенітних ракетних комплексів, є основним напрямком підвищення бойових можливостей підрозділів (угруповань) військ ППО по відбиттю ударів ЗПН противника.

Метою статті є розробка часткової моделі для розрахунку значень умовних ймовірностей ураження цілі, для формування найкращих варіантів відбиття удару повітряного противника, а також обґрунтування загальних напрямків доробки елементів системи УВ.

Результати

Для досягнення мети статті розглянемо спрощену схему УВ, яка зазвичай реалізується. Спрощена схема УВ складається з послідовно з'єднаних радіолокаційних станцій (РЛС) старшого начальника, командного пункту полка (КПП), батареїного командного пункту (БКП) та самохідних вогневих одиниць (бойових машин), підрозділу (батареї) [1-6].

1. Визначення дальнього та ближнього рубежів постановки вогневих завдань, дальньої та ближньої межі зони повітряної обстановки [1, 2].

Для типової цілі (ТЦ) обрали осереднену швидкість підльоту V у 230 м/с та висоту польоту H в 10^3 м.

$$\begin{aligned} D_{\text{ДПЗ}} &= \left\{ \{d_d + V[\tau_{\text{КПП}} + \tau_{\text{БКП}} + \tau_{\text{ППС}} + \tau_{\text{БПС}} + \tau_{\text{СТ}} + \tau_{\text{РД}}]\}^2 + H^2 \right\}^{0,5}, \\ D_{\text{БПЗ}} &= \left\{ \{d_b + V[\tau_{\text{КПП}} + \tau_{\text{БКП}} + \tau_{\text{ППС}} + \tau_{\text{БПС}} + \tau_{\text{СТ}} + \tau_{\text{РБ}}]\}^2 + H^2 \right\}^{0,5}, \quad h_{\text{ЦР}} = VT_{\text{Ц.стр.}}, \\ D_{\text{ДПО}} &= D_{\text{ДПЗ}} + 2h_{\text{ЦР}}, \quad D_{\text{БПО}} = D_{\text{ДПЗ}} + h_{\text{ЦР}}, \end{aligned} \quad (1)$$

- де $D_{\text{ДПЗ}}, D_{\text{БПЗ}}$ – відповідно дальній та ближній рубежі постановки вогневих завдань самохідними вогневими одиницями (бойовими машинами);
- d_d, d_b – горизонтальні дальності до дальньої та ближньої границі зони ураження (ЗУ);
- $\tau_{\text{КПП}}, \tau_{\text{БКП}}$ – робітні часи КПП та БКП відповідно;
- $\tau_{\text{ППС}}, \tau_{\text{БПС}}$ – відповідно часи попередньої та безпосередньої підготовки стрільби самохідними вогневими одиницями (бойовими машинами);
- $\tau_{\text{СТ}}$ – час затримки старту зенітної керованої ракети;

- $\tau_{рд}, \tau_{рб}$ – часи польоту ракети до дальньої межі зони ураження (ДМЗУ) та ближньої межі зони ураження (БМЗУ) відповідно;
 $D_{дпо}, D_{бпо}$ – дальня та ближня межі повітряної обстановки відповідно;
 $h_{цр}, T_{ц.стр.}$ – відповідно глибина ЦР та час циклу стрільби самохідної вогневої одиниці (бойової машини); причому час польоту ракети до i точки ЗУ дорівнює: $\tau_{pi} = 2,5 + 1,75 \cdot 10^3 D$.

Якщо $d_d = 10^4$ м, $\tau_{кпп} \approx \tau_{бкп} \approx 31$ с в умовах перешкод середньої щільності, $\tau_{ппс} = 218$ с, $\tau_{бпс} = 55$ с, $\tau_{ст} \approx 1,5$ с, $\tau_{рд} \approx 20$ с, $d_b = 1,5 \cdot 10^3$ м, $\tau_{рб} \approx 5,1$ с, $T_{ц.стр.} \approx 90$ с в умовах перешкод середньої щільності. Отримали при готовності самохідної вогневої одиниці (бойової машини) № 2 $D_{дпз} \approx 92 \cdot 10^3$ м, $D_{бпз} \approx 80 \cdot 10^3$ м, а з готовності № 1 – $D_{дпз} \approx 41,9 \cdot 10^3$ м, $D_{бпз} \approx 30 \cdot 10^3$ м та $h_{цр} \approx 20,7 \cdot 10^3$ м. Причому при готовності самохідної вогневої одиниці (бойової машини) № 1 маємо: $D_{дпо} \approx 83,3 \cdot 10^3$ м та $D_{бпо} \approx 62,6 \cdot 10^3$ м.

Відмічаємо достатньо значні дальності рубежів постановки вогневих завдань та меж повітряної обстановки при лише завадах середньої щільності та роботі по ТЦ.

2. Відношення сигнал/шум (с/ш) у радіолокаційному каналі РЛС старшого начальника та імовірності вірного виявлення цілей у різноманітних умовах застосування [4, 6-8].

В якості технічних характеристик РЛС старшого начальника обрали умовні характеристики евентуальної РЛС, наближені до характеристик РЛС П-18. Відношення с/ш $q_v(D, \sigma, \Delta)$ і імовірності вірного виявлення $P_v(D, \sigma, \Delta)$ при дії активних шумових перешкод (АШП) дорівнюють:

$$q_v(D, \sigma, \Delta) = \sqrt{(2,016 \cdot 10^{20} \sigma) / [D^4 (1 + \Delta)]},$$

$$P_v(D, \sigma, \Delta) = F\{1 / [1 + 0,5 q_v(D, \sigma, \Delta)^2]\}, \quad (2)$$

- де σ, D – відповідно ЕПР цілі (ЕПР ТЦ $\sigma_{ТЦ} = 1$ м²) та дальність до неї;
 Δ – відношення потужності АШП до потужності власних шумів радіолокаційного (РЛ) каналу РЛС, які залишилися після відповідної компенсації (для середньої щільності $\Delta = 7$ дБ (5 разів));
 F – фіксований рівень помилкової тривоги РЛ каналу (обрали $\sim 10^{-2}$).

Одержали $q_v(65 \cdot 10^3; 1; 0) \approx 3,36$ рази, $q_v(65 \cdot 10^3; 1; 5) \approx 1,37$ рази і відповідно $P_v(65 \cdot 10^3; 1; 0) = 0,5$ і $P_v(65 \cdot 10^3; 1; 5) \approx 0,1$. Результати розрахунків за виразами (1), (2) приведені на рис. 1.

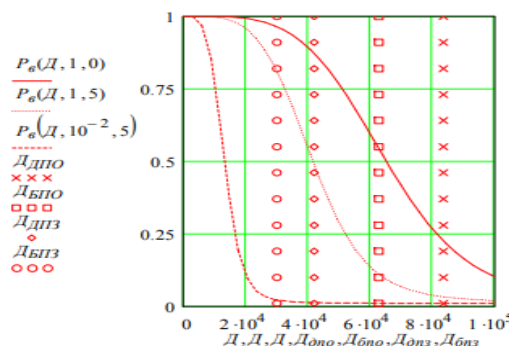


Рисунок 1 – Імовірності вірного виявлення $P_v(D, \sigma, \Delta)$ та меж зон повітряної обстановки $D_{дпо}$, $D_{бпо}$ і рубежі постановки вогневих завдань $D_{дпз}$ і $D_{бпз}$

Джерело: розроблено авторами

Перша крива $P_{B1}(D)$ позначена безперервною лінією, побудована при роботі по ТЦ і відсутності перешкод. Друга крива $P_{B2}(D)$ (точки) відображає значення імовірностей виявлення ТЦ при наявності АШП середньої щільності ($\Delta = 5$ разів). Третя крива $P_{B3}(D)$ (тире) отримана для випадку виявлення безпілотного літального апарату (БПЛА) на фоні перешкод $\Delta = 5$ разів. Четверта ($\times \times \times$) та п'ята ($\square \square \square$) прямі показують відповідно дальню $D_{ДПО}$ і ближню $D_{БПО}$ межі зон повітряної обстановки. Шоста ($\diamond \diamond \diamond$) та сьома ($\circ \circ \circ$) прямі відображають дальній $D_{ДПЗ}$ і ближній $D_{БПЗ}$ рубежі постановки вогневих завдань. При прийнятих технічних характеристиках РЛС старшого начальника на $D_{ДПО}$ маємо $P_B(83,3 \cdot 10^3; 1; 5) \approx 0,03$, а на $D_{БПО}$ $P_B(62,6 \cdot 10^3; 1; 5) \approx 0,11$, що не уможливорює проведення централізованого ЦР (ЦЦР) у підрозділі. Внаслідок цього застосовується не ЦЦР, а децентралізований ЦР (ДЦР). Лише на $D_{ДПЗ}$ отримали $P_B(41,9 \cdot 10^3; 1; 5) \approx 0,49$, що теж не задовольняє. При роботі по БПЛА (третя крива, рис. 1) самохідні вогневі одиниці (бойові машини) в змозі проводити стрільбу по цілях, які раптово з'являються. В цілому відмітимо не значний енергетичний потенціал РЛС старшого начальника та її перешкодостійкість.

3. Імовірності входу цілей в зони ЦР у різноманітних умовах [1, 2, 6, 7].

Визначення ймовірностей входу в зони ЦР передбачає розрахунок: а) середнє квадратичне відхилення (СКВ) помилки вимірювання азимуту цілі при відсутності викривлень пачки при флуктуації корисних сигналів $\sigma_B(D, \sigma, \Delta)$; б) часу $\tau_1(n)$ між n відмітками по цілі при огляду простору РЛС старшого начальника 6 об/хв.; в) СКВ помилки параметру цілі $\sigma_p(D, \sigma, \Delta, n, V)$. Так:

$$\begin{aligned}\sigma_B(D, \sigma, \Delta) &= \frac{\sqrt{\pi} \theta}{q_6(D, \sigma, \Delta) 180}, \\ \tau_1(n) &= n(60/6), \\ \sigma_p(D, \sigma, \Delta, n, V) &= \frac{\sqrt{2} \sigma_B(D, \sigma, \Delta)}{(n-1)V\tau_1(n)} \cdot \\ &\quad \left[D - \frac{(n-1)V\tau_1(n)}{2} \right]^2, \quad (3)\end{aligned}$$

де θ – напівширина діаграми спрямованості антени РЛС старшого начальника (прийняли 6°).

Також потрібно знайти граничний параметр цілі $P(V, H)$ для пари двох самохідних вогневих одиниць (бойових машинах) (наприклад відстань між ними ~ 3 км), СКВ помилки лінійного відхилення цілі $\sigma_\eta(V, H)$ і СКВ помилки щільності імовірності входу цілі у зону ЦР $\sigma_{Bx}(D, \sigma, \Delta, n, V, H)$.

$$\begin{aligned}P(V, H) &= 2 \cdot 10^3 + \sqrt{(8,7 \cdot 10^3 - 8V)^2 - H^2}, \\ \sigma_\eta(V, H) &= \left[\frac{2P(V, H)}{6} \right], \\ \sigma_{Bx}(D, \sigma, \Delta, n, V, H) &= [\sigma_p(D, \sigma, \Delta, n, V)^2 + \sigma_\eta(V, H)^2]^{0,5}. \quad (4)\end{aligned}$$

У підсумку значення ймовірностей входу цілей у зони ЦР знаходимо з виразу:

$$\Psi_{Bx}(D, \sigma, \Delta, n, V, H, P) = \int_{-P(V, H)}^{P(V, H)} \left\{ \frac{\exp - \left[\frac{(Z-P)^2}{2\sigma_{Bx}(D, \sigma, \Delta, n, V, H)^2} \right]}{\sqrt{2\pi} \sigma_{Bx}(D, \sigma, \Delta, n, V, H)} \right\} dZ, \quad (5)$$

де P – параметр повітряної цілі.

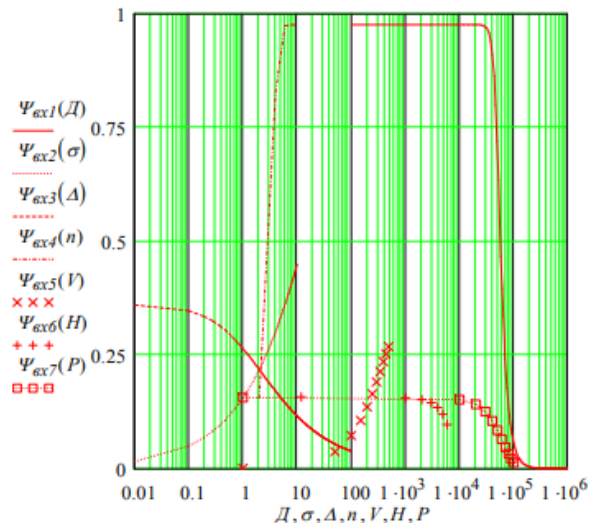


Рисунок 2 – Імовірності входу цілей в зони ЦР (ЗПу) $\Psi_{\text{вх}}(D, \sigma, \Delta, n, V, H, P)$

при зміні $D, \sigma, \Delta, n, V, H$ та P

Джерело: розроблено авторами

Результати розрахунку за виразами (3) – (5) приведені на рис. 2 для $D_{\text{БПО}}$ у 62,6 км. Перша крива $\Psi_{\text{вх}1}(D)$ (безперервна) побудована при $\sigma = 1 \text{ м}^2$, $\Delta = 0$, $n = 2$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$. Друга крива $\Psi_{\text{вх}2}(\sigma)$ (точки, $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\Delta = 0$, $n = 2$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$) відображає значення ймовірностей входу цілей у зону ЦР при зміні їх ЕПР σ . Низькі ймовірності входу, за другою кривою, пов'язані з не виявленням даних цілей РЛС старшого начальника. Вплив перешкод Δ і тривалість спостереження за ТЦ представлені відповідно третьою $\Psi_{\text{вх}3}(\Delta)$ (тире) та четвертою $\Psi_{\text{вх}4}(n)$ (точки і тире) кривими. Перешкоди Δ не дають можливостей своєчасно виявляти ТЦ, хоча при $n \geq 3$ якісно вимірюється РЛС параметр цілі. Третя крива здобута, якщо $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $n = 2$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$, а четверта – $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$. П'ята крива $\Psi_{\text{вх}5}(V)$ ($\times \times \times$), шоста $\Psi_{\text{вх}6}(H)$ ($+++$) та сьома $\Psi_{\text{вх}7}(P)$ ($\square \square \square$) криві показують зміну ймовірностей входу на $D_{\text{БПО}}$ залежно від V, H і P . Вхідні дані для $\Psi_{\text{вх}5}(V)$ ($\times \times \times$) $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $n = 2$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$, а для кривої шостої $\Psi_{\text{вх}6}(H)$ ($+++$) – $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $n = 2$, $V = 230 \text{ м/с}$, $P = 3 \cdot 10^3 \text{ м}$ та для сьомої $\Psi_{\text{вх}7}(P)$ ($\square \square \square$) – $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $n = 2$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$. З останніх трьох кривих слідує недостатні ймовірності входу ТЦ, що ускладнює проведення ЦР у підрозділі. Треба відмітити покращення результатів чисельного моделювання значень ймовірностей коли $D_{\text{ДПЗ}}$ дорівнює 41,9 км. Тобто при відпрацюванні цілевказівки (ЦВ) особовим складам (о/с) самохідної вогневої одиниці (бойової машини) імовірніші стрільба буде проведена. Так $\Psi_{\text{вх}}(62,6 \cdot 10^3; 1; 5; 2; 230; 10^3; 3 \cdot 10^3) \approx 0,16$ і $\Psi_{\text{вх}}(41,9 \cdot 10^3; 1; 5; 2; 230; 10^3; 3 \cdot 10^3) \approx 0,64$.

4. Імовірності не виходу цілей в ЗПу та ЗУ комплексу, після пуску ракет, при стрільбі по цілі, яка маневрує [1-4, 6-9].

Відношення с/ш у РЛ каналі станції супроводження цілей (ССЦ) самохідної вогневої одиниці (бойової машини) на дальній межі ЗПу (ДМЗПу) $q_c(D, \sigma, \Delta)$, СКВ помилки вимірювання азимуту цілі $\sigma_{\text{Бс}}(D, \sigma, \Delta)$ ССЦ та кількість луно – сигналів k_i по даній цілі на ДМЗПу дорівнює:

$$q_c(D, \sigma, \Delta) = \sqrt{(1,434 \cdot 10^{20} \sigma) / [D^4 (1 + \Delta)]},$$

$$\sigma_{\beta c}(D, \sigma, \Delta) = \frac{\sqrt{\pi} \Theta_c}{q_c(D, \sigma, \Delta) 180}, \quad k_i = \tau_k T^{-1}, \quad (6)$$

де Θ_c, τ_k – відповідно напівширина діаграми спрямованості (ДС) антени станції супроводження цілі (ССЦ) самохідної вогневої одиниці (бойової машини) (обрали $1,23^\circ$) та const контуру управління (прийняли $\sim 0,8$ с);
 T – період слідування радіоімпульсів ССЦ (взяли 390 мкс).

СКВ помилки виміру азимуту цілі, яка проводить односторонній коловий віраж у горизонтальній площині польоту без зміни V $\sigma_m(n_{\text{ц}}, V)$, СКВ помилки параметру цілі $\sigma_{\text{рм}}(D, \sigma, \Delta, n_{\text{ц}}, V)$, СКВ помилки щільності імовірності не виходу цілі з ЗПу (ЗУ) комплексу, а $P(V, H)$ і $\sigma_{\eta}(V, H)$ находимо з виразів (4), так:

$$\sigma_m(n_{\text{ц}}, V) = (\tau_k n_{\text{ц}} g) / (3V),$$

$$\sigma_{\text{рм}}(D, \sigma, \Delta, n_{\text{ц}}, V) = \frac{\sqrt{2} [\sigma_{\beta c}(D, \sigma, \Delta) + \sigma_m(n_{\text{ц}}, V)]}{(k_i - 1) V T} \cdot \left[D - \frac{(k_i - 1) V T}{2} \right]^2, \quad (7)$$

$$\sigma_{\text{вм}}(D, \sigma, \Delta, n_{\text{ц}}, V, H) = [\sigma_{\text{рм}}(D, \sigma, \Delta, n_{\text{ц}}, V)^2 + \sigma_{\eta}(V, H)^2]^{0,5},$$

де $n_{\text{ц}}$ – перевантаження ПЦ, з якими вона маневрує;
 g – прискорення вільного падіння ($\sim 9,81$ м/с²).

Для спрощення прийняли, що ДМЗПу комплексу $D \sim 15$ км. Безумовно бажано мати імовірності не виходу цілей з ЗПу (ЗУ), після пуску ракет, не менше 0,5, для отримання необхідної ефективності стрільби та УВ.

Значення ймовірностей не виходу цілей з ЗПу (ЗУ) комплексу після пуску ракети дорівнює:

$$\Psi_H(D, \sigma, \Delta, n_{\text{ц}}, V, H, P) =$$

$$= \int_{-P(V, H)}^{P(V, H)} \left\{ \frac{\exp \left[-\frac{(Z - P)^2}{2 \sigma_{\text{вм}}(D, \sigma, \Delta, n_{\text{ц}}, V, H)^2} \right]}{\sqrt{2} \pi \sigma_{\text{вм}}(D, \sigma, \Delta, n_{\text{ц}}, V, H)} \right\} dZ. \quad (8)$$

За аналогією з результати на рис. 2 отримали значення, які приведені на рис. 3. Перша $\Psi_{H1}(D)$ (безперервна), друга $\Psi_{H2}(\sigma)$ (точки), третя $\Psi_{H3}(\Delta)$ (тире) криві показують значення імовірності, яка досліджується при різних D , σ і Δ . В цілому хід вказаних кривих задовольняє якості стрільби ракетами. Вхідні данні для $\Psi_{H1}(D)$ наступні: $\sigma = 1$ м², $\Delta = 0$, $n_{\text{ц}} = 0$, $V = 230$ м/с, $H = 10^3$ м, $P = 3 \cdot 10^3$ м, а для кривої $\Psi_{H2}(\sigma)$ – $D = 15 \cdot 10^3$ м, $\Delta = 0$, $n_{\text{ц}} = 0$, $V = 230$ м/с, $H = 10^3$ м, $P = 3 \cdot 10^3$ м. Відповідно вхідні данні для $\Psi_{H3}(\Delta)$ і $\Psi_{H4}(n_{\text{ц}})$: $D = 15 \cdot 10^3$ м, $\sigma = 1$ м², $n_{\text{ц}} = 0$, $V = 230$ м/с, $H = 10^3$ м, $P = 3 \cdot 10^3$ м та $D = 15 \cdot 10^3$ м, $\sigma = 1$ м², $\Delta = 5$, $V = 230$ м/с, $H = 10^3$ м, $P = 3 \cdot 10^3$ м. Коли $n_{\text{ц}} \geq 1$ четверта крива $\Psi_{H4}(n_{\text{ц}})$ (точки і тире), п'ята $\Psi_{H5}(V)$ ($\times \cdot \times \cdot$), шоста $\Psi_{H6}(H)$ ($\square \cdot \square \cdot$) та сьома $\Psi_{H7}(P)$ ($\diamond \cdot \diamond \cdot$) криві надали малі значення не виходу цілі, при її маневруванні. Вхідні данні для $\Psi_{H5}(V)$: $D = 15 \cdot 10^3$ м, $\sigma = 1$ м², $\Delta = 5$, $n_{\text{ц}} = 3$, $H = 10^3$ м, $P = 3 \cdot 10^3$ м, та для $\Psi_{H6}(H)$ – $D = 15 \cdot 10^3$ м, $\sigma = 1$ м², $\Delta = 5$, $n_{\text{ц}} = 3$, $V = 230$ м/с, $P = 3 \cdot 10^3$ м і для $\Psi_{H7}(P)$ – $D = 15 \cdot 10^3$ м, $\sigma = 1$ м², $\Delta = 5$, $n_{\text{ц}} = 3$, V

$= 230$ м/с, $H = 10^3$ м. Останнє вкрай негативно буде проявлятися при застосуванні озброєння. Треба відмітити, що на ДМЗПу комплексу $\Psi_H(15 \cdot 10^3; 1; 5; 3; 400; 10^3; 3 \cdot 10^3) \approx 0,27$, хоча на ДМЗУ – $\Psi_H(10^4; 1; 5; 3; 400; 10^3; 3 \cdot 10^3) \approx 0,56$.

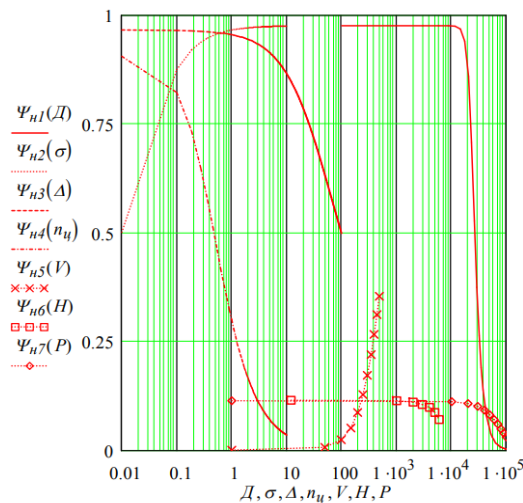


Рисунок 3 – Імовірності не виходу цілей з ЗПу (ЗУ) комплексу $\Psi_H(D, \sigma, \Delta, n_u, V, H, P)$ у різних умовах застосування

Джерело: розроблено авторами

5. Визначення першого роду помилок стрільби ракетами, а саме імовірності проходження ракети у “трубці” радіусу ρ [1 – 5, 10 – 13].

Розрахунок значень систематичної складової помилок наведення ракет (ПНР) $m_H(n_u)$ та СКВ ПНР $\sigma_H(\Delta)$ залежно від точки зустрічі ракети з ціллю (ТЗРЦ) у ЗУ комплексу.

Перший вираз в (9) показує зростання систематичної складової ПНР при маневруванні цілі, коли $v_H(n_u, t) \geq 0$. Другий вираз $t_1(n_u)$ вказує на час коли $v_H(n_u, t) = 0$, а третій вираз $m_c(n_u)$ – середнє значення систематичної складової ПНР.

$$v_H(n_u, t) \approx \begin{cases} 0,5n_u g \left\{ t^2 - \left[\frac{n_p}{n_u} (t - \tau_K)^2 \right] \right\}, & t \geq \tau_K, \\ 0,5n_u g t^2, & t < \tau_K, \end{cases}$$

$$t_1(n_u) = \tau_K \left(1 - \frac{n_p}{n_u} \right)^{-1},$$

$$m_c(n_u) = \frac{1}{t_1(n_u)} \int_0^{t_1(n_u)} v_H(n_u, t) dt,$$

$$m_H(n_u) = \{ (0,87r_\partial 10^{-4})^2 + [0,87r_\partial 10^{-4} + m_c(n_u)]^2 \}^{0,5}. \quad (9)$$

де n_p, t – відповідно перевантаження ракети у ТЗРЦ та час від початку маневру цілі до ТЗРЦ;
 $m_c(n_u)$ – усереднене значення систематичної складової ПНР при маневруванні цілі;
 r_∂ – похила дальність до ДМЗУ комплексу (прийняли 10^4 м).

За виразами (9) отримали: $m_c(3) \approx 5,7$ м, $m_c(5) \approx 12,4$ м та $m_H(3) \approx 6,6$ м, $m_H(5) \approx 13,3$ м, хоча без маневру – $m_H(0) \approx 1,2$ м. Значення $m_H(5)$ у ~ 13 м сумірні з відстанню де стійко спрацьовує радіопідричник (РП) ракети.

Вважають, що при дії АШП зростає лише флуктаційна складова ПНР $\sigma_{\Phi Z}(\Delta)$ [1, 3] та СКВ

ПНР находимо залежно від дальності до ТЗРЦ, так:

$$\begin{aligned}\sigma_{\phi z}(\Delta) &= \sigma_{\phi z} 10^{\Delta/20}, \\ \sigma_H(\Delta) &= \sqrt{\sigma_{dz}^2 + \sigma_{iz}^2 + \sigma_{\phi z}^2(\Delta)}, \\ \sigma_H(\Delta) &= r_d \operatorname{tg} \left\{ [\sigma_H(\Delta) \pi] / (180 \cdot 60) \right\},\end{aligned}\quad (10)$$

де $\sigma_{dz}, \sigma_{iz}, \sigma_{\phi z}$ – відповідно динамічна, інструментальна та флуктуаційна складові ПНР (прийняли усереднені значення $\sigma_{dz} \approx 1,9$ кутових хвилин (кут. хв.), $\sigma_{iz} \approx 0,4$ кут. хв., $\sigma_{\phi z} \approx 1,3$ кут. хв.), причому завжди $\sigma_H(\Delta) \geq 3$ м.

За виразами (10) маємо: $\sigma_H(0) \approx 6,8$ м і $\sigma_H(5) \approx 8,8$ м. Результати розрахунку систематичної складової ПНР $m_H(n_u)$ та СКВ ПНР $\sigma_H(\Delta)$ приведені на рис. 4. Перша крива залежно $m_H(n_u)$ (безперервна) побудована, якщо перевантаження цілі n_u змінюються до $10g$. Друга крива $\sigma_H(\Delta)$ (точки) отримана при практично відсутності АШП та її наявності до рівня щільності переважної перешкоди ($\Delta = 10^2$ разів).

Відмітимо суттєве зростання складових ПНР при протидії стрільбі у вигляді маневрування цілі та дії перешкод. Вказане приводить до зниження ефективності бойового застосування комплексу.

Імовірності проходження ракети у "трубці" радіусу ρ $P(\rho, \Delta, n_u)$ дорівнює:

$$\begin{aligned}P(\rho, \Delta, n_u) &= \\ &= \int_0^\rho \left\{ \frac{\rho \exp \left\{ -\frac{\rho^2 + m_H(n_u)^2}{2\sigma_H^2(\Delta)} \right\} I_0 \left[\frac{\rho^2 m_H(n_u)}{\sigma_H^2(\Delta)} \right]}{\sigma_H^2(\Delta)} \right\} d\rho.\end{aligned}\quad (11)$$

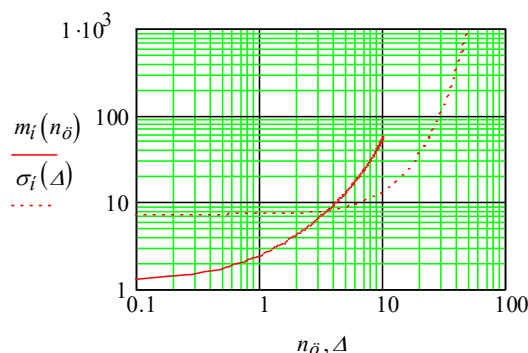


Рисунок 4 – Систематичної складової ПНР $m_H(n_u)$ та СКВ ПНР $\sigma_H(\Delta)$ залежно від перевантажень цілі n_u та рівня перешкод Δ

Джерело: розроблено авторами

Результати обчислень наведені на рис. 5. Перша крива $P(\rho, 0, 0)$ (безперервна) побудована при роботі по ТЦ і відсутності маневру цілі та перешкод.

Друга крива $P(14, \Delta, 0)$ (точки) та третя $P(14, 5, n_u)$ (тире) відповідно розраховані для випадків дії АШП та маневрування ТЦ на фоні перешкод середньої щільності ($\Delta = 5$ разів).

Вплив АШП та маневрування цілі знижує імовірності проходження ракет у "трубці" радіусу стійкого спрацювання РЗ ($\rho = 14$ м), отримали: $P(14; 0; 0) \approx 0,9$ та $P(14; 5; 0) \approx 0,7$ і $P(14; 5; 3) \approx 0,6$.

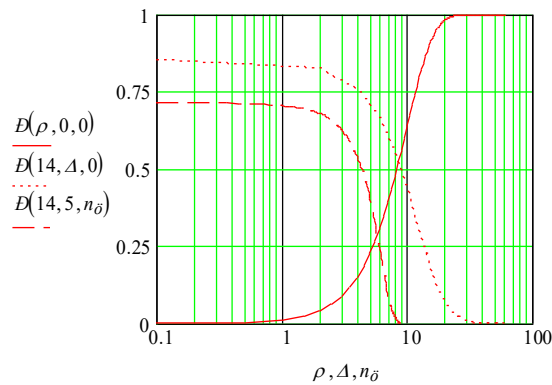


Рисунок 5 – Імовірності проходження ракети у “трубці” радіусу ρ $P(\rho, \Delta, n_\delta)$ залежно від промаху ракети ρ , рівня перешкод Δ та перевантажень цілі n_δ

Джерело: розроблено авторами

6. Визначення другого роду помилок стрільби ракетами, а саме імовірності спрацювання РП (системи підриву БЧ ракети) [1-3, 6-13].

Вводимо апроксимацію ширини ДС приймальної антени РП $\theta(\rho)$ [2, 9, 10] та знаходимо СКВ помилок РП ракети $\sigma_p(\rho)$ і математичне сподівання (МС) випадкової величини радіусу спрацювання РП ракети $m_p(\sigma)$.

На основі аналізу скалярного поля дифракції Френеля – Кірхгофа отримали наступне:

$$\begin{aligned} \theta(\rho) &= 0,5 \left\langle 0,0074 + 0,611 \left\{ 1 - e^{-[1,33 \sin(\varepsilon_a)/\rho]} \right\} \right\rangle, \\ \sigma_p(\rho) &= \frac{\rho \sin[\theta(\rho)]}{3 \sin(\varepsilon_a)} \left\{ \frac{1}{\sin[2,531 - \theta(\rho)]} + \frac{1}{\sin[0,611 - \theta(\rho)]} \right\}, \\ m_p(\sigma) &= \begin{cases} \rho_{\max} \sqrt[4]{\sigma/\sigma_{\text{ТЦ}}}, & \sigma \geq 0,1 \text{ м}^2, \\ \sqrt[3]{\frac{\rho_{\max}^4 \sigma \lambda}{\sigma_{\text{ТЦ}} L^2 \sin(\varepsilon_a + 3 \sigma_{\varepsilon a})}}, & \sigma < 0,1 \text{ м}^2, \end{cases} \end{aligned} \quad (12)$$

- де ε_a – кут нахилу приймальної антени РП ракети (прийняли $\sim 1,05$ рад.);
 $\rho_{\max}$ – найбільший промах ракети коли РП спрацьовує з імовірністю 0,5 при роботі по ТЦ ($\rho \sim 15,5$ м);
 λ, L – довжина хвилі РП ракети ($\sim 0,03$ м) та довжина її приймальної антени ($\sim 0,6$ м) відповідно;
 $\sigma_{\varepsilon a}$ – СКВ помилки спрацювання РП ракети ($\sim 0,062$ рад.).

Результати числового моделювання наведені на рис. 6. Перша крива $\sigma_p(\rho)$ (безперервна) побудована при роботі по ТЦ. Друга крива $m_p(\sigma)$ (точки) вказує на лінійне зростання МС випадкової величини радіусу спрацювання РП, при збільшенні ЕПР цілі, по якій здійснюється обстріл.

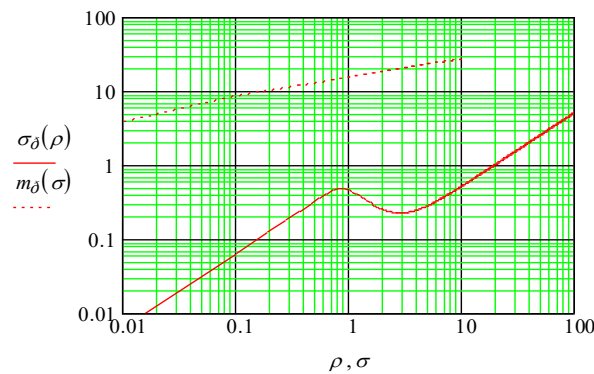


Рисунок 6 – Середнє квадратичне відхилення помилок радіопідричника ракети $\sigma_p(\rho)$ та математичного сподівання випадкової величини радіусу спрацювання радіопідричника ракети $m_p(\sigma)$ залежно від промаху ракети ρ та ефективної поверхні розсіювання цілі σ

Джерело: розроблено авторами

Одержали $m_p(1) = 15,5$ м та $m_p(10^{-2}) = 3,9$ м.

Імовірності спрацювання РП $P_{сп}(\rho, \sigma, k)$ – другий рід помилок стрільби ракетами.

$$P_{сп}(\rho, \sigma, k) = 1 - \text{snorm} \left[\frac{\rho - m_p(\sigma)}{k \sigma_p(\rho)} \right], \quad (13)$$

де $\text{snorm}[Z]$ – функція розподілу нормального та центрованого нормального розподілення у середовищі MathCAD;

k – рівень перешкод по РЛ каналу РП ракети (без перешкод $k = 1$, перешкоди слабкої щільності $k = 2$ рази, середньої – $k = 5$ разів, сильної – $k = 16$ разів та щільності перешкоди, що подавляє – $k = 10^2$ разів).

Підсумки розрахунків за виразами (12), (13) приведені на рис. 7. Перша крива $P_{сп}(\rho, 10^{-2}, 1)$ (безперервна) та друга крива $P_{сп}(\rho, 10^{-2}, 10^2)$ (точки) розраховані при обстрілі малорозмірної цілі ($\sigma = 10^{-2} \text{ м}^2$) при відсутності та наявності АШП щільності перешкоди, що подавляє по РЛ каналу РП ракети відповідно.

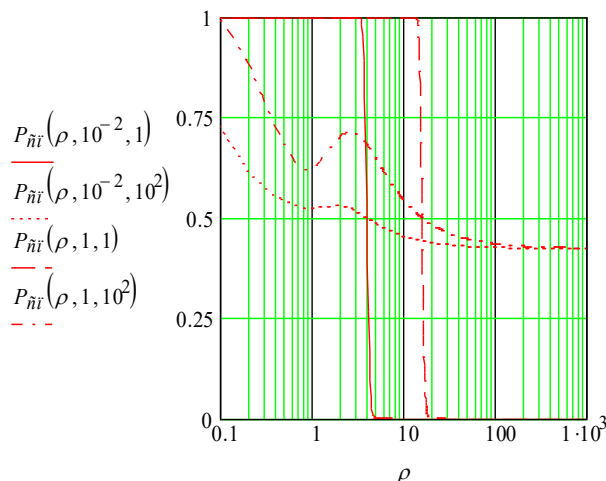


Рисунок 7 – Імовірності спрацювання радіопідричника ракети $P_{сп}(\rho, \sigma, k)$ залежно від промаху ракети ρ

Джерело: розроблено авторами

Третя крива $P_{сп}(\rho, 1, 1)$ (тире) та четверта крива $P_{сп}(\rho, 1, 10^2)$ (точки і тире) отримані для тих же самих умов, що і попередні, але при роботі по ТЦ ($\sigma_{ТЦ} = 1 \text{ м}^2$). Одержали $P_{сп}(15,5; 1; 0) =$

0,5 та надвеликі відстані спрацювання РП, коли цілі не будуть уражені вузьким потоком осколків бойової частини ракети. Так при АШП сильної щільності $P_{сп}(40; 1; 16) \approx 0,23$ та $P_{сп}(10^2; 1; 10^2) \approx 0,44$. Дане підтверджує необхідність забезпечення необхідної завадостійкості РЛ каналу радіопідривника ракети.

7. Розрахунок колового закону ураження ТЦ та умовних ймовірностей ураження різних цілей при стрільбі двома ракетами [1-3, 9, 12, 13].

Значення колового закону ураження ТЦ $G(\rho)$ та умовні імовірності ураження різних цілей при стрільбі двома ракетами $R_2(\rho, D, \sigma, \Delta, n_{ц}, V, H, P, k)$ у різноманітних умовах бойового застосування визначаємо з наступних виразів:

$$\begin{aligned} G(\rho) &= \exp(-\rho^2 / \beta_0^2), \\ R_2(\rho, D, \sigma, \Delta, n_{ц}, V, H, P, k) &= \\ &= \Psi_H(D, \sigma, \Delta, n_{ц}, V, H, P) \cdot \\ &\cdot \left\{ 1 - [1 - P(\rho, \Delta, n_{ц}) P_{сп}(\rho, \sigma, k)]^2 \right\}, \end{aligned} \quad (14)$$

де β_0 – параметр колового закону ураження ТЦ з врахуванням механічної, запалювальної та ініційованої дії осколків БЧ ракети (прийняли ~ 21 м).

За першим виразом (14) отримали при середньому промаху ракети $G(6) \approx 0,92$ та з СКВ промаху ракети $G(9) \approx 0,83$. При підриві БЧ ракети під впливом АШП ураження ТЦ не можливо – $G(50) \approx 3,4 \cdot 10^{-3}$. Зміна значень $G(\rho)$ показана першою, безперервною кривою на рис. 8.

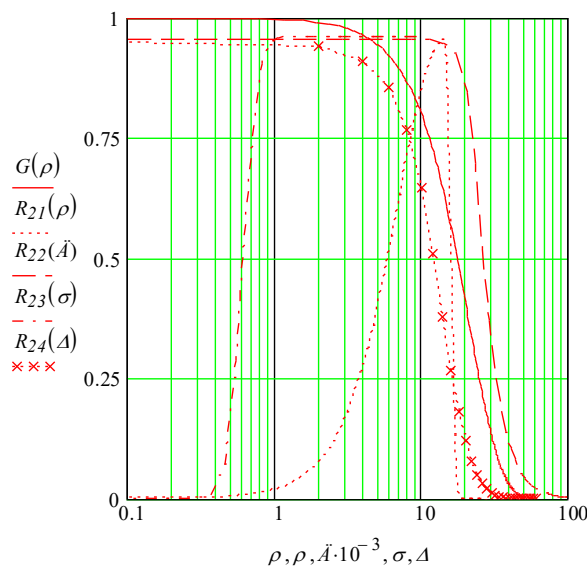


Рисунок 8 – Коловий закону ураження типової цілі $G(\rho)$ та умовні імовірності ураження цілей R_{2ij} при стрільбі двома ракетами
Джерело: розроблено авторами

Друга крива $R_{21}(\rho)$ (точки) та третя крива $R_{22}(\Delta)$ (тире) відображають значення умовних ймовірностей ураження цілей при зміні ρ та Δ відповідно. Причому $R_{21}(14)$ дорівнює на ДМЗУ комплексу $R_2(14; 10^4; 1; 0; 0; 230; 10^3; 3 \cdot 10^3; 1) \approx 0,96$, коли імовірність входу цілі на ДБПО (позначимо через $\Psi_{вх БПО}$) лише $\sim 0,36$ і імовірності вірного виявлення РЛС старшого начальника (позначимо через $P_{в БПО}$) $\sim 0,54$. На ДДПЗ результати кращі – $\Psi_{вх ДПЗ} \sim 0,89$ і $P_{в ДПЗ} \sim 0,87$. Значення для третьої кривої $\Psi_{вх БПО}$, $P_{в БПО}$, $\Psi_{вх ДПЗ}$ та $P_{в ДПЗ}$ ті самі, що і для другої кривої. Для кращої візуалізації результатів моделювання величина Δ , за віссю абсцис, зменшена у 10^3 .

разів. Четверта крива $R_{24}(\sigma)$ (точки і тире) та п'ята $R_{25}(\Delta)$ ($\cdot \times \cdot$) показують значення умовних ймовірностей ураження цілей при зміні σ і Δ відповідно. Розрахунки надали на ДМЗУ $R_2(14;10^4;0,5;0;0;230;10^3;3 \cdot 10^3;1) \approx 0,15$, при $\Psi_{\text{вх БПО}} \sim 0,26$ і $P_{\text{в БПО}} \sim 0,34$, або малорозмірна ціль може і не вийти на $D_{\text{БПО}}$, не буде охоплена ЦР. На $D_{\text{ДПЗ}}$ маємо $\Psi_{\text{вх БПО}} \sim 0,82$ і $P_{\text{в БПО}} \sim 0,77$. При роботі по ТЦ на рівні АСП середньої щільності отримали $R_2(14;10^4;0,5;0;0;230;10^3;3 \cdot 10^3;1) \approx 0,89$, коли $\Psi_{\text{вх БПО}}$ лише $\sim 0,16$ і $P_{\text{в БПО}} \sim 0,11$. Тобто ЦЦР у підрозділі не реалізується, залишається ДЦР, так як недостатня $P_{\text{в БПО}}$ РЛС старшого начальника.

Вплив маневру ТЦ показано кривою $R_{25}(n_u)$ (тире) на рис. 9.

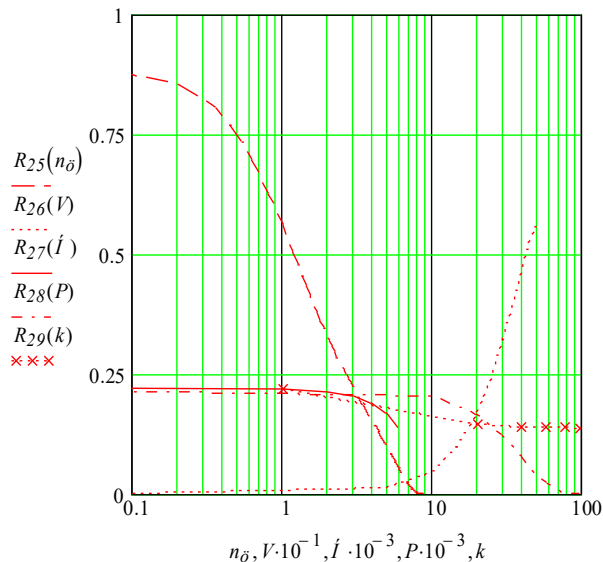


Рисунок 9 – Умовні ймовірності ураження цілей R_{2ij} при стрільбі ракетами у різних умовах застосування

Джерело: розроблено авторами

Перевантаження цілі у $n_u = 3$ надали $R_2(14;10^4;1;5;3;230;10^3;3 \cdot 10^3;1) \approx 0,22$, коли $\Psi_{\text{вх БПО}} \sim 0,16$ і $P_{\text{в БПО}} \sim 0,11$. При цьому знижується, від попереднього, ймовірність не виходу ТЦ з ЗУ комплексу (позначимо через $\Psi_{\text{нзу}}$) з $\sim 0,97$ до $\sim 0,26$. Тобто ТЦ в змозі покинути ЗУ комплексу. Друга крива $R_{26}(V)$ (точки) та третя $R_{27}(H)$ (безперервна) надають значення умовних ймовірностей ураження цілей при зміні V та H відповідно. Для кращої візуалізації розрахунків на рис. 9 значення V , за віссю абсцис, зменшена у 10 разів, а величини H і P зменшили у 10^3 разів. За другою кривою збільшення V до 400 м/с приводе до підвищення $\Psi_{\text{вх БПО}}$ з $\sim 0,16$ до $\sim 0,24$, а також поліпшується $\Psi_{\text{нзу}}$ з $\sim 0,26$ до $\sim 0,56$. При цьому покращуються умовні ймовірності ураження з $\sim 0,22$ до $\sim 0,48$, так $R_2(14;10^4;1;5;3;400;10^3;3 \cdot 10^3;1) = 0,476$. Останнє пояснюється зменшенням часу на входження цілі на $D_{\text{БПО}}$ і можливим не виходом з ЗУ комплексу. При підвищенні H до 5 км отримали зниження ефективності ЦР і стрільби двома ракетами – $R_2(14;10^4;1;5;3;230;5 \cdot 10^3;3 \cdot 10^3;1) \approx 0,17$, при $\Psi_{\text{вх БПО}} \sim 0,12$, $P_{\text{в БПО}} \sim 0,11$ та $\Psi_{\text{нзу}}$ лише $\sim 0,2$. Четверта крива $R_{28}(P)$ (точки і тире) та п'ята крива $R_{29}(k)$ ($\cdot \times \cdot$) приведені для різних P та k . Наприклад коли $P \sim 2 \cdot 10^4$ м то умовна ймовірність ураження дорівнює $R_2(14;10^4;1;5;3;230;10^3;2 \cdot 10^4;1) \approx 0,17$ і $\Psi_{\text{вх БПО}} \sim 0,14$ та $\Psi_{\text{нзу}} \sim 0,2$. Залишається можливість стрільби по цілям, які раптово з'являються і ДЦР у підрозділі. Перешкоди середньої щільності по РЛ каналу РП ракети знижують умовні ймовірності ураження (п'ята крива) до $R_2(14;10^4;1;5;3;230;10^3;3 \cdot 10^3;5) \approx 0,17$. При цьому $\Psi_{\text{вх БПО}}$, $P_{\text{в БПО}}$ та $\Psi_{\text{нзу}}$ такі самі, що і для випадку першої крива на рис. 9.

Отримані показники ефективності стрільби і УВ у різноманітних умовах з врахуванням

значень ймовірностей входу цілей у зону ЦР. Показані межі застосування ЦЦР у підрозділі, та обмеження, які зв'язані, з величинами ймовірностей вірного виявлення РЛС старшого начальника. Показано необхідність поліпшення енергетичного потенціалу РЛС та підвищення її перешкодостійкості [8, 12, 13]. Оптимізація системи УВ, впровадження мульті радарних систем виявлення та шумові радары [14-19] покращать показники ефективності стрільби ракетами.

Висновки

Таким чином, на основі існуючих технічних характеристик системи УВ знайдені рубежі постановки вогневих завдань і межі повітряної обстановки. Проведено порівняння рубежів та меж з відповідними ймовірностями вірного виявлення РЛС старшого начальника. Визначенні умови при яких вони відповідають вимогам до ЦР. Здобуті значення умовних ймовірностей ураження різних цілей з означеними величинами ймовірностей входу цілей в зони ЦР. Останнє не є достатнім, що може привести до хибного ЦР у підрозділі. Враховані імовірності не виходу цілей з зон пуску та ураження комплексу при маневруванні цілей. Означені межі впровадження ЦЦР і ДЦР у підрозділі. В цілому приведена залежність величин умовних ймовірностей ураження цілей від дев'яти основних параметрів, які описують стрільбу ракетами та УВ. Отримані практичні результати часткової моделі необхідні для ефективного застосування озброєння за призначенням.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Основы стрельбы и управления огнем войсковых зенитных ракетных комплексов. Часть 1. Казачинский В.З., Каипецкий А.А., Нестеренко Л.Г., Семенов Г.В., Солодовников Н.Д. – К.: КВАИУ, 1971. – 468с.
2. Основы стрільби та керування вогнем: навч. посіб. /В.Є. Кудряшов, С.Г. Леушин, В.І. Самоквіт. – Х. : ХУПС, 2016. – 232 с.
3. Пушкорис В. П. Управление огнем войск ПВО Сухопутных войск: Учебник. – К.:ВА ПВО СВ, 1989. – 556 с.
4. A private model for determining the efficiency of target distribution / М.С. Пискунов., В.Є. Кудряшов, В.Є., Філіппенков О.В. // Системи озброєння і військова техніка. – Х.: ХНУПС, 2021. – Вип. 1 (65) – С. 107 – 113.
5. Довідник з протиповітряної оборони. Торопчин А.Я., Романенко І.О., Даник Ю.Г., Пашенко Р.Е. та ін. – К.: МО України, Х.: 2003. – 368 с.
6. Модель протиповітряного бою як елемент системи управління вогнем підрозділами військ ППО Сухопутних військ/ О. В. Коломійцев, В. Є. Кудряшов, В.В. Машталір, П. В. Опенько, Р. М. Олійник // Збірник наукових праць ДНДІ ВС озброєння та військової техніки. – Чернівці: ДНДІ ВС ОБТ. – 2019. – Вип. № 1(1). – С. 94-101.
7. Теория и техника обработки радиолокационной информации на фоне помех / Ширман Я.Д., Манжос В.Н. – М.; Радио и связь, 1981. – 416с.
8. Радиоэлектронные системы: Основы построения и теория. Справочник. Изд. 2 – е, перераб. и доп. / Под. ред. Я. Д. Ширмана. – М.: Радиотехника, 2007. 512с.
9. Справочник по радиолокации/ под общей ред. К.Н. Трофимова. Том 1. Основы радиолокации. Под ред. Я.С. Ицхоки: – М.: Сов. радио, 1976. – 456 с.

10. Другий рід помилок стрільби ракетами по нетиповим цілям ЗРК малої дальності / О.В. Коломійцев, В.Є. Кудряшов, І.Я. Загоруйко, С.С. Ворошилов // Збірник наукових праць ХУ ПС. – Х.: ХУ ПС. – 2011.- Вип. 1(27) – С. 86 – 90.
11. Умовна імовірність ураження нетипової цілі ЗРК малої дальності / О.В. Коломійцев, В.Є. Кудряшов, І.Я. Загоруйко, С.С. Ворошилов // Збірник наукових праць ХУ ПС. – Х.: ХУ ПС. – 2012.- Вип. 2(30) – С. 170 – 174.
12. Кудряшов В.Є., Литовченко Д.М. Чисельне моделювання з основ стрільби ракетами та управління вогнем комплексів малої дальності: навч. посіб. Х. : ХНУПС, 2023. – 533 с.
13. Литовченко Д.М., Кудряшов В.Є. Чисельне моделювання з основ стрільби озброєння ближньої дії та інформаційного забезпечення військ: навч. посіб. Х. : ХНУПС, 2025. – 268 с.
14. Піскунов С.М. Перспективна структура системи управління силами і засобами протиповітряної оборони Сухопутних військ Збірник наукових праць ХУПС. – Х. : ХУПС, 2013. – Вип. 2(35) –С. 6-10.
15. Shevchenko, A.F., (2014) A comparative analysis of directional properties of phased ring arrays to be used in multi-static active/passive radars, Data processing systems, 9(125), pp.65-72, (in Ukrainian).
16. Kudriashov V.V., A Modified Maximum Likelihood Method for Estimation of Mutual Delay and Power of Noise Signals by Bistatic Radiometer, Comptes Rendus – L'Académie Bulgare des Sciences, 68(5), pp. 631-640.
17. Модель застосування мобільних комплексів/ О.С. Балабұха, К.Ю. Дергачов К.Ю., В.Ф. Слободенюк // Збірник наукових праць ЦНДІНУ. – К. ЦНДІНУ. – 2007. – Вип. 2. – С. 31 – 33.
18. Lukin, K. A. "Millimeter wave noise radar applications: theory and experiment", Fourth International Kharkov Symposium 'Physics and Engineering of Millimeter and Sub-Millimeter Waves'. Symposium Proceedings (Cat. No.01EX429), Kharkov, Ukraine, 2001, pp. 68-73, doi: 10.1109/MSMW.2001.946748.
19. Savci, K., Stove, A.G., De Palo, F., Erdogan, A.Y., Galati, G., Lukin, K.A., Lukin, S. Noise radar—overview and recent developments IEEE Aerospace and Electronic Systems Magazine, 2020, Vol.35 (9), pp.8-20.

References

1. Osnovy strel'by i upravleniya ognem voyskovykh zenitnykh raketnykh kompleksov. Chast' 1. Kazachinskiy V. Z., Kaipetskiy A. A., Nesterenko L. G., Semenov G. V., Solodovnikov N. D. – Kyiv: KVAIU, 1971. – 468s.
2. Osnovy stril'by ta keruvannya vohnem: navch. posib. /V.YE. Kudryashov, S.H. Leushyn, V.I. Samokvit. – Kharkov : KHUPS, 2016. – 232 s.
3. Pushkoris V. P. Upravleniye ognem voysk PVO Sukhoputnykh voysk: Uchebnik. – Kyiv:VA PVO SV, 1989. – 556 s.
4. A private model for determining the efficiency of target distribution / M.S. Piskunov., V.YE. Kudryashov, V.YE., Filippenkov O.V. // Systemy ozbroynnya i viys'kova tekhnika. – Kharkov: KHNUPS, 2021. – Vyp. 1 (65) – S. 107 – 113.
5. Dovidnyk z protypovitryanoyi oborony. Toropchyn A.YA., Romanenko I.O., Danyk YU.H., Pashchenko R.E. ta in. – Kyiv: MO Ukrainy, KH.: 2003. – 368 s.
6. Model' protypovitryanoho boyu yak element systemy upravlinnya vohnem pidrozdilamy viys'k PPO Sukhoputnykh viys'k/ O. V. Kolomiytsev, V. YE. Kudryashov, V.V. Mashtalir, P. V. Open'ko, R. M. Oliynyk // Zbirnyk naukovykh prats' DNDI VS ozbroynnya ta viys'kovoyi tekhniky. – Chernihiv: DNDI VS OVT. – 2019. – Vyp. № 1(1). – S. 94-101.
7. Teoriya i tekhnika obrabotki radiolokatsionnoy informatsii na fone pomekh / Shirman YA.D., Manzhos V.N. – Moscow; Radio i svyaz', 1981. – 416 s.

8. Radioelektronnyye sistemy: Osnovy postroyeniya i teoriya. Spravochnik. Izd. 2 – ye, pererab. i dop. / Pod. red. YA. D. Shirmana. – Moscow: Radiotekhnika, 2007. 512s.
9. Spravochnik po radiolokatsii/ pod obshchey red. K.N. Trofimova. Tom 1. Osnovy radiolokatsii. Pod red. YA.S. Itskhoki: – Moscow: Sov. radio, 1976. – 456 s.
10. Druhyy rid pomyl'ok stril'by raketamy po netypovym tsilyam ZRK maloyi dal'nosti / O.V. Kolomiytsev, V.YE. Kudryashov, I.YA. Zahoruyko, S.S. Voroshylov // Zbirnyk naukovykh pratsi KHU PS. – Kharkov: KHU PS. – 2011.- Vyp. 1(27) – S. 86 – 90.
11. Umovna imovirnist' urazhennya netypovoyi tsili ZRK maloyi dal'nosti / O.V. Kolomiytsev, V YE. Kudryashov, I.YA. Zahoruyko, S.S. Voroshylov // Zbirnyk naukovykh pratsi KHU PS. – Kharkov: KHU PS. – 2012.- Vyp. 2(30) – S. 170 – 174.
12. Kudryashov V.YE., Lytovchenko D.M. Chysel'ne modelyuvannya z osnov stril'by raketamy ta upravlinnya vohnem kompleksiv maloyi dal'nosti: navch. posib. Kharkov : KHNUPS, 2023. – 533.
13. Lytovchenko D.M., Kudryashov V.YE. Chysel'ne modelyuvannya z osnov stril'by ozbroynennya blyzhn'oyi diyi ta informatsiynoho zabezpechennya viys'k: navch. posib. Kharkov : KHNUPS, 2025. – 268 s.
14. Piskunov S. M. Perspektyvna struktura systemy upravlinnya sylamy i zasobamy protypovitryanoyi oborony Sukhoputnykh viys'k Zbirnyk naukovykh prats' KHUPS. – Kharkov : KHUPS, 2013. – Vyp. 2(35) –S. 6-10.
15. Shevchenko, A.F., (2014). A comparative analysis of directional properties of phased ring arrays to be used in multi-static active/passive radars, Data processing systems, 9(125), pp.65-72, (in Ukrainian).
16. Kudriashov V.V., A Modified Maximum Likelihood Method for Estimation of Mutual Delay and Power of Noise Signals by Bistatic Radiometer, Comptes Rendus – L'Académie Bulgare des Sciences, 68(5), pp. 631-640.
17. Model' zastosuvannya mobil'nykh kompleksiv/ O.S. Balabukha, K.YU. Derhachov K.YU., V.F. Slobodenyuk// Zbirnyk naukovykh prats' TSNDINU. – Kyiv. TSNDINU. – 2007. – Vyp. 2. – S. 31 – 33.
18. Lukin, K. A. "Millimeter wave noise radar applications: theory and experiment", Fourth International Kharkov Symposium 'Physics and Engineering of Millimeter and Sub-Millimeter Waves'. Symposium Proceedings (Cat. No.01EX429), Kharkov, Ukraine, 2001, pp. 68-73, <https://doi.org/10.1109/MSMW.2001.946748>.
19. Savci, K., Stove, A.G., De Palo, F., Erdogan, A.Y., Galati, G., Lukin, K.A., Lukin, S. Noise radar—overview and recent developments IEEE Aerospace and Electronic Systems Magazine, 2020, Vol.35 (9), pp.8-20.

Формування нормативної моделі життєвого циклу військових наземних роботизованих комплексів

Forming a Regulatory Model of the Life Cycle for Military Ground Robotic Systems

Андрій Дядечко ^A

Corresponding author: доктор філософії, начальник науково-дослідного відділу проблем супроводження експлуатації інформаційних систем, e-mail: andrewvvs@gmail.com, ORCID: 0000-0003-0191-8326

Andrii Diadechko ^A

Corresponding author: PhD, Head of the Research Department on Information Systems Support and Operation Issues, e-mail: andrewvvs@gmail.com, ORCID: 0000-0003-0191-8326

Віталій Зуйко ^A

кандидат технічних наук, доцент, доцент кафедри геопросторової підтримки та застосування космічних систем, e-mail: vitalikzu@ukr.net, ORCID: 0000-0003-1439-9502

Vitalii Zuiko ^A

Candidate of Technical Science, Associate Professor, Associate Professor of the Geospatial Support and Space Systems Application Department, e-mail: vitalikzu@ukr.net, ORCID: 0000-0003-1439-9502

^A Національний університет оборони України, м. Київ, Україна

^A National Defence University of Ukraine, Kyiv, Ukraine

Received: August 15, 2025 | Revised: August 21, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.9>

Мета роботи. Обґрунтування підходів до формування нормативної моделі життєвого циклу військових наземних роботизованих комплексів з урахуванням їхніх технологічних і функціональних особливостей, а також аналіз обмежень чинних нормативних документів щодо систем керування життєвим циклом озброєння та військової техніки.

Метод дослідження. Застосовано системний аналіз нормативної бази у сфері озброєння та військової техніки, а також порівняльний аналіз загальноприйнятих моделей життєвого циклу.

Результати дослідження. Розроблено адаптовану нормативну модель життєвого циклу військових наземних роботизованих комплексів, яка враховує необхідність гнучкої інтеграції швидких циклів модернізації, особливості управління конфігурацією, забезпечення підтримки програмного забезпечення та експлуатацію в умовах динамічних тактичних змін.

Теоретична цінність дослідження. Дослідження розширює теоретичну базу щодо нормативного регулювання життєвого циклу перспективних видів озброєння та військової техніки та сприяє подальшій розробці національних стандартів з урахуванням нових класів бойових систем.

Практична цінність дослідження. Запропонована модель може бути використана під час розроблення технічних завдань, програм випробувань, документів супроводження життєвого циклу та нормативних актів, що регулюють поставлення на озброєння та логістичне забезпечення військових наземних роботизованих комплексів.

Оригінальність дослідження. Полягає у поєднанні традиційного нормативного підходу з концепціями гнучкого управління життєвим циклом для кіберфізичних систем, а також у структурному розділенні життєвого циклу на апаратну й програмну підсистеми в межах однієї моделі.

Тип статті. Аналітично-дослідницька стаття.

Purpose. To substantiate approaches to the development of a regulatory life cycle model for military ground robotic systems, taking into account their technological and functional specificities, as well as to analyze the limitations of current regulatory documents on life cycle management of weapons and military equipment.

Method. The study applies a systems analysis of national regulatory standards in the field of weapons and military equipment, along with a comparative analysis of commonly used life cycle models.

Findings. An adapted regulatory life cycle model for military ground robotic systems is developed. The model accounts for the need for rapid modernization cycles, configuration management features, software support, and operation under dynamic tactical conditions.

Theoretical implications. The research expands the theoretical framework for regulatory control of the life cycle of advanced military systems and contributes to the development of national standards tailored to new classes of combat platforms.

Practical implications. The proposed model can be used in the development of technical requirements, testing programs, life cycle documentation, and regulatory acts governing the adoption and logistical support of military ground robotic systems.

Originality. Originality lies in the integration of traditional regulatory approaches with agile life cycle management principles for cyber-physical systems, and in the structural separation of hardware and software life cycles within a unified model.

Paper type. Analytical and research article.

Ключові слова: наземні роботизовані комплекси, життєвий цикл, нормативна модель, озброєння та військова техніка.

Key words: ground robotic systems, life cycle, regulatory model, weapons and military equipment.

Вступ

Сучасні тенденції розвитку озброєння та військової техніки (ОВТ) свідчать про стрімке зростання ролі наземних роботизованих комплексів (НРК) у забезпеченні бойових дій, охороні об'єктів, розвідці, логістиці та інших завданнях. Завдяки поєднанню автономних та дистанційно керованих функцій, такі системи значно розширюють можливості підрозділів у тактичній і оперативній площинах. Водночас, впровадження НРК вимагає принципово нових

підходів до управління їх життєвим циклом (ЖЦ), які мають враховувати кіберфізичну природу цих систем, динамічність оновлення програмного забезпечення, швидкі темпи морального старіння окремих компонентів, а також вимоги щодо адаптивного супроводження в умовах змінної тактичної обстановки.

Теоретичні основи дослідження

Розроблення та впровадження військових НРК відбувається в умовах стрімкого розвитку кіберфізичних систем (КФС), високої технологічної динаміки та необхідності нормативного регулювання ЖЦ. Теоретичні основи дослідження формуються на перетині концепцій управління ЖЦ ОВТ, моделювання КФС, стандартів оборонного призначення (зокрема ДСТУ В 15.003:2021 [1] та ДСТУ В 15.004:2022 [2]), а також сучасних наукових підходів [3-10] до створення та супроводу складних систем подвійного і військового призначення.

У вітчизняному науково-технічному просторі питання НРК набуває все більшої актуальності. У працях [3, 4] підкреслено необхідність системного підходу до класифікації НРК, з урахуванням їх масогабаритних характеристик, рівня автономності та типів бойового застосування. Вказані дослідження окреслюють функціональні та структурні відмінності НРК порівняно з традиційними зразками ОВТ, що вимагає адаптації або перегляду існуючих моделей ЖЦ.

З позицій технічного моделювання та розроблення, у роботах [5, 6] подано аналітичні та симуляційні методи оцінювання кінематичних характеристик роботизованих платформ, що слугують підґрунтям для формалізації та уніфікації підетапів ЖЦ, зокрема у частині верифікації конструкції, етапів адаптації до умов експлуатації та технічного супроводу.

Інший важливий аспект – забезпечення інформаційної безпеки та конфігураційної цілісності протягом усього ЖЦ. Цю проблему розглядають автори у роботі [7], в якій пропонують системний підхід до керування ЖЦ інформаційної безпеки систем через моделі DevSecOps та оцінку динаміки загроз. Оскільки НРК — це кіберфізичні системи, що містять сенсорні, виконавчі, комунікаційні й програмні компоненти, питання безпеки слід розглядати не як окрему фазу, а як наскрізний процес ЖЦ.

Міжнародні дослідження [8-10] висвітлюють концепцію інтеграції безпеки, адаптивної архітектури та цифрових двійників як інструментів оптимізації ЖЦ КФС. Наприклад, моделі CLOPA дозволяють враховувати ризики на кожному етапі розробки та використання КФС, що прямо корелює з вимогами до військових НРК у змінному тактичному середовищі.

Таким чином, у контексті формування нормативної моделі ЖЦ військових НРК доцільно спиратися на такі теоретичні засади:

ієрархічну структуру життєвого циклу згідно з положеннями ДСТУ В 15.003:2021 та ДСТУ В 15.004:2022;

урахування специфічних характеристик НРК (автономність, мобільність, керованість), як це обґрунтовано у вітчизняних роботах;

модельно-орієнтовані методики (Model-Driven Engineering, цифрові двійники) для інтеграції розробки, тестування та експлуатації;

принципи наскрізного забезпечення кібербезпеки;

інституційно-нормативне обґрунтування — як підстава для адаптації моделі до умов застосування у ЗС України.

Постановка проблеми

У сфері військового озброєння НРК становлять окремий клас техніки, що відрізняється високим рівнем інтеграції апаратного забезпечення, програмного керування та функціональної адаптивності до умов бойового застосування. Однак на практиці впровадження таких систем

супроводжується відсутністю цілісної нормативної моделі їх ЖЦ, яка б враховувала специфіку їх кіберфізичної природи та сучасних вимог до військової робототехніки.

Чинні нормативні документи визначають загальні підходи до управління ЖЦ ОВТ, однак не деталізують особливості ЖЦ систем із гнучкою архітектурою, високим рівнем автономності та інтенсивною взаємодією з інформаційно-телекомунікаційними мережами. Зокрема, існує низка ключових методологічних та прикладних прогалин:

відсутність чіткого розмежування між етапами розроблення апаратної частини й програмного забезпечення НРК;

невизначеність процесів інтеграції, тестування, сертифікації та експлуатаційного супроводу систем подвійного (технічного та інформаційного) характеру;

недостатнє нормативне закріплення методів цифрового моделювання, симуляції, створення цифрових двійників;

ігнорування сучасних підходів до безперервного вдосконалення функцій безпеки та адаптивності систем в умовах змін тактичної обстановки;

розрив між практикою створення НРК і наявною нормативною документацією з боку замовника.

Крім того, досвід провідних країн засвідчує ефективність модульного, конфігураційного та ризик-орієнтованого підходів до управління ЖЦ кіберфізичних систем, проте в українській системі оборонного управління ці підходи ще не стандартизовані.

Таким чином, актуальною науково-прикладною проблемою є обґрунтування та формалізація нормативної моделі ЖЦ НРК, яка відповідала б вимогам до адаптивності та масштабованості систем, принципам наскрізної кібербезпеки, необхідності стандартизованого супроводу на всіх етапах ЖЦ — від ініціації до завершення експлуатації.

Методологія дослідження

Методологічна база дослідження сформована на основі міждисциплінарного підходу, що поєднує принципи системного аналізу, нормативної інженерії, кіберфізичного моделювання та теорії ЖЦ складних технічних систем.

В межах дослідження застосовано такі основні методи:

Системний аналіз — для ідентифікації ключових етапів, процесів і взаємозв'язків у ЖЦ військових НРК, а також для формалізації структури ЖЦ як цілісної системи з ієрархічною організацією.

Порівняльно-нормативний аналіз — для вивчення положень чинних стандартів (зокрема ДСТУ В 15.003:2021, ДСТУ В 15.004:2022) з метою визначення їх відповідності специфіці НРК, а також для виявлення регуляторних прогалин і невідповідностей в існуючих моделях ЖЦ.

Елементи Model-Based Systems Engineering (MBSE) — як методологічний підхід для побудови концептуальної моделі ЖЦ НРК із врахуванням специфіки КФС, зокрема — циклів розроблення, верифікації, сертифікації, супроводу та виводу з експлуатації.

Функціонально-логічне моделювання — для структурування життєвого циклу НРК у вигляді набору послідовних, взаємопов'язаних процесів (із виділенням фаз, підетапів, зворотних зв'язків і точок контролю).

Експертно-аналітичний підхід — на основі аналізу наукових публікацій, технічних описів і досвіду застосування НРК у ЗС України та збройних силах інших країн, із залученням опосередкованих оцінок через відкриті джерела.

Крім того, дослідження опирається на концепцію ЖЦ КФС, що використовується у провідних міжнародних підходах (зокрема, Cyber LOPA, DevSecOps для CPS), а також на принципи безперервної модернізації, конфігураційного управління та наскрізного забезпечення кібербезпеки.

Загальна логіка дослідження реалізована у вигляді послідовних етапів:

1. Аналіз чинної нормативної бази з питань ЖЦ ОВТ.
2. Ідентифікація особливостей військових НРК як об'єктів кіберфізичної природи.
3. Виявлення регуляторних та методичних обмежень існуючих моделей ЖЦ.
4. Формування вимог до адаптованої моделі ЖЦ НРК.
5. Розроблення концептуальної нормативної моделі ЖЦ військових НРК.

Таким чином, обґрунтована методологія дозволяє не лише виявити невідповідності існуючих підходів до ЖЦ сучасним характеристикам роботизованих комплексів, але й запропонувати практичну модель, що може бути покладена в основу майбутнього нормативного документа оборонного призначення.

Результати

На першому етапі дослідження було здійснено системний аналіз нормативної бази, що регламентує процеси управління ЖЦ ОВТ в ЗС України. Основну увагу зосереджено на положеннях двох ключових документів — ДСТУ В 15.003:2021 та ДСТУ В 15.004:2022, які визначають відповідно процеси управління ЖЦ ОВТ та структурно-фазову модель його ЖЦ.

ДСТУ В 15.003:2021 регламентує набір процесів, що реалізуються на всіх етапах ЖЦ ОВТ — від ініціювання потреби до завершення експлуатації. Документ передбачає класифікацію процесів ЖЦ на основні, допоміжні та організаційні, і містить формалізований підхід до їх узгодження, управління та документального супроводу. Водночас, акцент зроблено на традиційні типи ОВТ, у яких домінує апаратна (фізична) компонента, а процеси розроблення програмного забезпечення розглядаються побічно — як допоміжні або супровідні.

ДСТУ В 15.004:2022, у свою чергу, встановлює етапну модель ЖЦ ОВТ, що включає стадії: формування концепції, дослідно-конструкторські роботи, підготовку виробництва, серійне виробництво, постачання, експлуатацію, ремонт, модернізацію та списання. Хоча в документі формально закладено можливість уточнення змісту стадій з урахуванням особливостей конкретного виду озброєння, він не передбачає спеціального трактування складних технічних систем кіберфізичної природи, таких як НРК.

Проведений аналіз дозволив виявити низку важливих обмежень чинної нормативної бази з точки зору її придатності для регламентування ЖЦ НРК:

По-перше, відсутнє розмежування між розробкою апаратної платформи та створенням програмного забезпечення, яке відіграє ключову роль у функціонуванні НРК. Програмна частина, що забезпечує автономне керування, адаптацію до середовища, виявлення об'єктів тощо, на практиці має окрему логіку створення, тестування та оновлення, яка не відображена в існуючих регламентуючих документах.

По-друге, етапи ЖЦ не враховують ітеративності та циклічності процесів, характерних для сучасних технологій створення складних систем. У життєвому циклі НРК критично важливо забезпечити можливість багаторазового оновлення програмного забезпечення, повторного тестування, впровадження нових алгоритмів керування — тобто передбачити адаптивну модель із численними зворотними зв'язками, чого немає в чинній лінійно-послідовній структурі.

По-третє, ігнорується роль цифрових технологій управління конфігурацією, таких як цифрові двійники, цифрові паспорти та інструменти симуляції, які мають принципове значення для експлуатації НРК у бойових умовах. На рівні стандартів ці процеси поки не формалізовані.

По-четверте, не регламентовано питання безперервного моніторингу та технічної адаптації, які є критичними для КФС, особливо у військовому середовищі з високим рівнем динамічності та непередбачуваності загроз.

Таким чином, проведений нормативний аналіз засвідчив, що чинна модель управління ЖЦ ОБТ не дозволяє повною мірою врахувати специфіку НРК як кіберфізичних систем, які поєднують в собі фізичні, програмні та інформаційно-телекомунікаційні компоненти. Це стало передумовою до формулювання наступного етапу дослідження — виокремлення ключових особливостей НРК як об'єктів з особливою архітектурною та функціональною природою.

Наступним етапом дослідження стало визначення ключових техніко-функціональних та архітектурних особливостей військових НРК, що відрізняють їх від класичних зразків ОБТ. Це дало змогу уточнити вимоги до нормативної моделі їхнього ЖЦ, яку необхідно адаптувати до сучасних технологічних реалій.

НРК за своєю сутністю є складними кіберфізичними системами. У них органічно поєднуються апаратна частина (мобільна платформа, сенсори, засоби ураження), програмна частина (вбудоване програмне забезпечення, алгоритми автономного керування, інтерфейси взаємодії) та інформаційно-телекомунікаційна складова (засоби зв'язку, захищені канали управління, інтеграція в мережоцентричне середовище).

До основних характеристик НРК, що суттєво впливають на вимоги до моделі їхнього ЖЦ, належать:

1. Кіберфізична архітектура. НРК є системами, де фізичні процеси та дії керуються, координуються і адаптуються в реальному часі за допомогою цифрових алгоритмів. Система прийняття рішень працює на основі даних від сенсорів, відеокамер, LIDAR- або RADAR-систем, які обробляються onboard-комп'ютерами з високою обчислювальною здатністю. Це означає, що оновлення програмного забезпечення чи зміна алгоритмів може радикально змінити поведінку НРК, без фізичного втручання у його конструкцію.

2. Модульність і масштабованість. Більшість сучасних НРК проектується за модульним принципом, що дозволяє змінювати сенсорне навантаження, замінювати виконавчі модулі (наприклад, зброю або системи транспортування), додавати нові програмні функції або комунікаційні інтерфейси. Це створює виклики для управління конфігурацією та відстеження змін протягом усього ЖЦ.

3. Інтенсивне використання програмного забезпечення. На відміну від класичних зразків ОБТ, НРК залежні від постійно оновлюваного ПЗ, яке може містити десятки або сотні тисяч рядків коду. До програмної частини НРК входять: система навігації, розпізнавання об'єктів, планування маршрутів, системи ухвалення рішень, засоби самоадаптації тощо. Тому управління ПЗ стає окремим і повноцінним процесом у ЖЦ, що має бути нормативно врегульовано.

4. Необхідність безперервного цифрового моніторингу. Функціонування НРК вимагає постійного віддаленого контролю стану апаратних вузлів, програмного забезпечення, батарей, зв'язку. Цей контроль зазвичай здійснюється через захищені канали та цифрові інтерфейси. У перспективі застосування цифрових двійників дозволить симулювати поведінку НРК в умовах, наближених до реальних, що потребує включення таких цифрових засобів до нормативної моделі ЖЦ.

5. Високий рівень кіберзалежності та вимоги до кіберзахисту. НРК функціонують у середовищі інформаційної боротьби, тому забезпечення стійкості до кібератак, захист каналів управління, криптографічна безпека, верифікація коду та перевірка цілісності ПЗ стають обов'язковими елементами експлуатації. Таким чином, функції кіберзахисту мають бути закладені в усі етапи ЖЦ, починаючи з проектування.

6. Адаптивність до динамічного бойового середовища. На відміну від статичних або прогнозованих умов застосування звичайного ОБТ, НРК діють у мінливому, непередбачуваному середовищі, що вимагає від них здатності до адаптації. Це обумовлює потребу в частих оновленнях функціоналу, гнучкому плануванні місій та зміні конфігурацій — усе це має бути передбачено на рівні ЖЦ.

Таким чином, НРК є високотехнологічними гібридними системами, ЖЦ яких вимагає зовсім іншого підходу до управління, ніж класичний лінійний. Ідентифіковані ознаки обґрунтовують необхідність трансформації чинної нормативної моделі ЖЦ відповідно до парадигми безперервного, адаптивного, цифрово-керованого ЖЦ.

Після ідентифікації характерних ознак НРК як кіберфізичних систем, наступним логічним кроком стало співставлення цих вимог із чинними нормативними та методичними підходами до управління ЖЦ ОВТ. Метою даного етапу було визначення тих регуляторних розривів, які обмежують ефективну інтеграцію НРК у діючу систему забезпечення ЖЦ в секторі безпеки і оборони України.

Аналіз нормативно-методичних документів, а також супровідних документів, які регламентують постановку ОВТ на виробництво, організацію дослідно-конструкторських робіт, вимоги до експлуатації та ремонту, виявив низку суттєвих обмежень, які знижують адаптивність чинної моделі ЖЦ до умов функціонування НРК.

По-перше, це лінійна структура життєвого циклу. Чинна нормативна модель ЖЦ ОВТ передбачає переважно лінійну послідовність етапів: від формування потреби — до списання. Такий підхід є ефективним у випадку техніки зі стабільною апаратною структурою та мінімальною динамікою оновлення. Проте НРК, як кіберфізичні системи, вимагають циклічної (ітеративної) моделі, що враховує часті оновлення програмного забезпечення, конфігурацій апаратних модулів, зміну призначення або тактики застосування. В існуючій моделі такі ітерації або не передбачені, або трактуються як винятки (модернізація, ремонт), що не відповідає їх системній природі.

Наступне обмеження це інтеграція цифрових процесів лише на рівні експлуатації. Незважаючи на визнання значення цифрових технологій у супроводі ЖЦ ОВТ, їх роль у чинних стандартах здебільшого обмежена етапом експлуатації (звітування, технічна діагностика тощо). Водночас НРК потребують цифрового супроводу на всіх етапах життєвого циклу, зокрема — у формі цифрових моделей, верифікаційних платформ, цифрових двійників, моделей місії, симуляцій середовища. Відсутність нормативної вимоги щодо використання таких інструментів у фазах розроблення та тестування унеможливорює комплексну перевірку поведінки НРК до моменту його бойового застосування.

Також має місце неврегульованість управління конфігурацією та оновленням ПЗ в існуючій моделі ЖЦ ОВТ. НРК функціонують у реальному часі за рахунок високодинамічного програмного забезпечення, яке може змінюватися навіть після початку експлуатації (через патчі, апдейти, зміну алгоритмів тощо). У чинних моделях ЖЦ управління ПЗ не виділено в окрему фазу або підпроцес. Оновлення ПЗ часто розглядаються як частина модернізації, хоча на практиці це нормальний і частий цикл супроводу. Відсутність процедур версифікації, атестації, технічного супроводу програмної частини призводить до ризику неконтрольованих змін бойових можливостей комплексу.

Ще одне з обмежень це неузгодженість ролей між розробниками ПЗ, виробником та експлуатантом. У кіберфізичних системах, де апаратна і програмна частини часто створюються різними організаціями, виникає проблема координації ролей між суб'єктами ЖЦ. В існуючій нормативній базі не визначено, хто відповідальний за технічну підтримку, аудит, виправлення вразливостей ПЗ, а також яким чином це відображається на гарантійних зобов'язаннях виробника. Така неузгодженість створює регуляторні "сірі зони", що унеможливають формалізацію управління ЖЦ у повному обсязі.

Поряд з цим формальний характер етапів тестування та сертифікації для складних адаптивних систем також створюють обмеження для ефективної інтеграції НРК у діючу систему забезпечення ЖЦ. НРК потребують досконалих і багатоетапних процедур тестування, які повинні охоплювати: валідацію функціоналу, стрес-тести, поведінкове тестування в симульованому середовищі, оцінювання адаптивності, відмовостійкості тощо. Проте існуючі

стандарти передбачають переважно формальні процедури приймальних та кваліфікаційних випробувань, які не охоплюють програмну та поведінкову складову повною мірою. Це ускладнює виявлення критичних помилок ще до постачання комплексів в підрозділи.

Таким чином, на основі співставлення вимог, обумовлених природою НРК, з наявною нормативною базою, було встановлено, що існуюча модель ЖЦ ОВТ є недостатньо придатною для повноцінного управління ЖЦ НРК. Це створює передумови для обґрунтування та формування вимог до альтернативної нормативної моделі ЖЦ НРК, що буде предметом наступного етапу дослідження.

Враховуючи виявлені на попередньому етапі обмеження чинної нормативної бази, а також специфіку НРК як високотехнологічних КФС, сформульовано узагальнені вимоги до нормативної моделі їхнього ЖЦ. Ці вимоги покликані забезпечити гнучкість, адаптивність, технологічну відповідність і наскрізну керованість ЖЦ НРК в умовах сучасного оборонного середовища.

Сформульовані вимоги згруповано за п'ятьма ключовими напрямками (див. таблицю):

Таблиця 1 – Вимоги до нормативної моделі життєвого циклу військових наземних роботизованих комплексів

№ з/п	Напрямок вимог	Сформульована вимога	Обґрунтування вимоги	Очікувані результати реалізації
1.	Циклічність і адаптивність ЖЦ	Життєвий цикл НРК має бути організований як замкнена адаптивна петля з можливістю зворотних переходів між етапами.	НРК потребують частого оновлення, адаптації до умов місії, модернізації та доопрацювання в умовах динамічної обстановки.	Підвищення оперативності реагування на зміни; можливість швидкого вдосконалення та корекції функцій.
2.	Управління життєвим циклом ПЗ	ПЗ повинно мати окремий, інтегрований у загальний ЖЦ НРК життєвий цикл із чіткими процедурами оновлення, тестування, атестації.	Програмне забезпечення — критичний компонент НРК, що визначає поведінку, функціональність і безпеку.	Забезпечення стабільності, передбачуваності та керованості при оновленнях ПЗ; зменшення ризиків збоїв.
3.	Цифровізація процесів ЖЦ	Усі етапи ЖЦ мають супроводжуватись цифровими моделями (цифрові двійники, digital thread), з єдиним цифровим простором.	Цифрові технології дозволяють проводити симуляції, моделювання та аналіз без реального втручання в НРК.	Прискорення прийняття рішень, оптимізація логістики, зниження вартості експлуатації.
4.	Управління конфігурацією та змінами	Модель ЖЦ має містити процедури управління конфігурацією, верифікації змін,	Часті модифікації НРК унеможливають статичний облік; потрібен динамічний контроль технічного стану.	Підвищення надійності, передбачуваності та сумісності систем після змін.

№ з/п	Напрямок вимог	Сформульована вимога	Обґрунтування вимоги	Очікувані результати реалізації
		контролю версій та фіксації впливу на		
5.	Інтеграція кіберзахисту	Усі етапи ЖЦ мають включати заходи з аналізу загроз, тестування на вразливості, сертифікації безпеки ПЗ та апаратури.	НРК як кіберфізичні системи є об'єктами потенційного зовнішнього втручання через мережу, сенсори чи ПЗ.	Зниження ймовірності кібератак, підвищення рівня довіри до систем.

Отже, сформульовані вимоги дозволяють окреслити рамки цільової нормативної моделі ЖЦ НРК — моделі, яка ґрунтується на принципах цифрової трансформації, адаптивного управління, відкритої архітектури, кіберзахищеності та наскрізної керованості.

На основі попередньо визначених напрямів та вимог, сформовано концептуальну структуру нормативної моделі ЖЦ НРК. Основою структури стали такі принципи:

Модульність — модель складається з чітко визначених процесних блоків;

Адаптивність — передбачено зворотні зв'язки між етапами;

Цифрова підтримка — кожен блок супроводжується цифровими представленнями (моделями, параметрами, документацією);

Безпековий вектор — заходи кіберзахисту інтегруються в кожен етап.

Запропонована структура нормативної моделі ЖЦ НРК:

1. Ініціація потреби:

аналіз оперативних задач;

ідентифікація функціональних прогалін;

формування тактико-технічного завдання.

2. Концептуальне проєктування:

побудова цифрової концептуальної моделі;

аналіз життєздатності у симульованому середовищі;

попередній аналіз ризиків і вразливостей.

3. Розроблення дослідного зразка:

створення фізичного прототипу НРК;

окреме створення версій ПЗ з модульною архітектурою;

розгортання цифрового двійника.

4. Випробування і сертифікація:

функціональні випробування;

кіберзахисна перевірка (пентести, статичний/динамічний аналіз ПЗ);

верифікація відповідності конфігурації цифровому двійнику.

5. Постачання і впровадження:

адаптація до оперативного середовища;

навчання операторів;

імплементация системи моніторингу в реальному часі.

6. Експлуатація з динамічним супроводженням:

постійний зворотний зв'язок (лог-файли, телеметрія);

впровадження оновлень ПЗ через захищені канали;

автоматичне керування конфігурацією.

7. Модернізація / Відновлення / Виведення з експлуатації:

інтеграція з новими технологіями (edge-AI, нові сенсори);

аналіз рентабельності модернізації;

цифрова фіксація утилізації.

Графічне представлення запропонованої нормативної моделі ЖЦ НРК представлена на рис. 1.

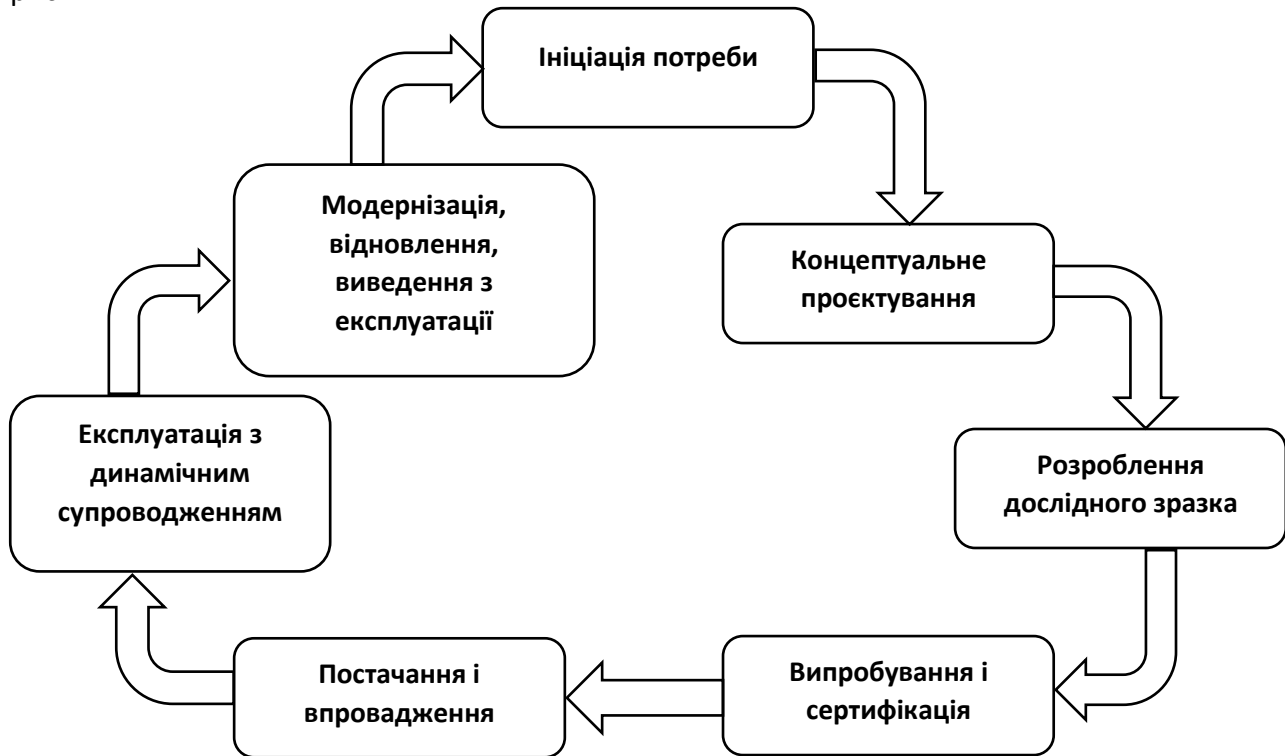


Рис. 1. Нормативна модель життєвого циклу наземних роботизованих комплексів

Висновки

В результаті дослідження сформовано нормативно орієнтовану структуру ЖЦ військових НРК, яка відображає особливості функціонування, цифрового супроводження та безперервної модернізації таких систем. Визначено сім послідовних етапів ЖЦ НРК, побудованих за принципом замкненого циклу, що передбачає повернення до ініціації потреби після модернізації або виведення з експлуатації.

Запропонована модель охоплює:

повний цикл від ідентифікації потреб до утилізації НРК;

інтеграцію цифрового двійника як інструмента супроводження на всіх етапах;

закладену здатність до динамічного оновлення та адаптації;

врахування вимог кіберзахисту, інтероперабельності та автономності.

Модель забезпечує структурну основу для подальшої розробки стандартів, методичних документів і цифрових рішень, орієнтованих на практичне впровадження військових роботизованих систем.

Подальші дослідження доцільно зосередити на формалізації критеріїв оцінювання ефективності процесів ЖЦ НРК, створенні моделей супроводження із використанням технологій цифрових двійників, а також на розробленні інформаційної платформи управління ЖЦ НРК у складі об'єднаної інформаційної інфраструктури.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. ДСТУ В 15.003:2021 Система керування життєвим циклом озброєння та військової техніки. Процеси життєвого циклу озброєння та військової техніки. Дійсний з 01.09.2022. ДП «УкрНДНЦ», 2021.
2. ДСТУ В 15.004:2022. Система розроблення і поставлення на виробництво озброєння та військової техніки. Стадії життєвого циклу озброєння та військової техніки. Дійсний з 01.10.2023. ДП «УкрНДНЦ», 2022.
3. Кириченко Іван. Наземні роботизовані комплекси: основи та майбутнє. Молодий вчений, № 12 (100), 2021, с. 16-20. <https://doi.org/10.32839/2304-5809/2021-12-100-4>.
4. Залипка В. Д. Особливості створення та застосування наземних роботизованих комплексів у провідних країнах світу та Україні. Науковий вісник НЛТУ України, № 32 (4), 2022, с. 60-65. <https://doi.org/10.36930/40320410>.
5. Струтинський В.Б., Гуржій А.М. Наземні роботизовані комплекси: монографія. ПП «Рута», Житомир, 2023, 497 с.
6. Alyokhina, S., Nevliudov, I., Romashov, Yu. Computer simulations of controllability processes for robotic wheeled platforms taking into account restrictions of jerk motions. Сучасний стан наукових досліджень та технологій в промисловості. № 1 (19), 2022, С. 65-75. <https://doi.org/10.30837/ITSSI.2022.19.065>.
7. Мохор В.В., Бакалинський О.О., Дорогий Я.Ю., Цуркан В.В. Життєвий цикл систем управління інформаційною безпекою. Тези XXIII міжнародної науково-технічної конференції «Проблеми інформатики та моделювання (ПІМ-2023)». Харків, 20-22 вересня 2023 року, НТУ «ХПІ», С.16. <https://doi.org/10.5281/zenodo.14601460>.
8. Sun Cong, Ma Jianfeng, Yao Qingsong. On the architecture and development life cycle of secure cyber-physical systems. Journal of Communications and Information Networks. № 1 (4), 2016, p. 1-21. <https://doi.org/10.11959/j.issn.2096-1081.2016.041>.
9. Ashraf Tantawy, Sherif Abdelwahed, Abdelkarim Erradi. Cyber LOPA: An integrated approach for the design of dependable and secure cyber-physical systems. IEEE Transaction on Reliability. Vol. 71, № 2, 2022, p. 1075-1091. <https://doi.org/10.1109/TR.2022.3163652>.
10. Mustafa Abshir Mohamed, Geylani Kardas, Moharram Challenger. A systematic literature review on model-driven engineering for cyber-physical systems: Technical report. Cornell University, Ithaca, NY, USA, 2021, 90 p. <https://doi.org/10.48550/arXiv.2103.08644>.

References

1. DSTU V 15.003:2021 Life cycle management system for weapons and military equipment. Life cycle processes for weapons and military equipment. Valid from 01.09.2022. "UkrNDNC", 2021.
2. DSTU V 15.004:2022. System for the development and commissioning of weapons and military equipment. Stages of the life cycle of weapons and military equipment. Valid from 01.10.2023. "UkrNDNC", 2022.
3. Ivan Kyrychenko. Ground robotic complexes: basics and future. Young Scientist, No. 12 (100), 2021, pp. 16-20. <https://doi.org/10.32839/2304-5809/2021-12-100-4>.
4. Zalyпка, V.D. Features of the creation and application of ground robotic complexes in leading countries of the world and Ukraine. Scientific Bulletin of the National Technical University of Ukraine, No. 32 (4), 2022, pp. 60-65. <https://doi.org/10.36930/40320410>.

5. Strutynskyi, V.B., Gurzhii, A.M. Ground robotic complexes: monograph. PP “Ruta”, Zhytomyr, 2023, 497 p.
6. Alyokhina, S., Nevliudov, I., Romashov, Yu. Computer simulations of controllability processes for robotic wheeled platforms taking into account restrictions of jerk motions. Current status of scientific research and technologies in industry. No. 1 (19), 2022, pp. 65-75. DOI: <https://doi.org/10.30837/ITSSI.2022.19.065>.
7. Mohor, V.V., Bakalynsky, O.O., Dorogy, Ya.Yu., Tsurkan, V.V. Life cycle of information security management systems. Abstracts of the XXIII International Scientific and Technical Conference “Problems of Informatics and Modeling (PIM-2023)”. Kharkiv, September 20-22, 2023, NTU “KhPI”, p.16. <https://doi.org/10.5281/zenodo.14601460>.
8. Sun Cong, Ma Jianfeng, Yao Qingsong. On the architecture and development life cycle of secure cyber-physical systems. *Journal of Communications and Information Networks*. № 1 (4), 2016, p. 1-21. DOI: <https://doi.org/10.11959/j.issn.2096-1081.2016.041>.
9. Ashraf Tantawy, Sherif Abdelwahed, Abdelkarim Erradi. Cyber LOPA: An integrated approach for the design of dependable and secure cyber-physical systems. *IEEE Transaction on Reliability*. Vol. 71, № 2, 2022, p. 1075-1091. DOI: <https://doi.org/10.1109/TR.2022.3163652>.
10. Mustafa Abshir Mohamed, Geylani Kardas, Moharram Challenger. A systematic literature review on model-driven engineering for cyber-physical systems: *Technical report*. Cornell University, Ithaca, NY, USA, 2021, 90 p. <https://doi.org/10.48550/arXiv.2103.08644>.

Формування моделей оцінки ефективності стрільби зенітними керованими ракетами з урахуванням ймовірностей ураження повітряних цілей

Development of Evaluation Models for Surface-to-Air Missile Firing Effectiveness with Consideration of Air Target Kill Probabilities

Павло Опенько ^A

Corresponding author: к.т.н. старший дослідник, Заслужений винахідник України, начальник кафедри, e-mail: pavel.openko@ukr.net, ORCID: 0000-0001-7777-5101

Олександр П'явчук ^A

доктор філософії, старший викладач кафедри, e-mail: pjawa0905@gmail.com, ORCID: 0000-0002-5623-1866

Юрій Целіщев ^A

к.т.н., доцент, доцент кафедри, e-mail: pjawa0905@gmail.com, ORCID: 0000-0002-3739-9567

Віктор Кудряшов ^B

к.т.н., старший науковий співробітник, старший науковий співробітник відділу нелінійної динаміки електронних систем інституту, e-mail: victor.e.kudryashov@gmail.com, ORCID: 0000-0002-7055-5357

Олексій Коломійцев ^C

д.т.н., професор, Заслужений винахідник України, професор кафедри комп'ютерної інженерії та програмування, e-mail: alexus_k@ukr.net, ORCID: 0000-0001-8228-8404

Валерій Воїнов ^D

к.т.н., доцент, заступник начальника факультету з навчальної та наукової роботи, e-mail: Vvoinov80@gmail.com, ORCID: 0000-0002-5732-5960

Pavlo Openko ^A

Corresponding author: Candidate of Technical Sciences, Senior Research Fellow, Honored Inventor of Ukraine, Head of the Department, e-mail: pavel.openko@ukr.net, ORCID: 0000-0001-7777-5101

Oleksandr Piavchuk ^A

PhD, Senior Lecturer of the Department, e-mail: pjawa0905@gmail.com, ORCID: 0000-0002-5623-1866

Yurii Tselishev ^A

Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department, e-mail: pjawa0905@gmail.com, ORCID: 0000-0002-3739-9567

Viktor Kudriashov ^B

Candidate of Technical Sciences, Senior Research Fellow, Senior Research Fellow Department, e-mail: victor.e.kudryashov@gmail.com, ORCID: 0000-0002-7055-5357

Oleksii Kolomiitsev ^C

Dr of Engineering Science, Professor, Professor of the Department, e-mail: alexus_k@ukr.net, ORCID: 0000-0001-8228-8404

Voinov Valerii ^D

Candidate of Technical Sciences, Associate Professor, Deputy Dean of Army Air Defence Faculty, e-mail: Vvoinov80@gmail.com, ORCID: 0000-0002-5732-5960

^A Національний університет оборони України, м. Київ, Україна

^B Інститут радіофізики та електроніки НАН України ім. О. Я. Усікова, м. Харків, Україна

^C Національний технічний університет "Харківський політехнічний інститут", м. Харків, Україна

^D Харківський національний університет Повітряних Сил ім. І. Кожедуба, м. Харків, Україна

^A National Defence University of Ukraine, Kyiv, Ukraine

^B O.Ya. Usikov Institute for Radiophysics and Electronics of the National Academy of Sciences of Ukraine, Kharkiv, Ukraine

^C National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

^D Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

Received: August 7, 2025 | Revised: August 19, 2025 | Accepted: August 31, 2025

УДК: 519.2-623.1/.7

DOI: 10.33445/sds.2025.15.4.2

Мета роботи: розробити часткову модель для розрахунку значень умовних ймовірностей ураження цілі, для формування найкращих варіантів відбиття удару повітряного противника, а також обґрунтування загальних напрямків удосконалення елементів системи управління вогнем.

Метод: основними методами дослідження є: статистичного аналізу, чисельний метод, порівняльного аналізу.

Результати дослідження: В цілому приведена залежність величин умовних ймовірностей ураження цілей від дев'яти основних параметрів, які описують стрільбу зенітними керованими ракетами та управління вогнем. Отримані практичні результати часткової моделі необхідні для ефективного застосування озброєння за призначенням.

Теоретична цінність дослідження: В статті приведено розрахунки, які дозволяють завчасно розробити декілька варіантів дій самохідних вогневих одиниць (бойових машин), підрозділів при відбитті повітряного удару противника.

Purpose: to develop a partial model for calculating the values of conditional probabilities of target engagement, to generate optimal options for countering enemy air strikes, and to justify the general directions for improving elements of the fire control system.

Method: the main research methods are: statistical analysis, numerical methods, and comparative analysis.

Findings: a relationship is presented between the values of conditional probabilities of target engagement and nine key parameters that characterize surface-to-air missile firing and fire control. The practical results obtained from the partial model are essential for the effective employment of weapon systems as intended.

Theoretical implications: the article provides calculations that make it possible to pre-plan several courses of action for self-propelled fire units (combat vehicles) and subunits in repelling enemy air strikes. The model takes into account the

При цьому враховано параметри удару повітряного противника по бойових порядках військ (сил). У теперішній час відсутня часткова модель, яка визначить значення ефективності стрільби з врахуванням ймовірностей входу повітряних цілей в зону цілерозподілу. Також проведена оцінка ймовірності не виходу повітряних цілей з зони пуску та зони ураження зенітного ракетного комплексу, після пуску зенітних керованих ракет, при цьому враховано вплив ефективної поверхні розсіювання цілей, рівень перешкод і перевантажень цілі, при її маневруванні. Тому задача розробки варіантів дій самохідних вогневих одиниць (бойових машин), підрозділів при відбитті удару противника є важливою та актуальною.

Тип статті: науково-практична.

parameters of the enemy air strike against the combat formations of friendly forces. Currently, there is no existing partial model that determines the effectiveness of missile firing while considering the probabilities of air targets entering the target allocation zone. The study also includes an assessment of the probability that air targets will not exit the missile launch and engagement zones of the surface-to-air missile system after launch. This assessment considers factors such as the effective radar cross-section (RCS) of targets, the level of jamming, and target overload during maneuvering. Therefore, the task of developing response options for self-propelled fire units and subunits in countering enemy strikes is both important and timely.

Paper type: scientific and practical.

Ключові слова: відношення сигнал-шум, ймовірності вірного виявлення, ймовірності входу цілей у зони цілерозподілу, ймовірності не виходу цілей з зон пуску (ураження) комплексу, параметри першого та другого родів стрільби ракетами, умовні ймовірності ураження цілей, цілерозподіл.

Key words: signal-to-noise ratio, probabilities of correct detection, probabilities of target entry into target allocation zones, probabilities of target retention within missile launch (engagement) zones, first- and second-type missile firing parameters, conditional probabilities of target engagement, target allocation.

Вступ

Управління вогнем (УВ) підрозділів протиповітряної оборони (ППО) передбачає завчасно розробку декількох варіантів дій самохідних вогневих одиниць (бойових машин), підрозділів (батареї) при відбитті удару повітряного противника. При цьому необхідно враховувати параметри удару повітряного противника по бойових порядках військ (сил) [1-5]. У теперішній час відсутня часткова модель, яка визначить значення ефективності стрільби з врахуванням ймовірностей входу цілей в зону цілерозподілу (ЦР). Також потрібно оцінювати ймовірності не виходу цілей з зони пуску (ЗПу) та зони ураження (ЗУ) зенітного ракетного комплексу, після пуску зенітних керованих ракет. Необхідно враховувати вплив ефективної поверхні розсіювання (ЕПР) цілей, рівень перешкод і перевантажень цілі, при її маневруванні. Тому задача розробки варіантів дій самохідних вогневих одиниць (бойових машин), підрозділів (батареї) при відбитті удару противника є важливою та актуальною. В якості показника ефективності УВ застосовуємо значення умовних ймовірностей ураження цілей [1-3].

Теоретичні основи дослідження

Відомо, що УВ підрозділами військ ППО полягає у цілеспрямованій діяльності командирів (начальників), штабів, бойових розрахунків сумісних командних пунктів авіації і протиповітряної оборони (СКП А і ППО), командних пунктів (КП), пунктів управління (ПУ) по підтримці бойової готовності військових частин (підрозділів) ППО, підготовці бойових дій (операцій) і управління ними при відбитті ударів засобів повітряного нападу (ЗПН) противника. Метою УВ підрозділами військ ППО є повне використання вогневих можливостей підрозділів військ ППО для надійного прикриття та захисту підрозділів (угруповань) військ та інших об'єктів від ударів ЗПН противника, для знищення засобів повітряної розвідки, носіїв високоточної зброї, повітряних десантів та повітрянодесантних військ противника в повітрі.

На сьогодні основними видами цілерозподілу (ЦР) є: централізований, децентралізований, автономний та змішаний ЦР повітряних цілей (ПЦ). Взагалі, ЦР ПЦ між вогневими засобами підрозділів (угруповання) військ ППО, які прикривають підрозділи (угруповання) військ та інші об'єкти з повітря, вимагає витрати часу, пов'язаного з обробкою інформації про повітряну обстановку. Автоматизація даного процесу прямо пов'язана з необхідністю вдосконалення цього елемента контуру управління, завдяки впровадженню методу ефективного ЦР при УВ підрозділу. Вибір методу дає можливість прискорити прийняття рішення командиром будь-якої ланки по ефективному розподілу цілей при УВ підрозділу і уникнути збитки об'єктам, які прикриваються.

Проблема вдосконалювання УВ підрозділами військ ППО полягає у вирішенні протиріччя між вже досягнутими та всезростаючими можливостями вогневих засобів з одного боку, та, з іншого – з можливостями системи управління по використанню вогню зенітних засобів для надійного прикриття та захисту підрозділів (угруповань) та об'єктів. Проведений для цього аналіз публікацій, котрі представлені у літературі [1-6] не дають можливості визначати показники ефективності стрільби по різних цілях, в умовах протидії противника, та в відповідності до технічних характеристик елементів схеми УВ. В вказаній літературі приведені загальні підходи до рішення даної задачі.

Постановка проблеми

На підставі вищевикладеного, можливо стверджувати, що пошук рішення для отримання централізації та децентралізації функцій управління КП і ПУ різних рівнів для використання достоїнств кожного з видів ЦР, установлення залежності ефективності застосування самохідних вогневих одиниць (бойових машин), підрозділів (батареї) від цього співвідношення та на даній основі – розробка оптимальних управляючих алгоритмів та визначення напрямків удосконалювання технічних засобів і структури системи УВ – одне з найважливіших завдань теорії і практики УВ підрозділами (угрупованнями) військ ППО при веденні бойових дій (операцій). Удосконалення управління самохідними вогневими одиницями (бойовими машинами), підрозділами (угрупованнями) військ ППО та його найважливішій складовій частини – УВ, поряд з якісним удосконалюванням зенітних ракетних комплексів, є основним напрямком підвищення бойових можливостей підрозділів (угруповань) військ ППО по відбиттю ударів ЗПН противника.

Метою статті є розробка часткової моделі для розрахунку значень умовних ймовірностей ураження цілі, для формування найкращих варіантів відбиття удару повітряного противника, а також обґрунтування загальних напрямків доробки елементів системи УВ.

Результати

Для досягнення мети статті розглянемо спрощену схему УВ, яка зазвичай реалізується. Спрощена схема УВ складається з послідовно з'єднаних радіолокаційних станцій (РЛС) старшого начальника, командного пункту полка (КПП), батарейного командного пункту (БКП) та самохідних вогневих одиниць (бойових машин), підрозділу (батареї) [1-6].

1. Визначення дальнього та ближнього рубежів постановки вогневих завдань, дальньої та ближньої межі зони повітряної обстановки [1, 2].

Для типової цілі (ТЦ) обрали осереднену швидкість підльоту V у 230 м/с та висоту польоту H в 10^3 м.

$$\begin{aligned} D_{\text{ДПЗ}} &= \left\{ \{d_d + V[\tau_{\text{КПП}} + \tau_{\text{БКП}} + \tau_{\text{ППС}} + \tau_{\text{БПС}} + \tau_{\text{СТ}} + \tau_{\text{РД}}]\}^2 + H^2 \right\}^{0,5}, \\ D_{\text{БПЗ}} &= \left\{ \{d_b + V[\tau_{\text{КПП}} + \tau_{\text{БКП}} + \tau_{\text{ППС}} + \tau_{\text{БПС}} + \tau_{\text{СТ}} + \tau_{\text{РБ}}]\}^2 + H^2 \right\}^{0,5}, \quad h_{\text{ЦР}} = VT_{\text{Ц.стр.}}, \\ D_{\text{ДПО}} &= D_{\text{ДПЗ}} + 2h_{\text{ЦР}}, \quad D_{\text{БПО}} = D_{\text{ДПЗ}} + h_{\text{ЦР}}, \end{aligned} \quad (1)$$

- де $D_{\text{ДПЗ}}, D_{\text{БПЗ}}$ – відповідно дальній та ближній рубежі постановки вогневих завдань самохідними вогневими одиницями (бойовими машинами);
- d_d, d_b – горизонтальні дальності до дальньої та ближньої границі зони ураження (ЗУ);
- $\tau_{\text{КПП}}, \tau_{\text{БКП}}$ – робітні часи КПП та БКП відповідно;
- $\tau_{\text{ППС}}, \tau_{\text{БПС}}$ – відповідно часи попередньої та безпосередньої підготовки стрільби самохідними вогневими одиницями (бойовими машинами);
- $\tau_{\text{СТ}}$ – час затримки старту зенітної керованої ракети;

- $\tau_{рд}, \tau_{рб}$ – часи польоту ракети до дальньої межі зони ураження (ДМЗУ) та ближньої межі зони ураження (БМЗУ) відповідно;
- $D_{дпо}, D_{бпо}$ – дальня та ближня межі повітряної обстановки відповідно;
- $h_{цр}, T_{ц.стр.}$ – відповідно глибина ЦР та час циклу стрільби самохідної вогневої одиниці (бойової машини); причому час польоту ракети до i точки ЗУ дорівнює: $\tau_{pi} = 2,5 + 1,75 \cdot 10^3 D$.

Якщо $d_d = 10^4$ м, $\tau_{кпп} \approx \tau_{бкп} \approx 31$ с в умовах перешкод середньої щільності, $\tau_{ппс} = 218$ с, $\tau_{бпс} = 55$ с, $\tau_{ст} \approx 1,5$ с, $\tau_{рд} \approx 20$ с, $d_b = 1,5 \cdot 10^3$ м, $\tau_{рб} \approx 5,1$ с, $T_{ц.стр.} \approx 90$ с в умовах перешкод середньої щільності. Отримали при готовності самохідної вогневої одиниці (бойової машини) № 2 $D_{дпз} \approx 92 \cdot 10^3$ м, $D_{бпз} \approx 80 \cdot 10^3$ м, а з готовності № 1 – $D_{дпз} \approx 41,9 \cdot 10^3$ м, $D_{бпз} \approx 30 \cdot 10^3$ м та $h_{цр} \approx 20,7 \cdot 10^3$ м. Причому при готовності самохідної вогневої одиниці (бойової машини) № 1 маємо: $D_{дпо} \approx 83,3 \cdot 10^3$ м та $D_{бпо} \approx 62,6 \cdot 10^3$ м.

Відмічаємо достатньо значні дальності рубежів постановки вогневих завдань та меж повітряної обстановки при лише завадах середньої щільності та роботі по ТЦ.

2. Відношення сигнал/шум (с/ш) у радіолокаційному каналі РЛС старшого начальника та імовірності вірного виявлення цілей у різноманітних умовах застосування [4, 6-8].

В якості технічних характеристик РЛС старшого начальника обрали умовні характеристики евентуальної РЛС, наближені до характеристик РЛС П-18. Відношення с/ш $q_b(D, \sigma, \Delta)$ і імовірності вірного виявлення $P_b(D, \sigma, \Delta)$ при дії активних шумових перешкод (АШП) дорівнюють:

$$q_b(D, \sigma, \Delta) = \sqrt{(2,016 \cdot 10^{20} \sigma) / [D^4 (1 + \Delta)]},$$

$$P_b(D, \sigma, \Delta) = F\{1 / [1 + 0,5 q_b(D, \sigma, \Delta)^2]\}, \quad (2)$$

- де σ, D – відповідно ЕПР цілі (ЕПР ТЦ $\sigma_{ТЦ} = 1$ м²) та дальність до неї;
- Δ – відношення потужності АШП до потужності власних шумів радіолокаційного (РЛ) каналу РЛС, які залишилися після відповідної компенсації (для середньої щільності $\Delta = 7$ дБ (5 разів));
- F – фіксований рівень помилкової тривоги РЛ каналу (обрали $\sim 10^{-2}$).

Одержали $q_b(65 \cdot 10^3; 1; 0) \approx 3,36$ рази, $q_b(65 \cdot 10^3; 1; 5) \approx 1,37$ рази і відповідно $P_b(65 \cdot 10^3; 1; 0) = 0,5$ і $P_b(65 \cdot 10^3; 1; 5) \approx 0,1$. Результати розрахунків за виразами (1), (2) приведені на рис. 1.

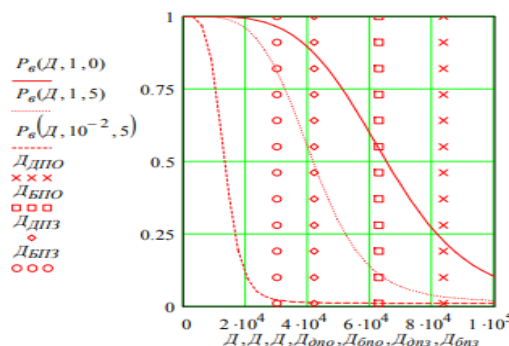


Рисунок 1 – Імовірності вірного виявлення $P_b(D, \sigma, \Delta)$ та меж зон повітряної обстановки $D_{дпо}$, $D_{бпо}$ і рубежі постановки вогневих завдань $D_{дпз}$ і $D_{бпз}$

Джерело: розроблено авторами

Перша крива $P_{B1}(D)$ позначена безперервною лінією, побудована при роботі по ТЦ і відсутності перешкод. Друга крива $P_{B2}(D)$ (точки) відображає значення імовірностей виявлення ТЦ при наявності АШП середньої щільності ($\Delta = 5$ разів). Третя крива $P_{B3}(D)$ (тире) отримана для випадку виявлення безпілотного літального апарату (БПЛА) на фоні перешкод $\Delta = 5$ разів. Четверта ($\times \times \times$) та п'ята ($\square \square \square$) прямі показують відповідно дальню $D_{ДПО}$ і ближню $D_{БПО}$ межі зон повітряної обстановки. Шоста ($\diamond \diamond \diamond$) та сьома ($\circ \circ \circ$) прямі відображають дальній $D_{ДПЗ}$ і ближній $D_{БПЗ}$ рубежі постановки вогневих завдань. При прийнятих технічних характеристиках РЛС старшого начальника на $D_{ДПО}$ маємо $P_B(83,3 \cdot 10^3; 1; 5) \approx 0,03$, а на $D_{БПО}$ $P_B(62,6 \cdot 10^3; 1; 5) \approx 0,11$, що не уможливорює проведення централізованого ЦР (ЦЦР) у підрозділі. Внаслідок цього застосовується не ЦЦР, а децентралізований ЦР (ДЦР). Лише на $D_{ДПЗ}$ отримали $P_B(41,9 \cdot 10^3; 1; 5) \approx 0,49$, що теж не задовольняє. При роботі по БПЛА (третя крива, рис. 1) самохідні вогневі одиниці (бойові машини) в змозі проводити стрільбу по цілях, які раптово з'являються. В цілому відмітимо не значний енергетичний потенціал РЛС старшого начальника та її перешкодостійкість.

3. Імовірності входу цілей в зони ЦР у різноманітних умовах [1, 2, 6, 7].

Визначення ймовірностей входу в зони ЦР передбачає розрахунок: а) середнє квадратичне відхилення (СКВ) помилки вимірювання азимуту цілі при відсутності викривлень пачки при флуктуації корисних сигналів $\sigma_B(D, \sigma, \Delta)$; б) часу $\tau_1(n)$ між n відмітками по цілі при огляду простору РЛС старшого начальника 6 об/хв.; в) СКВ помилки параметру цілі $\sigma_p(D, \sigma, \Delta, n, V)$. Так:

$$\begin{aligned}\sigma_B(D, \sigma, \Delta) &= \frac{\sqrt{\pi} \Theta}{q_B(D, \sigma, \Delta) 180}, \\ \tau_1(n) &= n(60/6), \\ \sigma_p(D, \sigma, \Delta, n, V) &= \frac{\sqrt{2} \sigma_B(D, \sigma, \Delta)}{(n-1)V\tau_1(n)} \cdot \\ &\quad \left[D - \frac{(n-1)V\tau_1(n)}{2} \right]^2, \end{aligned} \quad (3)$$

де Θ – напівширина діаграми спрямованості антени РЛС старшого начальника (прийняли 6°).

Також потрібно знайти граничний параметр цілі $P(V, H)$ для пари двох самохідних вогневих одиниць (бойових машинах) (наприклад відстань між ними ~ 3 км), СКВ помилки лінійного відхилення цілі $\sigma_\eta(V, H)$ і СКВ помилки щільності імовірності входу цілі у зону ЦР $\sigma_{Bx}(D, \sigma, \Delta, n, V, H)$.

$$\begin{aligned}P(V, H) &= 2 \cdot 10^3 + \sqrt{(8,7 \cdot 10^3 - 8V)^2 - H^2}, \\ \sigma_\eta(V, H) &= \left[\frac{2P(V, H)}{6} \right], \\ \sigma_{Bx}(D, \sigma, \Delta, n, V, H) &= [\sigma_p(D, \sigma, \Delta, n, V)^2 + \sigma_\eta(V, H)^2]^{0,5}. \end{aligned} \quad (4)$$

У підсумку значення ймовірностей входу цілей у зони ЦР знаходимо з виразу:

$$\Psi_{Bx}(D, \sigma, \Delta, n, V, H, P) = \int_{-P(V, H)}^{P(V, H)} \left\{ \frac{\exp\left[-\frac{(Z-P)^2}{2\sigma_{Bx}(D, \sigma, \Delta, n, V, H)^2}\right]}{\sqrt{2\pi} \sigma_{Bx}(D, \sigma, \Delta, n, V, H)} \right\} dZ, \quad (5)$$

де P – параметр повітряної цілі.

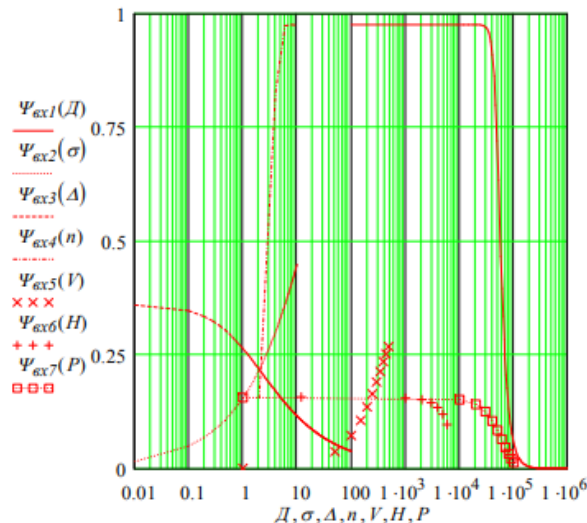


Рисунок 2 – Імовірності входу цілей в зони ЦР (ЗПу) $\Psi_{\text{вх}}(D, \sigma, \Delta, n, V, H, P)$ при зміні $D, \sigma, \Delta, n, V, H$ та P

Джерело: розроблено авторами

Результати розрахунку за виразами (3) – (5) приведені на рис. 2 для $D_{\text{БПО}}$ у 62,6 км. Перша крива $\Psi_{\text{вх}1}(D)$ (безперервна) побудована при $\sigma = 1 \text{ м}^2$, $\Delta = 0$, $n = 2$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$. Друга крива $\Psi_{\text{вх}2}(\sigma)$ (точки, $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\Delta = 0$, $n = 2$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$) відображає значення ймовірностей входу цілей у зону ЦР при зміні їх ЕПР σ . Низькі ймовірності входу, за другою кривою, пов'язані з не виявленням даних цілей РЛС старшого начальника. Вплив перешкод Δ і тривалість спостереження за ТЦ представлені відповідно третьою $\Psi_{\text{вх}3}(\Delta)$ (тире) та четвертою $\Psi_{\text{вх}4}(n)$ (точки і тире) кривими. Перешкоди Δ не дають можливостей своєчасно виявляти ТЦ, хоча при $n \geq 3$ якісно вимірюється РЛС параметр цілі. Третя крива здобута, якщо $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $n = 2$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$, а четверта – $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$. П'ята крива $\Psi_{\text{вх}5}(V)$ ($\times \times \times$), шоста $\Psi_{\text{вх}6}(H)$ ($++$) та сьома $\Psi_{\text{вх}7}(P)$ ($\square \square \square$) криві показують зміну ймовірностей входу на $D_{\text{БПО}}$ залежно від V, H і P . Вхідні данні для $\Psi_{\text{вх}5}(V)$ ($\times \times \times$) $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $n = 2$, $H = 10^3 \text{ м}$, $P = 3 \cdot 10^3 \text{ м}$, а для кривої шостої $\Psi_{\text{вх}6}(H)$ ($++$) – $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $n = 2$, $V = 230 \text{ м/с}$, $P = 3 \cdot 10^3 \text{ м}$ та для сьомої $\Psi_{\text{вх}7}(P)$ ($\square \square \square$) – $D_{\text{БПО}} = 62,6 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $n = 2$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$. З останніх трьох кривих слідує недостатні ймовірності входу ТЦ, що ускладнює проведення ЦР у підрозділі. Треба відмітити покращення результатів чисельного моделювання значень ймовірностей коли $D_{\text{ДПЗ}}$ дорівнює 41,9 км. Тобто при відпрацюванні цілевказівки (ЦВ) особовим складам (о/с) самохідної вогневої одиниці (бойової машини) ймовірніша стрільба буде проведена. Так $\Psi_{\text{вх}}(62,6 \cdot 10^3; 1; 5; 2; 230; 10^3; 3 \cdot 10^3) \approx 0,16$ і $\Psi_{\text{вх}}(41,9 \cdot 10^3; 1; 5; 2; 230; 10^3; 3 \cdot 10^3) \approx 0,64$.

4. Імовірності не виходу цілей в ЗПу та ЗУ комплексу, після пуску ракет, при стрільбі по цілі, яка маневрує [1-4, 6-9].

Відношення с/ш у РЛ каналі станції супроводження цілей (ССЦ) самохідної вогневої одиниці (бойової машини) на дальній межі ЗПу (ДМЗПу) $q_c(D, \sigma, \Delta)$, СКВ помилки вимірювання азимуту цілі $\sigma_{\text{БС}}(D, \sigma, \Delta)$ ССЦ та кількість луно – сигналів k_i по даній цілі на ДМЗПу дорівнює:

$$q_c(D, \sigma, \Delta) = \sqrt{(1,434 \cdot 10^{20} \sigma) / [D^4 (1 + \Delta)]},$$

$$\sigma_{\beta c}(D, \sigma, \Delta) = \frac{\sqrt{\pi} \Theta_c}{q_c(D, \sigma, \Delta) 180}, \quad k_i = \tau_k T^{-1}, \quad (6)$$

де Θ_c, τ_k – відповідно напівширина діаграми спрямованості (ДС) антени станції супроводження цілі (ССЦ) самохідної вогневої одиниці (бойової машини) (обрали $1,23^\circ$) та const контуру управління (прийняли $\sim 0,8$ с);
 T – період слідування радіоімпульсів ССЦ (взяли 390 мкс).

СКВ помилки виміру азимуту цілі, яка проводить односторонній коловий віраж у горизонтальній площині польоту без зміни $V \sigma_m(n_{\text{ц}}, V)$, СКВ помилки параметру цілі $\sigma_{\text{рм}}(D, \sigma, \Delta, n_{\text{ц}}, V)$, СКВ помилки щільності імовірності не виходу цілі з ЗПу (ЗУ) комплексу, а $P(V, H)$ і $\sigma_{\eta}(V, H)$ находимо з виразів (4), так:

$$\sigma_m(n_{\text{ц}}, V) = (\tau_k n_{\text{ц}} g) / (3V),$$

$$\sigma_{\text{рм}}(D, \sigma, \Delta, n_{\text{ц}}, V) = \frac{\sqrt{2} [\sigma_{\beta c}(D, \sigma, \Delta) + \sigma_m(n_{\text{ц}}, V)]}{(k_i - 1) V T} \cdot \left[D - \frac{(k_i - 1) V T}{2} \right]^2, \quad (7)$$

$$\sigma_{\text{вм}}(D, \sigma, \Delta, n_{\text{ц}}, V, H) = [\sigma_{\text{рм}}(D, \sigma, \Delta, n_{\text{ц}}, V)^2 + \sigma_{\eta}(V, H)^2]^{0,5},$$

де $n_{\text{ц}}$ – перевантаження ПЦ, з якими вона маневрує;
 g – прискорення вільного падіння ($\sim 9,81$ м/с²).

Для спрощення прийняли, що ДМЗПу комплексу $D \sim 15$ км. Безумовно бажано мати імовірності не виходу цілей з ЗПу (ЗУ), після пуску ракет, не менше 0,5, для отримання необхідної ефективності стрільби та УВ.

Значення ймовірностей не виходу цілей з ЗПу (ЗУ) комплексу після пуску ракети дорівнює:

$$\Psi_H(D, \sigma, \Delta, n_{\text{ц}}, V, H, P) =$$

$$= \int_{-P(V, H)}^{P(V, H)} \left\{ \frac{\exp \left[-\frac{(Z - P)^2}{2 \sigma_{\text{вм}}(D, \sigma, \Delta, n, V, H)^2} \right]}{\sqrt{2} \pi \sigma_{\text{вм}}(D, \sigma, \Delta, n, V, H)} \right\} dZ. \quad (8)$$

За аналогією з результати на рис. 2 отримали значення, які приведені на рис. 3. Перша $\Psi_{\text{н1}}(D)$ (безперервна), друга $\Psi_{\text{н2}}(\sigma)$ (точки), третя $\Psi_{\text{н3}}(\Delta)$ (тире) криві показують значення імовірності, яка досліджується при різних D, σ і Δ . В цілому хід вказаних кривих задовольняє якості стрільби ракетами. Вхідні данні для $\Psi_{\text{н1}}(D)$ наступні: $\sigma = 1 \text{ м}^2$, $\Delta = 0$, $n_{\text{ц}} = 0$, $V = 230$ м/с, $H = 10^3$ м, $P = 3 \cdot 10^3$ м, а для кривої $\Psi_{\text{н2}}(\sigma)$ – $D = 15 \cdot 10^3$ м, $\Delta = 0$, $n_{\text{ц}} = 0$, $V = 230$ м/с, $H = 10^3$ м, $P = 3 \cdot 10^3$ м. Відповідно вхідні данні для $\Psi_{\text{н3}}(\Delta)$ і $\Psi_{\text{н4}}(n_{\text{ц}})$: $D = 15 \cdot 10^3$ м, $\sigma = 1 \text{ м}^2$, $n_{\text{ц}} = 0$, $V = 230$ м/с, $H = 10^3$ м, $P = 3 \cdot 10^3$ м та $D = 15 \cdot 10^3$ м, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $V = 230$ м/с, $H = 10^3$ м, $P = 3 \cdot 10^3$ м. Коли $n_{\text{ц}} \geq 1$ четверта крива $\Psi_{\text{н4}}(n_{\text{ц}})$ (точки і тире), п'ята $\Psi_{\text{н5}}(V)$ ($\cdot \times \cdot \times \cdot$), шоста $\Psi_{\text{н6}}(H)$ ($\square \cdot \square \cdot$) та сьома $\Psi_{\text{н7}}(P)$ ($\diamond \cdot \diamond \cdot$) криві надали малі значення не виходу цілі, при її маневруванні. Вхідні данні для $\Psi_{\text{н5}}(V)$: $D = 15 \cdot 10^3$ м, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $n_{\text{ц}} = 3$, $H = 10^3$ м, $P = 3 \cdot 10^3$ м, та для $\Psi_{\text{н6}}(H)$ – $D = 15 \cdot 10^3$ м,

$\sigma = 1 \text{ м}^2$, $\Delta = 5$, $n_{\text{ц}} = 3$, $V = 230 \text{ м/с}$, $P = 3 \cdot 10^3 \text{ м}$ і для $\Psi_{\text{н}7}(P) - \Delta = 15 \cdot 10^3 \text{ м}$, $\sigma = 1 \text{ м}^2$, $\Delta = 5$, $n_{\text{ц}} = 3$, $V = 230 \text{ м/с}$, $H = 10^3 \text{ м}$. Останнє вкрай негативно буде проявлятися при застосуванні озброєння. Треба відмітити, що на ДМЗПу комплексу $\Psi_{\text{н}}(15 \cdot 10^3; 1; 5; 3; 400; 10^3; 3 \cdot 10^3) \approx 0,27$, хоча на ДМЗУ – $\Psi_{\text{н}}(10^4; 1; 5; 3; 400; 10^3; 3 \cdot 10^3) \approx 0,56$.

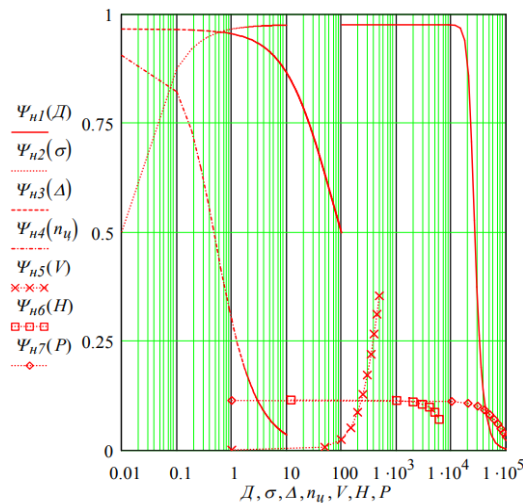


Рисунок 3 – Імовірності не виходу цілей з ЗПу (ЗУ) комплексу $\Psi_{\text{н}}(D, \sigma, \Delta, n_{\text{ц}}, V, H, P)$ у різних умовах застосування

Джерело: розроблено авторами

5. Визначення першого роду помилок стрільби ракетами, а саме імовірності проходження ракети у “трубці” радіусу ρ [1 – 5, 10 – 13].

Розрахунок значень систематичної складової помилок наведення ракет (ПНР) $m_{\text{н}}(n_{\text{ц}})$ та СКВ ПНР $\sigma_{\text{н}}(\Delta)$ залежно від точки зустрічі ракети з ціллю (ТЗРЦ) у ЗУ комплексу.

Перший вираз в (9) показує зростання систематичної складової ПНР при маневруванні цілі, коли $v_{\text{н}}(n_{\text{ц}}, t) \geq 0$. Другий вираз $t_1(n_{\text{ц}})$ вказує на час коли $v_{\text{н}}(n_{\text{ц}}, t) = 0$, а третій вираз $m_{\text{с}}(n_{\text{ц}})$ – середнє значення систематичної складової ПНР.

$$v_{\text{н}}(n_{\text{ц}}, t) \approx \begin{cases} 0,5n_{\text{ц}}g \left\{ t^2 - \left[\frac{n_{\text{п}}}{n_{\text{ц}}} (t - \tau_{\text{к}})^2 \right] \right\}, & t \geq \tau_{\text{к}}, \\ 0,5n_{\text{ц}}gt^2, & t < \tau_{\text{к}}, \end{cases}$$

$$t_1(n_{\text{ц}}) = \tau_{\text{к}} \left(1 - \frac{n_{\text{п}}}{n_{\text{ц}}} \right)^{-1},$$

$$m_{\text{с}}(n_{\text{ц}}) = \frac{1}{t_1(n_{\text{ц}})} \int_0^{t_1(n_{\text{ц}})} v_{\text{н}}(n_{\text{ц}}, t) dt,$$

$$m_{\text{н}}(n_{\text{ц}}) = \{ (0,87r_{\text{д}}10^{-4})^2 + [0,87r_{\text{д}}10^{-4} + m_{\text{с}}(n_{\text{ц}})]^2 \}^{0,5}. \quad (9)$$

де $n_{\text{п}}, t$ – відповідно перевантаження ракети у ТЗРЦ та час від початку маневру цілі до ТЗРЦ;

$m_{\text{с}}(n_{\text{ц}})$ – усереднене значення систематичної складової ПНР при маневруванні цілі;

$r_{\text{д}}$ – похила дальність до ДМЗУ комплексу (прийняли 10^4 м).

За виразами (9) отримали: $m_{\text{с}}(3) \approx 5,7 \text{ м}$, $m_{\text{с}}(5) \approx 12,4 \text{ м}$ та $m_{\text{н}}(3) \approx 6,6 \text{ м}$, $m_{\text{н}}(5) \approx 13,3 \text{ м}$, хоча без маневру – $m_{\text{н}}(0) \approx 1,2 \text{ м}$. Значення $m_{\text{н}}(5)$ у $\sim 13 \text{ м}$ сумірні з відстанню де стійко спрацьовує радіопідричник (РП) ракети.

Вважають, що при дії АШП зростає лише флуктуаційна складова ПНР $\sigma_{\phi z}(\Delta)$ [1, 3] та СКВ ПНР находимо залежно від дальності до ТЗРЦ, так:

$$\begin{aligned}\sigma_{\phi z}(\Delta) &= \sigma_{\phi z} 10^{\Delta/20}, \\ \sigma_H(\Delta) &= \sqrt{\sigma_{dz}^2 + \sigma_{iz}^2 + \sigma_{\phi z}(\Delta)^2}, \\ \sigma_H(\Delta) &= r_d \operatorname{tg} \{ [\sigma_H(\Delta) \pi] / (180 \cdot 60) \},\end{aligned}\quad (10)$$

де $\sigma_{dz}, \sigma_{iz}, \sigma_{\phi z}$ – відповідно динамічна, інструментальна та флуктуаційна складові ПНР (прийняли усереднені значення $\sigma_{dz} \approx 1,9$ кутових хвилин (кут. хв.), $\sigma_{iz} \approx 0,4$ кут. хв., $\sigma_{\phi z} \approx 1,3$ кут. хв.), причому завжди $\sigma_H(\Delta) \geq 3$ м.

За виразами (10) маємо: $\sigma_H(0) \approx 6,8$ м і $\sigma_H(5) \approx 8,8$ м. Результати розрахунку систематичної складової ПНР $m_H(n_u)$ та СКВ ПНР $\sigma_H(\Delta)$ приведені на рис. 4. Перша крива залежно $m_H(n_u)$ (безперервна) побудована, якщо перевантаження цілі n_u змінюються до $10g$. Друга крива $\sigma_H(\Delta)$ (точки) отримана при практично відсутності АШП та її наявності до рівня щільності переважної перешкоди ($\Delta = 10^2$ разів).

Відмітимо суттєве зростання складових ПНР при протидії стрільбі у вигляді маневрування цілі та дії перешкод. Вказане приводить до зниження ефективності бойового застосування комплексу.

Імовірності проходження ракети у "трубці" радіусу ρ $P(\rho, \Delta, n_u)$ дорівнює:

$$\begin{aligned}P(\rho, \Delta, n_u) &= \\ &= \int_0^\rho \left\{ \frac{\rho \exp \left\{ -\frac{\rho^2 + m_H(n_u)^2}{2\sigma_H^2(\Delta)} \right\} I_0 \left[\frac{\rho^2 m_H(n_u)}{\sigma_H^2(\Delta)} \right]}{\sigma_H^2(\Delta)} \right\} d\rho.\end{aligned}\quad (11)$$

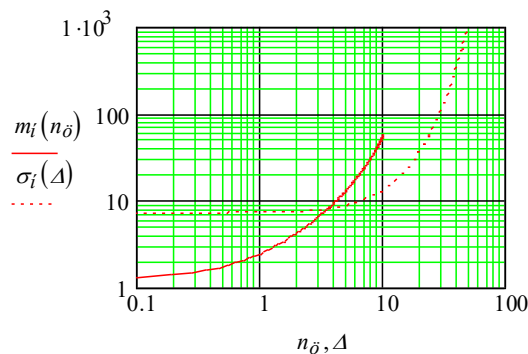


Рисунок 4 – Систематичної складової ПНР $m_H(n_u)$ та СКВ ПНР $\sigma_H(\Delta)$ залежно від перевантажень цілі n_u та рівня перешкод Δ

Джерело: розроблено авторами

Результати обчислень наведені на рис. 5. Перша крива $P(\rho, 0, 0)$ (безперервна) побудована при роботі по ТЦ і відсутності маневру цілі та перешкод.

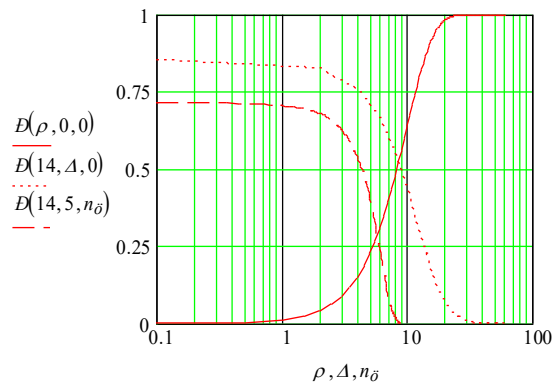


Рисунок 5 – Імовірності проходження ракети у “трубці” радіусу ρ $P(\rho, \Delta, n_\delta)$ залежно від промаху ракети ρ , рівня перешкод Δ та перевантажень цілі n_δ

Джерело: розроблено авторами

Друга крива $P(14, \Delta, 0)$ (точки) та третя $P(14, 5, n_\delta)$ (тире) відповідно розраховані для випадків дії АШП та маневруванні ТЦ на фоні перешкод середньої щільності ($\Delta = 5$ разів).

Вплив АШП та маневрування цілі знижує імовірності проходження ракет у “трубці” радіусу стійкого спрацювання РЗ ($\rho = 14$ м), отримали: $P(14; 0; 0) \approx 0,9$ та $P(14; 5; 0) \approx 0,7$ і $P(14; 5; 3) \approx 0,6$.

6. Визначення другого роду помилок стрільби ракетами, а саме імовірності спрацювання РП (системи підриву БЧ ракети) [1-3, 6-13].

Вводимо апроксимацію ширини ДС приймальної антени РП $\theta(\rho)$ [2, 9, 10] та знаходимо СКВ помилок РП ракети $\sigma_p(\rho)$ і математичне сподівання (МС) випадкової величини радіусу спрацювання РП ракети $m_p(\sigma)$.

На основі аналізу скалярного поля дифракції Френеля – Кірхгофа отримали наступне:

$$\begin{aligned} \theta(\rho) &= 0,5 \left\langle 0,0074 + 0,611 \left\{ 1 - e^{-[1,33 \sin(\varepsilon_a)/\rho]} \right\} \right\rangle, \\ \sigma_p(\rho) &= \frac{\rho \sin[\theta(\rho)]}{3 \sin(\varepsilon_a)} \left\{ \frac{1}{\sin[2,531 - \theta(\rho)]} + \frac{1}{\sin[0,611 - \theta(\rho)]} \right\}, \\ m_p(\sigma) &= \begin{cases} \rho_{\max} \sqrt[4]{\sigma/\sigma_{\text{ТЦ}}}, & \sigma \geq 0,1 \text{ м}^2, \\ \sqrt[3]{\frac{\rho_{\max}^4 \sigma \lambda}{\sigma_{\text{ТЦ}} L^2 \sin(\varepsilon_a + 3\sigma_{\varepsilon a})}}, & \sigma < 0,1 \text{ м}^2, \end{cases} \end{aligned} \quad (12)$$

- де ε_a – кут нахилу приймальної антени РП ракети (прийняли $\sim 1,05$ рад.);
 $\rho_{\max}$ – найбільший промах ракети коли РП спрацює з імовірністю 0,5 при роботі по ТЦ ($\rho \sim 15,5$ м);
 λ, L – довжина хвилі РП ракети ($\sim 0,03$ м) та довжина її приймальної антени ($\sim 0,6$ м) відповідно;
 $\sigma_{\varepsilon a}$ – СКВ помилки спрацювання РП ракети ($\sim 0,062$ рад.).

Результати числового моделювання наведені на рис. 6. Перша крива $\sigma_p(\rho)$ (безперервна) побудована при роботі по ТЦ. Друга крива $m_p(\sigma)$ (точки) вказує на лінійне зростання МС випадкової величини радіусу спрацювання РП, при збільшенні ЕПР цілі, по якій здійснюється обстріл.

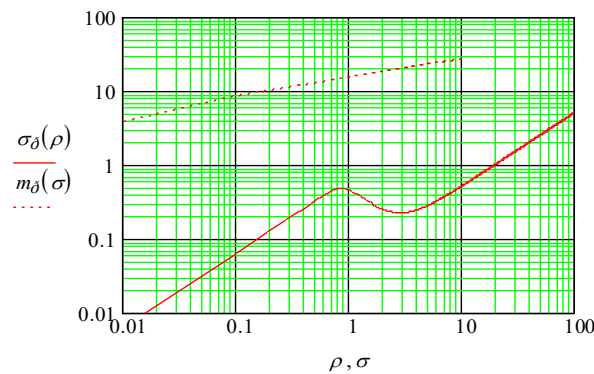


Рисунок 6 – Середнє квадратичне відхилення помилок радіопідричника ракети $\sigma_p(\rho)$ та математичного сподівання випадкової величини радіусу спрацювання радіопідричника ракети $m_p(\sigma)$ залежно від промаху ракети ρ та ефективної поверхні розсіювання цілі σ

Джерело: розроблено авторами

Одержали $m_p(1) = 15,5$ м та $m_p(10^{-2}) = 3,9$ м.

Імовірності спрацювання РП $P_{сп}(\rho, \sigma, k)$ – другий рід помилок стрільби ракетами.

$$P_{сп}(\rho, \sigma, k) = 1 - \text{snorm}\left[\frac{\rho - m_p(\sigma)}{k\sigma_p(\rho)}\right], \quad (13)$$

де $\text{snorm}[Z]$ – функція розподілу нормального та центрованого нормального розподілення у середовищі MathCAD;

k – рівень перешкод по РЛ каналу РП ракети (без перешкод $k = 1$, перешкоди слабкої щільності $k = 2$ рази, середньої – $k = 5$ разів, сильної – $k = 16$ разів та щільності перешкоди, що подавляє – $k = 10^2$ разів).

Підсумки розрахунків за виразами (12), (13) приведені на рис. 7. Перша крива $P_{сп}(\rho, 10^{-2}, 1)$ (безперервна) та друга крива $P_{сп}(\rho, 10^{-2}, 10^2)$ (точки) розраховані при обстрілі малорозмірної цілі ($\sigma = 10^{-2} \text{ м}^2$) при відсутності та наявності АШП щільності перешкоди, що подавляє по РЛ каналу РП ракети відповідно.

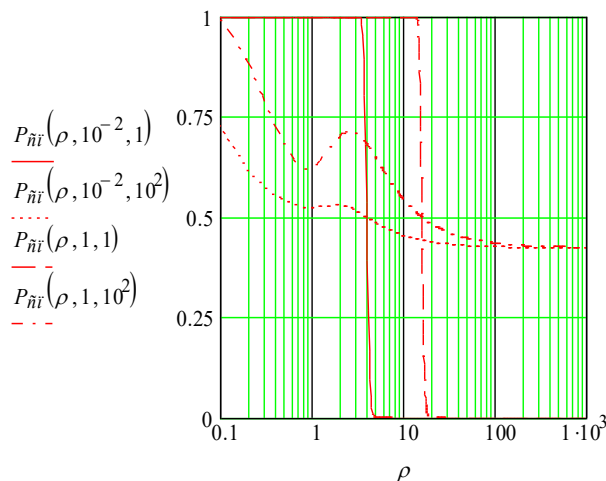


Рисунок 7 – Імовірності спрацювання радіопідричника ракети $P_{сп}(\rho, \sigma, k)$ залежно від промаху ракети ρ

Джерело: розроблено авторами

Третя крива $P_{сп}(\rho, 1, 1)$ (тире) та четверта крива $P_{сп}(\rho, 1, 10^2)$ (точки і тире) отримані для тих же самих умов, що і попередні, але при роботі по ТЦ ($\sigma_{ТЦ} = 1 \text{ м}^2$). Одержали $P_{сп}(15,5;1;0) =$

0,5 та надвеликі відстані спрацювання РП, коли цілі не будуть уражені вузьким потоком осколків бойової частини ракети. Так при АШП сильної щільності $P_{сп}(40; 1; 16) \approx 0,23$ та $P_{сп}(10^2; 1; 10^2) \approx 0,44$. Дане підтверджує необхідність забезпечення необхідної завадостійкості РЛ каналу радіопідривника ракети.

7. Розрахунок колового закону ураження ТЦ та умовних ймовірностей ураження різних цілей при стрільбі двома ракетами [1-3, 9, 12, 13].

Значення колового закону ураження ТЦ $G(\rho)$ та умовні ймовірності ураження різних цілей при стрільбі двома ракетами $R_2(\rho, D, \sigma, \Delta, n_{ц}, V, H, P, k)$ у різноманітних умовах бойового застосування визначаємо з наступних виразів:

$$\begin{aligned} G(\rho) &= \exp(-\rho^2 / \beta_0^2), \\ R_2(\rho, D, \sigma, \Delta, n_{ц}, V, H, P, k) &= \\ &= \Psi_H(D, \sigma, \Delta, n_{ц}, V, H, P) \cdot \\ &\cdot \left\{ 1 - [1 - P(\rho, \Delta, n_{ц}) P_{сп}(\rho, \sigma, k)]^2 \right\}, \end{aligned} \quad (14)$$

де β_0 – параметр колового закону ураження ТЦ з врахуванням механічної, запалювальної та ініційованої дії осколків БЧ ракети (прийняли ~ 21 м).

За першим виразом (14) отримали при середньому промаху ракети $G(6) \approx 0,92$ та з СКВ промаху ракети $G(9) \approx 0,83$. При підриві БЧ ракети під впливом АШП ураження ТЦ не можливо – $G(50) \approx 3,4 \cdot 10^{-3}$. Зміна значень $G(\rho)$ показана першою, безперервною кривою на рис. 8.

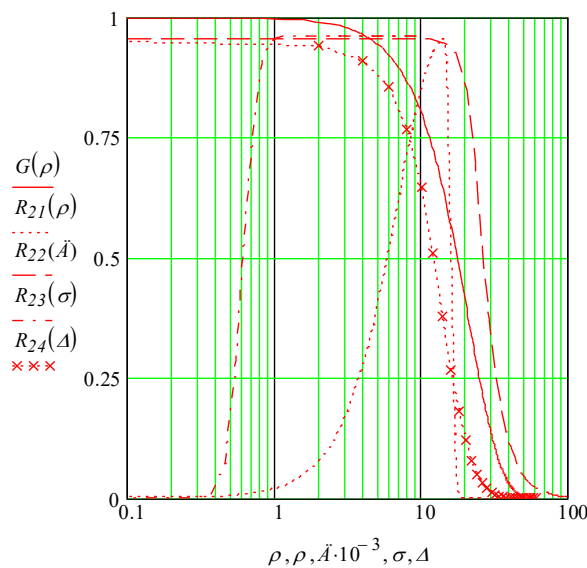


Рисунок 8 – Коловий закону ураження типової цілі $G(\rho)$ та умовні ймовірності ураження цілей R_{2ij} при стрільбі двома ракетами

Джерело: розроблено авторами

Друга крива $R_{21}(\rho)$ (точки) та третя крива $R_{22}(\Delta)$ (тире) відображають значення умовних ймовірностей ураження цілей при зміні ρ та Δ відповідно. Причому $R_{21}(14)$ дорівнює на ДМЗУ комплексу $R_2(14; 10^4; 1; 0; 0; 230; 10^3; 3 \cdot 10^3; 1) \approx 0,96$, коли ймовірність входу цілі на ДБПО (позначимо через $\Psi_{вх\ БПО}$) лише $\sim 0,36$ і ймовірності вірного виявлення РЛС старшого начальника (позначимо через $P_{в\ БПО}$) $\sim 0,54$. На $\Delta_{ДПЗ}$ результати кращі – $\Psi_{вх\ ДПЗ} \sim 0,89$ і $P_{в\ ДПЗ} \sim 0,87$. Значення для третьої кривої $\Psi_{вх\ БПО}$, $P_{в\ БПО}$, $\Psi_{вх\ ДПЗ}$ та $P_{в\ ДПЗ}$ ті самі, що і для другої кривої. Для кращої візуалізації результатів моделювання величина Δ , за віссю абсцис, зменшена у 10^3 .

разів. Четверта крива $R_{24}(\sigma)$ (точки і тире) та п'ята $R_{25}(\Delta)$ ($\cdot \times \cdot$) показують значення умовних ймовірностей ураження цілей при зміні σ і Δ відповідно. Розрахунки надали на ДМЗУ $R_2(14;10^4;0,5;0;0;230;10^3;3 \cdot 10^3;1) \approx 0,15$, при $\Psi_{\text{вх БПО}} \sim 0,26$ і $P_{\text{в БПО}} \sim 0,34$, або малорозмірна ціль може і не вийти на $D_{\text{БПО}}$, не буде охоплена ЦР. На $D_{\text{ДПЗ}}$ маємо $\Psi_{\text{вх БПО}} \sim 0,82$ і $P_{\text{в БПО}} \sim 0,77$. При роботі по ТЦ на рівні АСП середньої щільності отримали $R_2(14;10^4;0,5;0;0;230;10^3;3 \cdot 10^3;1) \approx 0,89$, коли $\Psi_{\text{вх БПО}}$ лише $\sim 0,16$ і $P_{\text{в БПО}} \sim 0,11$. Тобто ЦЦР у підрозділі не реалізується, залишається ДЦР, так як недостатня $P_{\text{в БПО}}$ РЛС старшого начальника.

Вплив маневру ТЦ показано кривою $R_{25}(n_u)$ (тире) на рис. 9.

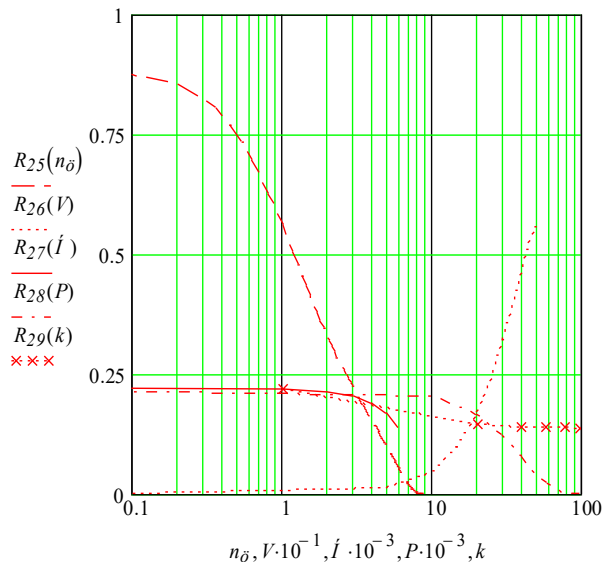


Рисунок 9 – Умовні ймовірності ураження цілей R_{2ij} при стрільбі ракетами у різних умовах застосування

Джерело: розроблено авторами

Перевантаження цілі у $n_u = 3$ надали $R_2(14;10^4;1;5;3;230;10^3;3 \cdot 10^3;1) \approx 0,22$, коли $\Psi_{\text{вх БПО}} \sim 0,16$ і $P_{\text{в БПО}} \sim 0,11$. При цьому знижується, від попереднього, ймовірність не виходу ТЦ з ЗУ комплексу (позначимо через $\Psi_{\text{нЗУ}}$) з $\sim 0,97$ до $\sim 0,26$. Тобто ТЦ в змозі покинути ЗУ комплексу. Друга крива $R_{26}(V)$ (точки) та третя $R_{27}(H)$ (безперервна) надають значення умовних ймовірностей ураження цілей при зміні V та H відповідно. Для кращої візуалізації розрахунків на рис. 9 значення V , за віссю абсцис, зменшена у 10 разів, а величини H і P зменшили у 10^3 разів. За другою кривою збільшення V до 400 м/с приводе до підвищення $\Psi_{\text{вх БПО}} \sim 0,16$ до $\sim 0,24$, а також поліпшується $\Psi_{\text{нЗУ}}$ з $\sim 0,26$ до $\sim 0,56$. При цьому покращуються умовні ймовірності ураження з $\sim 0,22$ до $\sim 0,48$, так $R_2(14;10^4;1;5;3;400;10^3;3 \cdot 10^3;1) = 0,476$. Останнє пояснюється зменшенням часу на входження цілі на $D_{\text{БПО}}$ і можливим не виходом з ЗУ комплексу. При підвищенні H до 5 км отримали зниження ефективності ЦР і стрільби двома ракетами – $R_2(14;10^4;1;5;3;230;5 \cdot 10^3;3 \cdot 10^3;1) \approx 0,17$, при $\Psi_{\text{вх БПО}} \sim 0,12$, $P_{\text{в БПО}} \sim 0,11$ та $\Psi_{\text{нЗУ}}$ лише $\sim 0,2$. Четверта крива $R_{28}(P)$ (точки і тире) та п'ята крива $R_{29}(k)$ ($\cdot \times \cdot$) приведені для різних P та k . Наприклад коли $P \sim 2 \cdot 10^4$ м то умовна ймовірність ураження дорівнює $R_2(14;10^4;1;5;3;230;10^3;2 \cdot 10^4;1) \approx 0,17$ і $\Psi_{\text{вх БПО}} \sim 0,14$ та $\Psi_{\text{нЗУ}} \sim 0,2$. Залишається можливість стрільби по цілям, які раптово з'являються і ДЦР у підрозділі. Перешкоди середньої щільності по РЛ каналу РП ракети знижують умовні ймовірності ураження (п'ята крива) до $R_2(14;10^4;1;5;3;230;10^3;3 \cdot 10^3;5) \approx 0,17$. При цьому $\Psi_{\text{вх БПО}}$, $P_{\text{в БПО}}$ та $\Psi_{\text{нЗУ}}$ такі самі, що і для випадку першої кривої на рис. 9.

Отримані показники ефективності стрільби і УВ у різноманітних умовах з врахуванням

значень ймовірностей входу цілей у зону ЦР. Показані межі застосування ЦЦР у підрозділі, та обмеження, які зв'язані, з величинами ймовірностей вірного виявлення РЛС старшого начальника. Показано необхідність поліпшення енергетичного потенціалу РЛС та підвищення її перешкодостійкості [8, 12, 13]. Оптимізація системи УВ, впровадження мульті радарних систем виявлення та шумові радары [14-19] покращать показники ефективності стрільби ракетами.

Висновки

Таким чином, на основі існуючих технічних характеристик системи УВ знайдені рубежі постановки вогневих завдань і межі повітряної обстановки. Проведено порівняння рубежів та меж з відповідними ймовірностями вірного виявлення РЛС старшого начальника. Визначенні умови при яких вони відповідають вимогам до ЦР. Здобуті значення умовних ймовірностей ураження різних цілей з означеними величинами ймовірностей входу цілей в зони ЦР. Останнє не є достатнім, що може привести до хибного ЦР у підрозділі. Враховані ймовірності не виходу цілей з зон пуску та ураження комплексу при маневруванні цілей. Означені межі впровадження ЦЦР і ДЦР у підрозділі. В цілому приведена залежність величин умовних ймовірностей ураження цілей від дев'яти основних параметрів, які описують стрільбу ракетами та УВ. Отримані практичні результати часткової моделі необхідні для ефективного застосування озброєння за призначенням.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Основы стрельбы и управления огнем войсковых зенитных ракетных комплексов. Часть 1. Казачинский В.З., Каипецкий А.А., Нестеренко Л.Г., Семенов Г.В., Солодовников Н.Д. – К.: КВАИУ, 1971. – 468с.
2. Основы стрільби та керування вогнем: навч. посіб. /В.Є. Кудряшов, С.Г. Леушин, В.І. Самоквіт. – Х. : ХУПС, 2016. – 232 с.
3. Пушкорис В. П. Управление огнем войск ПВО Сухопутных войск: Учебник. – К.:ВА ПВО СВ, 1989. – 556 с.
4. A private model for determining the efficiency of target distribution / М.С. Пискунов., В.Є. Кудряшов, В.Є., Філіппенков О.В. // Системи озброєння і військова техніка. – Х.: ХНУПС, 2021. – Вип. 1 (65) – С. 107 – 113.
5. Довідник з протиповітряної оборони. Торопчин А.Я., Романенко І.О., Даник Ю.Г., Пашенко Р.Е. та ін. – К.: МО України, Х.: 2003. – 368 с.
6. Модель протиповітряного бою як елемент системи управління вогнем підрозділами військ ППО Сухопутних військ/ О. В. Коломійцев, В. Є. Кудряшов, В.В. Машталір, П. В. Опенько, Р. М. Олійник // Збірник наукових праць ДНДІ ВС озброєння та військової техніки. – Чернівці: ДНДІ ВС ОБТ. – 2019. – Вип. № 1(1). – С. 94-101.
7. Теория и техника обработки радиолокационной информации на фоне помех / Ширман Я.Д., Манжос В.Н. – М.; Радио и связь, 1981. – 416с.
8. Радиоэлектронные системы: Основы построения и теория. Справочник. Изд. 2 – е, перераб. и доп. / Под. ред. Я. Д. Ширмана. – М.: Радиотехника, 2007. 512с.
9. Справочник по радиолокации/ под общей ред. К.Н. Трофимова. Том 1. Основы радиолокации. Под ред. Я.С. Ицхоки: – М.: Сов. радио, 1976. – 456 с.

10. Другий рід помилок стрільби ракетами по нетиповим цілям ЗРК малої дальності / О.В. Коломійцев, В.Є. Кудряшов, І.Я. Загоруйко, С.С. Ворошилов // Збірник наукових праць ХУ ПС. – Х.: ХУ ПС. – 2011.- Вип. 1(27) – С. 86 – 90.
11. Умовна імовірність ураження нетипової цілі ЗРК малої дальності / О.В. Коломійцев, В.Є. Кудряшов, І.Я. Загоруйко, С.С. Ворошилов // Збірник наукових праць ХУ ПС. – Х.: ХУ ПС. – 2012.- Вип. 2(30) – С. 170 – 174.
12. Кудряшов В.Є., Литовченко Д.М. Чисельне моделювання з основ стрільби ракетами та управління вогнем комплексів малої дальності: навч. посіб. Х. : ХНУПС, 2023. – 533 с.
13. Литовченко Д.М., Кудряшов В.Є. Чисельне моделювання з основ стрільби озброєння ближньої дії та інформаційного забезпечення військ: навч. посіб. Х. : ХНУПС, 2025. – 268 с.
14. Піскунов С.М. Перспективна структура системи управління силами і засобами протиповітряної оборони Сухопутних військ Збірник наукових праць ХУПС. – Х. : ХУПС, 2013. – Вип. 2(35) –С. 6-10.
15. Shevchenko, A.F., (2014) A comparative analysis of directional properties of phased ring arrays to be used in multi-static active/passive radars, Data processing systems, 9(125), pp.65-72, (in Ukrainian).
16. Kudriashov V.V., A Modified Maximum Likelihood Method for Estimation of Mutual Delay and Power of Noise Signals by Bistatic Radiometer, Comptes Rendus – L'Académie Bulgare des Sciences, 68(5), pp. 631-640.
17. Модель застосування мобільних комплексів/ О.С. Балабұха, К.Ю. Дергачов К.Ю., В.Ф. Слободенюк // Збірник наукових праць ЦНДІНУ. – К. ЦНДІНУ. – 2007. – Вип. 2. – С. 31 – 33.
18. Lukin, K. A. "Millimeter wave noise radar applications: theory and experiment", Fourth International Kharkov Symposium 'Physics and Engineering of Millimeter and Sub-Millimeter Waves'. Symposium Proceedings (Cat. No.01EX429), Kharkov, Ukraine, 2001, pp. 68-73, doi: 10.1109/MSMW.2001.946748.
19. Savci, K., Stove, A.G., De Palo, F., Erdogan, A.Y., Galati, G., Lukin, K.A., Lukin, S. Noise radar—overview and recent developments IEEE Aerospace and Electronic Systems Magazine, 2020, Vol.35 (9), pp.8-20.

References

1. Osnovy strel'by i upravleniya ognem voyskovykh zenitnykh raketnykh kompleksov. Chast' 1. Kazachinskiy V. Z., Kaipetskiy A. A., Nesterenko L. G., Semenov G. V., Solodovnikov N. D. – Kyiv: KVAIU, 1971. – 468s.
2. Osnovy stril'by ta keruvannya vohnem: navch. posib. /V.YE. Kudryashov, S.H. Leushyn, V.I. Samokvit. – Kharkov : KHUPS, 2016. – 232 s.
3. Pushkoris V. P. Upravleniye ognem voysk PVO Sukhoputnykh voysk: Uchebnik. – Kyiv:VA PVO SV, 1989. – 556 s.
4. A private model for determining the efficiency of target distribution / M.S. Piskunov., V.YE. Kudryashov, V.YE., Filippenkov O.V. // Systemy ozbroynnya i viys'kova tekhnika. – Kharkov: KHNUPS, 2021. – Vyp. 1 (65) – S. 107 – 113.
5. Dovidnyk z protypovitryanoyi oborony. Toropchyn A.YA., Romanenko I.O., Danyk YU.H., Pashchenko R.E. ta in. – Kyiv: MO Ukrainy, KH.: 2003. – 368 s.
6. Model' protypovitryanoho boyu yak element systemy upravlinnya vohnem pidrozdilamy viys'k PPO Sukhoputnykh viys'k/ O. V. Kolomiytsev, V. YE. Kudryashov, V.V. Mashtalir, P. V. Open'ko, R. M. Oliynyk // Zbirnyk naukovykh prats' DNDI VS ozbroynnya ta viys'kovoyi tekhniky. – Chernihiv: DNDI VS OVT. – 2019. – Vyp. № 1(1). – S. 94-101.
7. Teoriya i tekhnika obrabotki radiolokatsionnoy informatsii na fone pomekh / Shirman YA.D., Manzhos V.N. – Moscow; Radio i svyaz', 1981. – 416 s.

8. Radioelektronnyye sistemy: Osnovy postroyeniya i teoriya. Spravochnik. Izd. 2 – ye, pererab. i dop. / Pod. red. YA. D. Shirmana. – Moscow: Radiotekhnika, 2007. 512s.
9. Spravochnik po radiolokatsii/ pod obshchey red. K.N. Trofimova. Tom 1. Osnovy radiolokatsii. Pod red. YA.S. Itskhoki: – Moscow: Sov. radio, 1976. – 456 s.
10. Druhyy rid pomyl'ok stril'by raketamy po netypovym tsilyam ZRK maloyi dal'nosti / O.V. Kolomiytsev, V.YE. Kudryashov, I.YA. Zahoruyko, S.S. Voroshylov // Zbirnyk naukovykh pratsi KHU PS. – Kharkov: KHU PS. – 2011.- Vyp. 1(27) – S. 86 – 90.
11. Umovna imovirnist' urazhennya netypovoyi tsili ZRK maloyi dal'nosti / O.V. Kolomiytsev, V YE. Kudryashov, I.YA. Zahoruyko, S.S. Voroshylov // Zbirnyk naukovykh pratsi KHU PS. – Kharkov: KHU PS. – 2012.- Vyp. 2(30) – S. 170 – 174.
12. Kudryashov V.YE., Lytovchenko D.M. Chysel'ne modelyuvannya z osnov stril'by raketamy ta upravlinnya vohnem kompleksiv maloyi dal'nosti: navch. posib. Kharkov : KHNUPS, 2023. – 533.
13. Lytovchenko D.M., Kudryashov V.YE. Chysel'ne modelyuvannya z osnov stril'by ozbroynennya blyzhn'oyi diyi ta informatsiynoho zabezpechennya viys'k: navch. posib. Kharkov : KHNUPS, 2025. – 268 s.
14. Piskunov S. M. Perspektyvna struktura systemy upravlinnya sylamy i zasobamy protypovitryanoyi oborony Sukhoputnykh viys'k Zbirnyk naukovykh prats' KHUPS. – Kharkov : KHUPS, 2013. – Vyp. 2(35) –S. 6-10.
15. Shevchenko, A.F., (2014). A comparative analysis of directional properties of phased ring arrays to be used in multi-static active/passive radars, Data processing systems, 9(125), pp.65-72, (in Ukrainian).
16. Kudriashov V.V., A Modified Maximum Likelihood Method for Estimation of Mutual Delay and Power of Noise Signals by Bistatic Radiometer, Comptes Rendus – L'Académie Bulgare des Sciences, 68(5), pp. 631-640.
17. Model' zastosuvannya mobil'nykh kompleksiv/ O.S. Balabukha, K.YU. Derhachov K.YU., V.F. Slobodenyuk// Zbirnyk naukovykh prats' TSNDINU. – Kyiv. TSNDINU. – 2007. – Vyp. 2. – S. 31 – 33.
18. Lukin, K. A. "Millimeter wave noise radar applications: theory and experiment", Fourth International Kharkov Symposium 'Physics and Engineering of Millimeter and Sub-Millimeter Waves'. Symposium Proceedings (Cat. No.01EX429), Kharkov, Ukraine, 2001, pp. 68-73, <https://doi.org/10.1109/MSMW.2001.946748>.
19. Savci, K., Stove, A.G., De Palo, F., Erdogan, A.Y., Galati, G., Lukin, K.A., Lukin, S. Noise radar—overview and recent developments IEEE Aerospace and Electronic Systems Magazine, 2020, Vol.35 (9), pp.8-20.

Особливості усвідомлення студентами сучасних проблем безпеки дорожнього руху

The Features of Students' Awareness of Modern Road Safety Issues

Соломія Писаревська^A

Corresponding author: к.х.н., доцент, доцент кафедри безпеки життєдіяльності, e-mail: solomiya.pysarevska@lnu.edu.ua, ORCID: 0000-0003-4043-1692

Вікторія Ващук^A

к.т.н., асистент кафедри безпеки життєдіяльності, e-mail: viktoriya.vashchuk@lnu.edu.ua, ORCID: 0000-0002-5344-3820

Зіновій Яремко^A

д.х.н., професор, завідувач кафедри безпеки життєдіяльності, e-mail: zinoviy.yaremko@lnu.edu.ua, ORCID: 0000-0001-8508-7763

Solomiya Pysarevska^A

Corresponding author: PhD, Associate Professor, e-mail: solomiya.pysarevska@lnu.edu.ua, ORCID: 0000-0003-4043-1692

Viktoriya Vashchuk^A

PhD, Assistant Professor, e-mail: viktoriya.vashchuk@lnu.edu.ua, ORCID: 0000-0002-5344-3820

Zinoviy Yaremko^A

DSc, Head of Life Safety Department, e-mail: zinoviy.yaremko@lnu.edu.ua, ORCID: 0000-0001-8508-7763

^A Львівський національний університет імені Івана Франка, м. Львів, Україна

^A Ivan Franko National University of Lviv, Lviv, Ukraine

Received: July 16, 2025 | Revised: August 13, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.10>

Мета роботи. Оцінити рівень усвідомлення студентами небезпечної поведінки пішоходів, їхнє ставлення до заходів підвищення безпеки дорожнього руху та суб'єктивне сприйняття безпеки різних способів пересування.

Метод дослідження. Дослідження базувалося на кількісному методі онлайн-опитування (Google Forms). Участь взяли 410 студентів віком 16–23 років з України (місто Львів). Використано адаптований опитувальник ESRA 2, який включав соціодемографічні питання, оцінку власної поведінки пішоходів та сприйняття безпеки транспорту.

Результати дослідження. Виявлено, що найпоширенішими видами ризикованої поведінки були користування телефоном, перехід дороги поза пішохідним переходом і прослуховування музики під час ходьби (95 %, 86 % і 75 % відповідно). Студенти суб'єктивно вважають найбезпечнішим способом пересування – приватний автомобіль, хоча статистично він є найнебезпечнішим видом транспорту. Підтримка заходів безпеки вища для фізичних засобів захисту (шоломи, світловідбивальний одяг), ніж для обмеження використання смартфонів. Стать і місце проживання достовірно впливають на поведінку пішоходів.

Теоретична цінність дослідження. Результати підтверджують і розвивають наявні концепції впливу когнітивних та соціальних чинників на ризиковану поведінку пішоходів. Дослідження демонструє значущість цифрових відволікань як незалежного предиктора небезпечної поведінки.

Практична цінність дослідження. Отримані дані можуть бути використані для розроблення освітніх програм у закладах вищої освіти, спрямованих на підвищення обізнаності студентів щодо реальних ризиків та ефективних заходів безпеки. Крім того, результати можуть слугувати основою для цільових соціальних кампаній і формування державної політики щодо профілактики дорожньо-транспортних пригод.

Цінність дослідження. Робота пропонує комплексний аналіз самодекларованої поведінки українських студентів-пішоходів у контексті сучасної цифрової культури, що до цього часу практично не досліджувалося. Зіставлення суб'єктивної оцінки безпеки транспорту з реальною статистикою дорожньо-транспортних пригод дозволяє виявити суттєві когнітивні викривлення у сприйнятті ризиків.

Обмеження дослідження. Обмеженнями дослідження є географічна вибірка (Львів) і самодекларативний характер даних, що можуть супроводжуватися соціально бажаними відповідями. Перспективними напрямками подальших досліджень є експериментальні спостереження за реальною поведінкою пішоходів, а також розширення вибірки на інші регіони України та порівняння з іншими віковими групами.

Тип статті. науково-практична.

Purpose. To assess the level of students' awareness of risky pedestrian behaviours, their attitudes towards road safety improvement measures, and their subjective perception of the safety of different modes of movement.

Method. A quantitative method of online surveying (Google Forms) was used in the study. A total of 410 students aged 16–23 from Ukraine (the city of Lviv) participated in the survey. An adapted ESRA 2 questionnaire was used, which included sociodemographic questions, an assessment of self-reported pedestrian behaviour, and perceptions of transport safety.

Findings. It was found that the most common types of risky behavior were using a mobile phone, crossing the road outside of a pedestrian crossing, and listening to music while walking (95%, 86%, and 75%, respectively). Students subjectively consider private cars to be the safest mode of transportation, although statistically, it is the most dangerous. Support for safety measures is higher for physical protective equipment (helmets, reflective clothing) than for restrictions on smartphone use. Gender and place of residence significantly influence pedestrian behavior.

Theoretical implications. The results confirm and extend existing concepts regarding the influence of cognitive and social factors on risky pedestrian behaviour. The study demonstrates the significance of digital distractions as an independent predictor of unsafe behaviour.

Practical implications. The obtained data can be used to develop educational programs in higher education institutions aimed at increasing students' awareness of actual risks and effective safety measures. In addition, the results can serve as a basis for targeted social campaigns and for shaping public policy on the prevention of road traffic accidents.

Originality/Value. The paper offers a comprehensive analysis of self-declared pedestrian behavior among Ukrainian students in the context of modern digital culture, which has so far been virtually unexplored. Comparing the subjective assessment of transport safety with actual road traffic accident statistics makes it possible to identify significant cognitive distortions in risk perception.

Research limitations/Future research. The limitations of the study include the geographical sample (Lviv) and the self-declarative nature of the data, which may be accompanied by socially desirable responses. Promising directions for further research include experimental observations of actual pedestrian behavior, as well as expanding the sample to other regions of Ukraine and comparing different age groups.

Paper type. scientific and practical.

Ключові слова: пішохід, дорожньо-транспортна пригода, безпека, пішохідний перехід.

Key words: pedestrian, traffic accident, safety, pedestrian crossing.

Вступ

За даними Всесвітньої організації охорони здоров'я (ВООЗ) дорожньо-транспортний травматизм залишається основною причиною смерті дітей та молодих людей віком від 5 до 29 років (ВООЗ, 2023). Більше половини цих смертельних випадків припадає на пішоходів, велосипедистів та мотоциклістів у країнах із низьким та середнім рівнем доходів. Глобальною метою ВООЗ у найближчому періоді часу, до 2030 року є скорочення смертності та травматизму внаслідок дорожньо-транспортних пригод (ДТП) вдвічі у порівнянні із сьогоднішнім.

Забезпечення безпеки усіх учасників дорожнього руху є складним процесом, який в найпростішому підході до його аналізу враховує поведінку, навички, знання водіїв, пішоходів, технічний стан транспортних засобів та відповідну дорожню інфраструктуру. Тому дослідження усіх складових забезпечення безпеки дорожнього руху є відповідальним і актуальним завданням.

У цій праці розглянута поведінка пішоходів, як найуразливіших учасників дорожнього руху. Зокрема, в Україні наїзд на пішохода є на першому місці серед причин смертності від ДТП і за даними Світового банку у 2019 році він зумовив 10,2 смертей на 100 000 населення (World Bank, 2019). Отож, одним з перших кроків до розроблення заходів щодо попередження ДТП з вини пішоходів є вивчення проявів їхньої небезпечної поведінки під час руху.

Тенденції змін показників безпеки дорожнього руху та успішність впроваджених заходів можна відстежити за допомогою відповідних індикаторів (Torfs, 2019). Основними джерелами даних для оцінювання безпеки на дорогах є статистика ДТП, обстеження дорожньої інфраструктури та анкетування. Останній метод, особливо якщо він проводиться онлайн, є відносно недорогим способом отримання інформації про культуру безпеки та поведінку учасників дорожнього руху. Проте в основі цього методу є самооцінювання, що може спричинити соціально бажані відповіді. Основна перевага анкетування полягає в тому, що воно дозволяє отримати уявлення про соціально-когнітивні чинники поведінки, зокрема такі як ставлення, сприйняття соціальних норм, оцінювання ризиків або вкорінені звички. Такі чинники можуть допомогти зрозуміти мотивацію, що лежить в основі певної поведінки людини (Torfs, 2019).

У цьому дослідженні ми використали анкетування для оцінювання ризикованої поведінки пішоходів в Україні. Зміст анкети був сформований на основі найновіших результатів, які розглядають найважливіші аспекти оцінювання ризикованої поведінки пішоходів за допомогою різних підходів (ESRA, 2018).

Теоретичні основи дослідження

Поведінку пішоходів та їхнє ставлення до безпеки дорожнього руху автори (Nikolaou, 2023; Torfs, 2019; Saxena, 2023) оцінювали за результатами анкетування як одного із способів отримання необхідних даних. На основі логістичних регресійних моделей з випадковими ефектами та моделі структурного рівняння виявлено, що жінки-пішоходи та мешканці напівміських або сільських територій менш схильні до небезпечної поведінки у порівнянні з чоловіками та мешканцями міст (Nikolaou, 2023). Пішоходи, які слухали музику у навушниках або читали повідомлення під час ходьби, мали вищу ймовірність небезпечної поведінки, ніж ті, хто не відволікався. До того ж ті, хто частіше переходив дорогу на червоне світло, з більшою ймовірністю також переходили дорогу в недозволеному місці.

Автори (Torfs, 2019) аналізували ставлення пішоходів та інших вразливих учасників дорожнього руху до безпеки на дорозі. Згідно з результатами, всі вразливі учасники дорожнього руху частіше ставали учасниками ДТП у порівнянні з водіями автомобілів і почувалися менш захищеними. Водночас пішоходи почувалися безпечніше порівняно з

іншими вразливими учасниками. Моделі логістичної регресії показали, що використання навушників під час ходьби залежить від статі, віку та підтримки певної політики безпеки.

Звичка пішоходів писати повідомлення у смартфоні під час переходу дороги негативно корелює із їхнім віком і позитивно – з їхнім рівнем доходів. Значний вплив на намір використовувати телефон під час руху мають ставлення, суб'єктивні норми та рівень контролю поведінки. Найвагомішим чинником є рівень контролю поведінки, далі – суб'єктивні норми (Saxena, 2023).

Одним із найнадійніших способів збирання даних про поведінку пішоходів на переходах є дослідження відеозаписів на цих переходах. Автори (Wang, 2024; Sheykhfard, 2023) використовували відеоспостереження для дослідження переходів на 12 тротуарах у 9 міських перехрестях міста Нанкін і порушень правил переходу на червоне світло на двох перехрестях у місті Бабол відповідно.

Автори (Wang, 2024) вивчали вплив мобільного телефону на відволікання уваги під час переходу дороги. Ризики, пов'язані з відволіканням, оцінювали шляхом побудови моделі логістичної та *relogit*-регресії. Використання пішоходами телефону було поширеним явищем, особливо інтенсивно він використовувався перед самим переходом.

Три рівні ризику порушень переходу перехрестя з світлофором визначали автори (Sheykhfard, 2023), використовуючи "K-means" алгоритм. Кожен рівень характеризували структурним рівнянням з урахуванням чотирьох чинників: людського, дорожнього, навколишнього середовища та транспортного. Найбільший вплив на рівень ризику має людський чинник — зокрема використання мобільного телефону та чинники, які сприяють відволіканню уваги пішоходів.

Оскільки умови реального світу дуже динамічні, важливо зрозуміти, якою мірою різні чинники (відволікання, особливості ходьби, візуальна поведінка тощо) впливають на ризик небезпечної взаємодії пішоходів з транспортними засобами. Автори (Krishna, 2024) провели експеримент із трекером погляду на нерегульованому перехресті в Делі. Виявилося, що використання мобільного телефону під час переходу підвищує ризик небезпечної взаємодії з автомобілем приблизно у вісім разів. Візуальні характеристики, разом із демографією та особливостями трафіку, мають важливе значення для формування ефективної політики запобігання ДТП.

На сьогоднішній день використання віртуального середовища дорожнього руху є поширеною методологічною стратегією, оскільки дозволяє етично досліджувати поведінку пішоходів без ризику ДТП і дає змогу стандартизувати умови для учасників (Wang, 2022). Автори досліджували вплив віку та прагнення отримати нові відчуття на поведінку пішоходів під час переходу дороги. У дослідженні брали участь діти (10–13 років), підлітки (14–18 років) і молодь (20–24 роки). Аналізувалися три показники безпеки: затримка старту, пропущені можливості та небезпечні переходи. За результатами дослідження виявлено, що на безпеку пішоходів впливають як вік, так і прагнення до новизни. Підлітки ризикували більше, ніж дорослі або діти. Вплив прагнення до новизни спостерігався у всіх вікових групах, але був сильнішим серед підлітків.

Постановка проблеми

Підсумовуючи результати попередніх досліджень та враховуючи статистику ВООЗ, можна стверджувати, що ДТП є першопричиною смерті дітей та молоді. Тому ця вікова категорія потребує особливої уваги як відповідних органів регулювання, контролю та управління дорожнім рухом, так і науковців. Метою цієї роботи є оцінювання поведінки пішоходів-студентів та їхнього ставлення до заходів щодо підвищення рівня безпеки учасників дорожнього шляхом анкетування. Отримані результати зможуть доповнити доступні в літературі дані, а також бути джерелом підтвердження уже запропонованих теорій та

спостережень. Дані нашого дослідження можуть бути використані для зміни методик викладання дисциплін безпекового спектра у закладах вищої освіти та для розробки рекомендацій щодо цільових соціальних заходів зі зменшення рівня ризикованої поведінки пішоходів.

Методологія дослідження

Вихідні дані для оцінювання поведінки пішоходів отримані шляхом онлайн-опитування (через Google-forms) студентів протягом листопада 2024 року в місті Львів, Україна. Жодних заохочень для участі в опитуванні не передбачалося.

Участь в опитуванні взяло 410 осіб віком 16–23 роки з розподілом 57 % осіб жіночої статі та 43 % осіб чоловічої статі. Усі опитані мали середню шкільну освіту і 23 % студентів проживали у сільській місцевості, а 77 % – у міській.

У цьому опитуванні використали питання з опитувальника ESRA 2, який містив 3 блоки питань (ESRA, 2018). Перший блок питань стосувався соціодемографічної інформації (стать, вік, місцевість проживання, освіта). У другому блоці були питання щодо оцінювання студентами власної небезпечної поведінки під час руху в конкретних ситуаціях. У третьому блоці респондентам було запропоновано оцінити безпеку різних видів транспортних засобів, які вони використовують. Також у цей блок увійшли запитання щодо схвалення студентами загальноприйнятих заходів безпеки під час дорожнього руху. Додатково опитували студентів, щодо їхнього потрапляння в ДТП впродовж останніх 12 місяців з такими наслідками як травми чи лише матеріальні втрати.

Результати та обговорення

Сьогодні забезпечення безпеки громадян вимагає нових підходів до управління сукупністю транспортних і пішохідних потоків. Складність такого управління полягає як у неоднозначності критеріїв, обраних для забезпечення безпеки дорожнього руху та пішоходів, так і в наявності численних обмежень, які супроводжують функціонування інфраструктури великого міста. У цій праці проаналізовано окремі аспекти забезпечення безпеки громадян, а саме:

- оцінювання безпечності способів пересування;
- оцінювання поведінки пішоходів під час руху;
- оцінювання заходів щодо підвищення безпеки під час руху.

Хоча розглянуті чинники пов'язані із незначною частиною проблем у вирішенні питань безпеки дорожнього руху, їхнє усвідомлення безумовно сприятиме підвищенню рівня безпеки пішоходів.

Оцінювання безпечності способів пересування

Результати опитування підтвердили, що респонденти для переміщення в місті поряд з ходьбою пішки використовують різні транспортні засоби, а саме:

- міський громадський транспорт (автобус, електротранспорт) — 96 % опитаних,
- приватний автомобіль — 67 % опитаних,
- велосипед — 41 % опитаних,
- електросамокат — 41 % опитаних.

Тому серед способів пересування для опитування були вибрані наступні:

1. Пішохід.
2. Велосипедист.
3. Водій електросамоката.
4. Пасажир міського електротранспорту.
5. Пасажир автобуса.
6. Пасажир приватного автомобіля.

Респондентам запропонували оцінити власне відчуття безпеки у разі використання різних засобів пересування за шкалою від 0 до 10, де 0 — дуже небезпечно, а 10 — дуже безпечно. Результати опитування — середній бал та медіана (зменшує вплив екстремальних значень) для кожного способу пересування та статистика Патрульної поліції щодо смертності від ДТП різних учасників дорожнього руху за 2019-2023 рр. [Patrol Police, 2024] наведені у таблиці 1.

Таблиця 1 — Оцінка безпечності способів пересування

Параметр оцінювання	Учасник дорожнього руху					
	Пішохід	Велосипедист	Водій електросамоката	Пасажир міського електротранспорту	Пасажир автобуса	Пасажир приватного автомобіля
Середній бал	7.5±1.6	6.4±2.6	4.4±2.9	8.0±1.7	7.1±2.4	8.6±1.4
Медіана	8	7	5	8	7	9
Частка смертей (у %)	30-36	5-7	-	-	0.5-0.8	56-62

Отже, за результатами опитування найбезпечніше респонденти почувають себе як пасажир приватного автомобіля, далі у порядку зменшення відчуття безпеки розташовані *пасажир міського електротранспорту > пішохід > пасажир автобуса > велосипедист > водій електросамоката*. Однак статистика смертності від ДТП свідчить, що приватний автомобіль є найменш безпечним способом пересування — водії та пасажир приватного автомобіля найчастіше помирають у ДТП, а на другому місці за смертністю є пішоходи. Можна зазначити, що оцінювання студентами власного відчуття безпеки є досить суб'єктивним і свідчить про недостатню обізнаність щодо ризиків у разі використання різних видів транспорту. Також причиною цієї різниці може бути недостатнє розуміння самого поняття безпеки, чи той факт, що під час оцінювання могли бути помилково враховані комфортність транспорту, наявність відповідної інфраструктури для безпечного пересування, а також власний (негативний чи позитивний) досвід користування певним видом транспорту. Так, за даними цього опитування 6 % студентів ставали учасниками ДТП внаслідок якого отримували травми. Такі студенти оцінювали безпечність способів пересування в середньому на 1–2 бали нижче, ніж загальний середній бал. Отож, негативний життєвий досвід також має вплив на об'єктивність оцінювання студентами власної безпеки.

Оцінювання поведінки пішоходів під час руху

Для оцінювання власної небезпечної поведінки респонденти відповідали на чотири питання, як часто протягом останніх 30 днів вони:

- а) переходили дорогу на червоне світло світлофора;
- б) переходили дорогу в місцях, відмінних від найближчого пішохідного переходу;
- в) читали текстові повідомлення/електронну пошту або переглядали соціальні мережі (наприклад, Facebook, Instagram тощо), йдучи вулицею;
- г) слухали музику в навушниках під час ходьби по вулиці.

Шкала оцінок на ці питання варіювалася від 1 — ніколи до 5 — завжди.

Найризикованішою поведінкою респондентів виявилось читання повідомлень або перегляд інформації на смартфоні під час ходьби — в середньому 95 % опитаних вказали, що хоча б один раз за останні 30 днів діяли так (табл. 2). Трохи менше, але також значна частка респондентів (в середньому 86 %) зазначила, що переходили дорогу поза межами пішохідного переходу, і в середньому 75 % опитаних — слухали музику в навушниках,

рухаючись вулицями. Найрідше пішоходи переходили дорогу на червоне світло — в середньому лише 40 % опитаних зазначили, що робили це хоча б раз за останній місяць.

Таблиця 2 — Частота прояву небезпечної поведінки під час руху пішки та χ^2 -критерій

	Перехід на червоний сигнал світлофора (у %)		Перехід у недозволеному місці (у %)		Перегляд інформації на телефоні під час ходьби на вулиці (у %)		Слухання музики через навушники під час ходьби на вулиці (у %)	
в середньому	40		86		95		75	
стать	жіноча	чоловіча	жіноча	чоловіча	жіноча	чоловіча	жіноча	чоловіча
	36	53	87	80	95	95	74	80
$\chi_{\text{розр}}^2$	22.82		26.55		26.99		21.65	
$\chi_{\text{табл}}^2$	9.49 (v=4, α=0.05)							
місцевість	сільська	міська	сільська	міська	сільська	міська	сільська	міська
	58	36	88	85	100	93	69	77
$\chi_{\text{розр}}^2$	26.37		3.27		34.68		3.19	
$\chi_{\text{табл}}^2$	9.49 (v=4, α=0.05)							

Результати опитування щодо дотримання правил переходу дороги за статтю особи та місцевістю її проживання наведені на рис. 1. Використовуючи дані цих вибірок була проаналізована за допомогою критерію χ^2 достовірність двох статистичних гіпотез:

H_0 : відмінності в розподілах є випадковими, якщо $\chi^2_{\text{розр}} < \chi^2_{\text{табл}}$ (для $\alpha = 0,05$),

H_1 : відмінності в розподілах є закономірними, якщо $\chi^2_{\text{розр}} > \chi^2_{\text{табл}}$ (для $\alpha = 0,05$).

Кількість ступенів свободи, критичне значення $\chi^2_{\text{табл}}$ і розраховане значення χ^2 наведено в табл. 2. Результати показують, що для рівня значущості $\alpha = 0,05$ стать особи та місцевість її проживання мають суттєвий вплив на поведінку пішоходів під час руху пішки ($\chi^2_{\text{розрах}} > \chi^2_{\text{табл}}$) і відмінності в поведінці пішоходів є закономірними. Лише у випадку переходу дороги у недозволеному місці та слухання музики під час руху пішки, поведінка студентів не залежить від місцевості їхнього проживання.



а



б

Рисунок 1 — Розподіл відповідей студентів (у %) щодо переходу дороги у недозволеному місці залежно від статі особи (а) та місцевості її проживання (б), де 1 — ніколи, 2 — принаймні раз на місяць, 3 — час від часу, 4 — часто і 5 - завжди

Порівняння одержаних результатів про самодекларовану ризиковану поведінку пішоходів із реальною статистикою ДТП за участю пішоходів за останні п'ять років показало хорошу кореляцію, оскільки 6–7 % смертей від загальної кількості внаслідок ДТП трапляються

через перехід дороги в недозволеному місці, а 0,3–0,5% — через перехід дороги на червоне світло пішохідного світлофора. Таким чином, опитування пішоходів дає важливу інформацію, яка певною мірою об'єктивно відображає реальну поведінку респондентів.

Оцінювання заходів щодо підвищення безпеки під час руху

Заходи щодо підвищення безпеки вразливих учасників дорожнього руху (пішоходів, велосипедистів та водіїв електричного самоката) респонденти оцінювали, відповідаючи на наступні питання:

1. Як Ви оцінюєте обов'язковість одягати шолом для велосипедистів?
2. Як Ви оцінюєте обов'язковість одягати шолом разі використання електричного самоката?
3. Як Ви оцінюєте обов'язковість пішоходами носити світловідбивальний одяг чи стрічки у темну пору доби?
4. Як Ви підтримуєте заборону слухати музику під час їзди на велосипеді / електричному самокаті?
5. Як Ви підтримуєте заборону слухати музику під час руху пішки?
6. Як Ви підтримуєте заборону читати інформацію на телефоні під час руху пішки?
7. Як Ви підтримуєте заборону читати інформацію на телефоні під час переходу дороги?
8. Як Ви підтримуєте заборону слухати музику під час переходу дороги?

Студенти оцінювали запропоновані заходи за шкалою від 1 – зовсім не підтримую до 5 – повністю підтримую. Середній бал та медіана для запропонованих заходів наведені у табл. 3.

Таблиця 3 – Оцінювання заходів безпеки

	Заходи безпеки							
	1	2	3	4	5	6	7	8
Середній бал	4,1±2,0	3,4±1,3	4,0±1,2	3,5±1,4	2,7±1,3	2,8±1,2	4,0±1,4	3,3±1,5
Медіана	4	3	5	4	2	3	5	3

Найбільшу підтримку отримали заходи, які стосуються фізичного захисту учасників дорожнього руху такі як носіння шолома під час їзди на велосипеді (4,1±2,0) чи світловідбивального одягу (4,0±1,2). Найнижчу оцінку отримали заходи, пов'язані з використанням телефону під час руху пішки, чи то слухати музику (2,7±1,3), чи читати інформацію (2,8±1,2). Це може свідчити про недооцінку ризиків, пов'язаних з використанням навушників і смартфонів у русі, або про високий рівень звикання до цифрових технологій серед молоді. Залежність між рівнем використання телефона для читання інформації під час руху пішки та підтримкою заходів щодо його обмеження наведена на рис.2. Для можливості співставлення результатів щодо рівня використання телефона для читання інформації під час руху пішки та підтримкою заходів щодо його обмеження шкалу підтримки заходів зробили зворотною від того варіанту, який був запропонований респондентам в опитуванні, а саме відповіді оцінювалися у діапазоні від 1 – повністю підтримую до 5 – зовсім не підтримую. Така шкала добре співставляється з варіантами відповіді щодо використання телефона для читання інформації під час руху пішки, а саме 1 – ніколи не використовував/ла за останні 30 днів, 2 – використовував/ла принаймні 1 раз на місяць, 3 – час від часу, 4 – часто чи 5 – завжди.

Рівень відволікання на телефон під час руху пішки та рівень підтримки заходів, пов'язаних з обмеженням його використання, добре корелюють між собою ($R^2=0,868$).

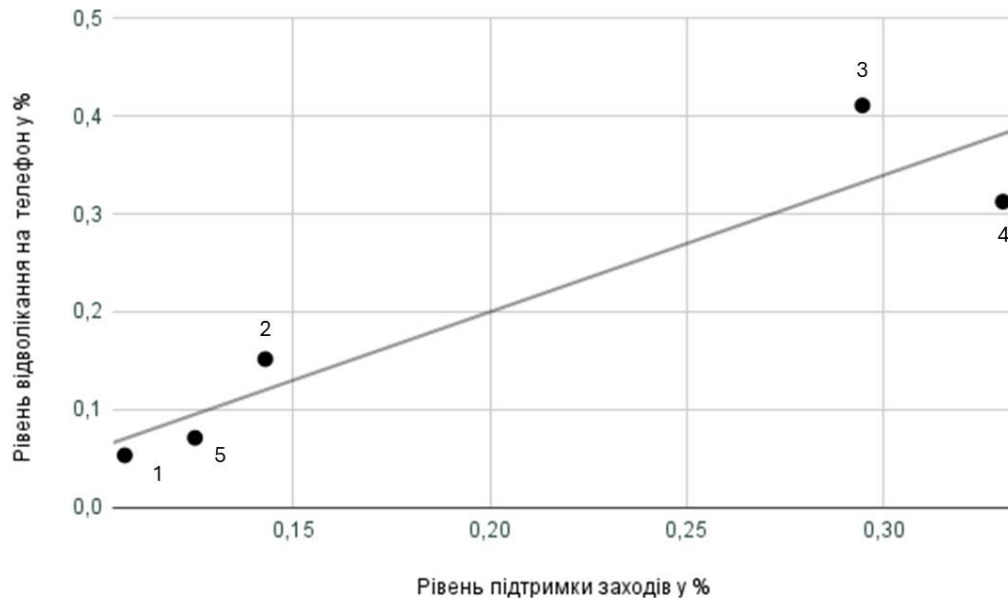


Рисунок 2 – Залежність між рівнем використання телефона для читання інформації під час руху пішки та рівнем підтримки заходів щодо його обмеження, де 1-5 – це рівень відволікання на читання інформації з телефона під час руху пішки (1 – ніколи, 2 – принаймні 1 раз на місяць, 3 – час від часу, 4 – часто, 5 – завжди) та рівень підтримки заходів щодо заборони використання телефона для читання інформації під час руху пішки (від 1 – повністю підтримую до 5 – зовсім не підтримую)

Отже, студенти схильні більше підтримувати заходи, пов'язані з фізичними засобами безпеки (шоломи, світловідбивальні елементи), ніж обмеження особистої поведінки, пов'язаної з використанням гаджетів. Проте студенти добре підтримують заборону читати інформацію на телефоні під час переходу дороги ($4,0 \pm 1,4$). Це свідчить про неоднозначність оцінок респондентів та необхідність підвищення їхньої обізнаності щодо впливу цифрових відволікань на безпеку.

Висновки

Оцінювання безпеки видів транспортних засобів респондентами свідчить про низький рівень обізнаності щодо реальної статистики ДТП з їхньою участю, тому середня оцінка безпеки та медіана, отримані з результатів опитування, відрізняються від статистики смертності у ДТП із залученням різних видів транспорту. Власний досвід, як учасника ДТП, сприяє адекватнішій оцінці безпечності засобів пересування.

Переходи в недозволених місцях та відволікання уваги на читання інформації на смартфоні чи слухання музики через навушники — це основні прояви небезпечної поведінки пішоходів під час ходьби вулицею. Частота цих видів небезпечної поведінки в деяких випадках залежить як від статі особи, так і місцевості її проживання.

Узагальнюючи, можна зробити висновок, що хоча молодь готова під час переміщення підтримувати певні обмеження задля особистої безпеки, важливо працювати над формуванням безпечної поведінки, зокрема щодо цифрових відволікань під час руху.

Отримані результати є цінними та інформативними для експертів з безпеки дорожнього руху, органів влади та освітян у прийнятті рішень, спрямованих на запобігання ДТП, де ризикована поведінка пішоходів є одним із основних чинників. Тому соціальні заходи, як-от реклама, семінари та викладання дисциплін з безпеки життєдіяльності, повинні

базуватися на наукових дослідженнях — таких, як це, і подібних. Одним із практичних застосувань отриманих висновків є підвищення культури безпеки дорожнього руху через освітній компонент.

Очевидно що результати цього дослідження стосуються безпеки громадян, які за певних обставин можуть порушувати встановлені норми поведінки під час переходу дороги або під час ходьби по вулиці. Проте коли таких пішоходів не буде на вулицях міст — передбачити наразі неможливо, тому ці результати є актуальними.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

- ESRA. (2018). *E-Survey of Road users' Attitudes*. ESRA2. Available from : <https://www.esranet.eu/en/about-the-project/esra2/>
- Krishna, K. V., Kapruwan, R., & Choudhary, P. (2024). Understanding distracted pedestrians' risky behaviour: The role of walking and visual characteristics through a field study. *Transportation Research Part F: Traffic Psychology and Behaviour*, 101, 111–129. <https://doi.org/10.1016/j.trf.2024.01.003>
- Nikolaou, D., Ntontis, A., Michelaraki, E., Ziakopoulos, A., & Yannis, G. (2023). Pedestrian safety attitudes and self-declared behaviour in Greece. *IATSS Research*, 47(1), 14–24.
- Patrol Police. (2024). Statistics. Available from : <https://patrolpolice.gov.ua/statystyka/>
- Saxena, A. (2023). Texting and crossing: An extended theory of planned behaviour to model the psychological and demographic factors related to pedestrians' use of cell phone for texting at crosswalks in developing country. *IATSS Research*, 47(1), 50–60. <https://doi.org/10.1016/j.iatssr.2023.01.003>
- Sheykhfard, A., Haghighi, F., Kavianpour, Sh., Das, S., Farahani, P. S., & Fountas, G. (2023). Risk assessment of pedestrian red-light violation behavior using surrogate safety measures: Influence of human, road, vehicle, and environmental factors. *IATSS Research*, 47(4), 514–525. <https://doi.org/10.1016/j.iatssr.2023.11.003>
- Torfs, K., & Meesmann, U. (2019). How do vulnerable road users look at road safety? International comparison based on ESRA data from 25 countries. *Transportation Research Part F: Traffic Psychology and Behaviour*, 63, 144–152. <https://doi.org/10.1016/j.trf.2019.04.001>
- Wang, Ch., Hou, M., Easa, S. M., & Cheng, J. (2024). Safety analysis of pedestrians distracted by mobile phones at street crossings: Field study in Nanjing. *Accident Analysis & Prevention*, 200, Article 107563. <https://doi.org/10.1016/j.aap.2024.107563>
- Wang, H., Wang, A., Su, F., & Schwebel, D. C. (2022). The effect of age and sensation seeking on pedestrian crossing safety in a virtual reality street. *Transportation Research Part F: Traffic Psychology and Behaviour*, 88, 99–110. <https://doi.org/10.1016/j.trf.2022.05.010>
- World Bank. (2019). Road traffic death rate (per 100,000 population). Available from : <https://data.worldbank.org/indicator/SH.STA.TRAF.P5?end=2019&start=2019&view=map>
- World Health Organization. (2023). *Global status report on road safety 2023*. Available from : <https://www.who.int/publications/i/item/9789240086517>

References

- ESRA. (2018). *E-Survey of Road users' Attitudes*. ESRA2. Available from : <https://www.esranet.eu/en/about-the-project/esra2/>

- Krishna, K. V., Kapruwan, R., & Choudhary, P. (2024). Understanding distracted pedestrians' risky behaviour: The role of walking and visual characteristics through a field study. *Transportation Research Part F: Traffic Psychology and Behaviour*, 101, 111–129. <https://doi.org/10.1016/j.trf.2024.01.003>
- Nikolaou, D., Ntontis, A., Michelaraki, E., Ziakopoulos, A., & Yannis, G. (2023). Pedestrian safety attitudes and self-declared behaviour in Greece. *IATSS Research*, 47(1), 14–24.
- Patrol Police. (2024). Statistics. Available from : <https://patrolpolice.gov.ua/statystyka/>
- Saxena, A. (2023). Texting and crossing: An extended theory of planned behaviour to model the psychological and demographic factors related to pedestrians' use of cell phone for texting at crosswalks in developing country. *IATSS Research*, 47(1), 50–60. <https://doi.org/10.1016/j.iatssr.2023.01.003>
- Sheykhfard, A., Haghighi, F., Kavianpour, Sh., Das, S., Farahani, P. S., & Fountas, G. (2023). Risk assessment of pedestrian red-light violation behavior using surrogate safety measures: Influence of human, road, vehicle, and environmental factors. *IATSS Research*, 47(4), 514–525. <https://doi.org/10.1016/j.iatssr.2023.11.003>
- Torfs, K., & Meesmann, U. (2019). How do vulnerable road users look at road safety? International comparison based on ESRA data from 25 countries. *Transportation Research Part F: Traffic Psychology and Behaviour*, 63, 144–152. <https://doi.org/10.1016/j.trf.2019.04.001>
- Wang, Ch., Hou, M., Easa, S. M., & Cheng, J. (2024). Safety analysis of pedestrians distracted by mobile phones at street crossings: Field study in Nanjing. *Accident Analysis & Prevention*, 200, Article 107563. <https://doi.org/10.1016/j.aap.2024.107563>
- Wang, H., Wang, A., Su, F., & Schwebel, D. C. (2022). The effect of age and sensation seeking on pedestrian crossing safety in a virtual reality street. *Transportation Research Part F: Traffic Psychology and Behaviour*, 88, 99–110. <https://doi.org/10.1016/j.trf.2022.05.010>
- World Bank. (2019). Road traffic death rate (per 100,000 population). Available from : <https://data.worldbank.org/indicator/SH.STA.TRAF.P5?end=2019&start=2019&view=map>
- World Health Organization. (2023). *Global status report on road safety 2023*. Available from : <https://www.who.int/publications/i/item/9789240086517>

Концепції охорони праці, безпеки праці та здоров'я і благополуччя працівників на роботі

Concepts of occupational protection, occupational safety and health and well-being of employees at work

Віталій Цопа ^A

Corresponding author: д.т.н., професор, професор кафедри, e-mail: dr.tsopav@gmail.com, ORCID: 0000-0003-4652-9180

Сергій Чеберячко ^B

д.т.н., професор, професор кафедри, e-mail: sicheb@ukr.net, ORCID: 0000-0001-5866-4393

Олена Шароватова ^C

к.п.н., доцент, доцент кафедри, e-mail: sharovatova.elen@ukr.net, ORCID: 0000-0002-2736-2189

Олег Дерюгін ^B

к.т.н., доцент, доцент кафедри, e-mail: deryugin_o@ukr.net, ORCID: 0000-0002-2456-7664

Кирило Лапко ^B

аспірант, e-mail: klapko@childcare.org.ua, ORCID: 0009-0008-3984-686X

Vitaly Tsopa ^A

Corresponding author: Dr of Technical Sciences, Professor, Professor of Department, e-mail: dr.tsopav@gmail.com, ORCID: 0000-0003-4652-9180

Serhii Cheberyachko ^B

Dr of Technical Sciences, Professor, Professor of Department, e-mail: sicheb@ukr.net, ORCID: 0000-0001-5866-4393

Olena Sharovatova ^C

PhD, Associate Professor, Associate Professor of Department, e-mail: sharovatova.elen@ukr.net, ORCID: 0000-0002-2736-2189

Oleg Deryugin ^B

PhD, Associate Professor, Associate Professor of Department, e-mail: deryugin_o@ukr.net, ORCID: 0000-0002-2456-7664

Kyrylo Lapko ^B

Graduate Student, e-mail: klapko@childcare.org.ua, ORCID: 0009-0008-3984-686X

^A Міжнародний інститут менеджменту, Київ, Україна

^B Національний технічний університет «Дніпровська політехніка», Дніпро, Україна

^C Національний університет цивільного захисту України, Черкаси, Україна

^A International Institute of Management, Kyiv, Ukraine

^B Dnipro University of Technology, Dnipro, Ukraine

^C National University of Civil Protection of Ukraine, Cherkasy, Ukraine

Received: August 07, 2025 | Revised: August 23, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.11>

Мета роботи. Аналіз концепцій охорони праці, безпеки праці і здоров'я на роботі та благополуччя працівників на роботі щодо пошуку подальших шляхів розвитку систем управління організаціями.

Метод дослідження. Порівняльний аналіз різних існуючих концепцій з охорони праці та бенчмаркінгу з елементами мозкового штурму.

Результати дослідження. Проведено аналіз трьох існуючих концепцій та визначено їх сильні сторони, які дозволяють зменшити кількість травматизму, підвищити продуктивність праці та створити умови для всебічного розвитку працівника. Встановлено базові складові кожної концепції з охорони праці, безпеки і здоров'я працівників на роботі та благополуччя працівників на роботі. Визначені переваги кожної концепції. Показано, що концепція благополуччя працівників на роботі дозволяє забезпечити створення психологічно позитивного та підтримуючого робочого середовища.

Теоретична цінність дослідження. Полягає у визначенні складових з формування благополуччя на роботі, які виходять за межі фізичної безпеки та включають цілісну турботу про психічне, соціальне та фінансове здоров'я працівників, вказуючи на майбутній вектор розвитку особистості працівника.

Практична цінність дослідження. Полягає у визначенні сильних і слабких сторін існуючих концепцій з охорони праці та безпеки і здоров'я працівників на роботі, що стало основою для визначення ключових ідей для розробки концепції благополуччя працівників на роботі.

Тип статті. Теоретичний, описовий, методичний.

Purpose. Analysis of concepts of labor protection, occupational safety and health at work and well-being of employees at work in order to find further ways of developing organizational management systems.

Method. Comparative analysis of various existing concepts of labor protection and benchmarking with elements of brainstorming.

Research results. An analysis of three existing concepts was conducted and their strengths were identified, which allows reducing the number of injuries, increasing labor productivity and creating conditions for the comprehensive development of the employee. The basic components of each concept on labor protection, safety and health of employees at work and well-being of employees at work were established. The advantages of each concept were determined. It was shown that the concept of well-being of employees at work allows creating a psychologically positive and supportive working environment.

Theoretical implications. Consists in identifying the components of well-being at work that go beyond physical safety and include holistic care for the mental, social, and financial health of employees, indicating the future vector of employee personality development.

Practical implications. Consists in identifying the strengths and weaknesses of existing concepts of occupational safety and health and safety of workers at work, which became the basis for identifying key ideas for developing the concept of well-being of workers at work.

Paper type. Theoretical, descriptive, methodical.

Ключові слова: концепції, охорона праці, безпека праці, благополуччя, ризик, працівник, небезпека.

Key words: concepts, occupational health and safety, occupational safety, well-being, risk, employee, danger.

Вступ

Систему управління безпекою праці та здоров'ям працівників запроваджують для зменшення рівня травматизму в організаціях [1]. Її впровадження потребує залучення певних фінансових ресурсів для розробки і реалізації дієвих процесів і практик. Разом з тим, частина виробничих компаній розглядають “безпеку праці” як другорядну систему, яка мало пов'язана із конкурентоспроможністю та виробничими цілями [2, 3]. Тому керівники таких компаній обмежуються тільки витратами, пов'язаними із виконанням законодавчих вимог [4, 5]. Щоб змінити такий світогляд, виникає необхідність пошуку нових концепцій безпеки і здоров'я на роботі (БЗР), яка б перетворилась із витратної статті на прибуткову. Зазначена проблема підкреслює критичну прогалину в сучасній літературі: потребу в моделях, які не лише відповідають міжнародним стандартам, але й помітно покращують економічні можливості організацій та добробут працівників [6]. Звідси формується актуальне завдання щодо пошуку шляхів підвищення рентабельності системи управління організаціями, яке можна вирішити тільки завдяки розробці нових концепцій, нових поглядів у сфері безпеки.

Теоретичні основи дослідження

У роботі [7] автори розглянули бізнес-практики, практики охорони здоров'я, безпеки та добробуту, якими б було доцільно доповнити існуючу систему управління безпекою праці та здоров'я працівників. Проведене дослідження, що складалося з восьми напівструктурованих інтерв'ю та дев'яносто п'яти відповідей на опитування серед керівників приватного та державного секторів, фахівців з охорони здоров'я, безпеки, добробуту та людського капіталу, показало, що подібні практики мають місце і потребують методологічного опрацювання для інтеграції в загальну систему управління організацією. Реалізація подібного підходу, на думку авторів, дозволить підвищити економічну привабливість організації.

У роботі [8] автори закликали до інноваційних та адаптивних підходів в системах управління охороною праці (БЗР). Це, на їхню думку, допоможе краще зрозуміти зростаючі проблеми безпеки праці, використати наявні можливості та вирішити виявлені проблеми. Автори пропонують запровадити рамкову програму “Загальне здоров'я працівників”, яка надає пріоритет принципам здорового планування праці для захисту та сприяння благополуччю працівників як на робочому місці, так і поза ним.

У роботах [9, 10] автори обговорюють аспекти розробки, впровадження та оцінки програми наставництва з питань здоров'я та благополуччя новоприйнятих працівників у виправних установах. Вважається, що працівники в таких установах підпадають під вплив високого ризику кумулятивного стресу. Автори виявили погіршення загального фізичного та психічного стану здоров'я у працівників, що змусило керівництво запровадити кілька соціальних програми для покращення стосунків між різними групами засуджених.

У роботі [11] автори досліджували рівень БЗР у закладах охорони здоров'я. Дійшли думки, що запровадження системи управління безпекою праці за стандартом ISO45001 є не достатнім для реального зменшення кількості професійних захворювань. Це пов'язано зі складнощами комунікації між усіма працівниками та пацієнтами. Особливо стресову напругу викликає невідповідність комунікації щодо конфіденційності особистої медичної інформації. На думку авторів, це потребує як мінімум інтеграції декількох стандартів для створення системи управління безпекою праці, а також створення відповідних програм по захисту психічного здоров'я, в яких були б описані дії щодо різноманітних стандартних ситуацій при взаємодії різних груп працівників і пацієнтів закладів охорони здоров'я.

У роботі [12] автори запропонували розширену модель управління БЗР, яка поєднує традиційну безпеку та гігієну праці з урахуванням особистих, соціальних та економічних факторів ризику із додатковими сферами діяльності людини, як благополуччя та здорового

способу життя. Це забезпечить керівникам компанії більше інструментів для мотивації й підтримки працівників у сфері БЗР для зменшення травматизму.

У роботі [13] говориться про добробут працівників та необхідність розширення та розвитку системи управління БЗР через призму стимулювання зміни у підходах до навчання, досліджень та розробки політики. Нова система управління безпекою праці повинна позиціонувати себе як сфера зусиль щодо запобігання небезпекам на робочому місці, забезпечення безпеки працівників та сприяння загальному добробуту працівників.

Постановка проблеми

Постановка проблеми полягає в аналізі концепцій охорони праці, безпеки праці і здоров'я на роботі та благополуччя працівників на роботі щодо пошуку подальших шляхів розвитку систем управління організаціями.

Методологія дослідження

Для розробки концепції благополуччя працівників на роботі використовувалась комбінація методів – порівняльного аналізу різних існуючих концепцій з охорони праці та бенчмаркінгу з елементами мозкового штурму. Під час порівняльного аналізу зосереджувались на визначенні основного фокусу концепції, області охоплення (які аспекти добробуту працівників вона покриває?), підходах (проактивний/реактивний), ключових заходах/інструментах, нормативно-правовій базі щодо з'ясування основ концепції, впливах на продуктивність/бізнес-результати, складності впровадження. Усі зазначені характеристики концепцій далі аналізувались з позицій залученості найкращих практик успішних компаній або галузей у сфері охорони праці для пошуку ідей на основі порівняння з існуючими рішеннями у галузі.

Результати

Концепція “Охорона праці” полягає у створенні безпечних і нешкідливих умов праці на кожному робочому місці, належних умов для формування у працівників свідомого ставлення до особистої безпеки та безпеки оточуючих, запровадженні нових і вдосконаленні існуючих механізмів управління в галузі охорони праці на підприємствах. Для цього передбачені правові, організаційні, науково-технічні, санітарно-гігієнічні, соціально-економічні, лікувально-профілактичні заходи. Разом вони утворюють жорстку систему правил, вимог і норм, які повинні забезпечити всеосяжний захист працівників. Разом з тим, це реактивна (реагуюча) концепція, яка зосереджується на діях після нещасного випадку, виявлення професійного захворювання чи інциденту (рис. 1).



Рисунок 1 – Базові складові концепції “Охорона праці”

Концепція “Безпека і здоров’я працівників на роботі” є рушійною силою поточної сучасної реформи, що зумовлено європейською інтеграцією України (рис. 2). Зазначена концепція ґрунтується на гнучкому, проактивному підході до створення безпечних і нешкідливих умов праці на кожному робочому місті, який орієнтований на постійне вдосконалення, адаптацію до змін та превентивне запобігання професійним ризикам замість статичного дотримання правил або реагування на вже наявні проблеми. Для цього передбачені превентивні, організаційні, технічні, санітарно-гігієнічні, медичні, психологічні та соціальні заходи, що дозволяють не тільки знизити травматизм, а вплинути на свідомість працівника щодо необхідності дотримання вимог з безпеки праці. При цьому для запровадження зазначених заходів передбачаються процеси керування ризиками, моніторингу, аудитів, постійне навчання працівників тощо. Разом вони запобігають появі небезпечних подій та раціонально розподіляють фінансування.



Рисунок 2 – Базові складові концепції “Безпека і здоров’я працівників на роботі”

Концепція “Благополуччя на роботі” є найновішою і найбільш дієвою щодо зниження втрат життя і здоров’я працівників на роботі. Ця концепція виходить за межі фізичної безпеки, тобто професійних ризиків, охоплює не тільки турботу про психічне, соціальне та фінансове здоров’я працівників, а й формує основу для підвищення якості особистого життя працівника, його задоволеності, можливості для розвитку та загального відчуття щастя. Цей тренд, що зароджується, значною мірою ініційований приватними підприємствами, став потужною відповіддю на безпрецедентні виклики та психологічні травми, спричинені повномасштабною війною (рис. 3).



Рисунок 3 – Базові складові концепції “Благополуччя працівників”

Загальний аналіз трьох зазначених концепцій наведено в табл. 1.

Таблиця 1 – Порівняльний аналіз трьох концепцій

Критерій	Концепції		
	Охорона праці	Безпека і здоров'я працівників на роботі	Благополуччя
Фокус	Фізична безпека, запобігання травмам і профзахворюванням	Комплексне здоров'я (фізичне, психічне, соціальне) на роботі	Всебічне благополуччя працівника (фізичне, психічне, соціальне, фінансове, професійне, суспільне)
Основна мета	Захист від небезпек, мінімізація ризиків травматизму	Створення здорового та безпечного робочого середовища	Сприяння розквіту, щастю та повноцінному життю працівників
Підхід	Переважно нормативно-правовий, реагуючий	Проактивний, системний	Холістичний, проактивний, стратегічний
Масштаб	Зосереджений на виробничих небезпеках	Зосереджений на аспектах підтримки здоров'я на роботі на основі своєчасного усунення ризиків	Зосереджений на аспектах підтримки здоров'я на роботі та підтримці щасливого особистого життя
Зиски	Зниження травматизму	Зниження травматизму і підвищення продуктивності	Зниження травматизму і плинності, підвищення продуктивності, залученості, інновацій, лояльності, іміджу

На тлі складних процесів реформування системи охорони праці та екзистенційних викликів війни в Україні почав формуватися новий, ще більш прогресивний підхід до турботи про працівників – концепція «благополуччя на роботі». Ця парадигма виходить далеко за межі традиційного фокусу щодо фізичної безпеки та гігієни праці охоплюючи психологічний, соціальний та фінансовий стан людини. Цікаво, що рушійною силою цього тренду став не державний примус чи законодавчі вимоги, а ініціатива провідних приватних компаній, які усвідомили, що в умовах національної кризи сталість бізнесу напряду залежить від стійкості та добробуту працівників.

Концепція “благополуччя на роботі” не є новою у світовій практиці, проте в Україні вона набуває особливого значення. На відміну від концепції «безпеки і здоров'я працівників на роботі», яка зосереджена на запобіганні шкоді працівникам та фокусується на керуванні професійними ризиками, “благополуччя” є цілісною концепцією, спрямованою на створення психологічно позитивного та підтримуючого робочого середовища. Незважаючи на відсутність єдиного, загальноприйнятого визначення, ця концепція зазвичай включає кілька ключових компонентів, які відрізняють її від концепцій “охорони праці” та “безпеки і здоров'я працівників на роботі” (рис. 4):

- **Психічне здоров'я**, тобто управління стресом, профілактика вигорання, надання доступу до професійної психологічної допомоги, розвиток емоційного інтелекту тощо.
- **Фізичне здоров'я**, тобто не лише запобігання травмам, а й заохочення здорового способу життя, профілактичні медичні огляди, програми правильного харчування, спортивні ініціативи тощо.

- **Фінансове благополуччя**, тобто справедлива та конкурентна оплата праці, програми підвищення фінансової грамотності, консультації щодо особистих фінансів, надання позик чи матеріальної допомоги тощо.
- **Соціальне благополуччя**, тобто побудова позитивної атмосфери в колективі, розвиток корпоративної культури, заходи для згуртування команди, підтримка балансу між роботою та особистим життям тощо.

В українському контексті становлення цієї концепції є прикладом «кризової інновації», яка виникла при воєнному стані. Якщо на Заході програми благополуччя часто є інструментом для утримання талантів та підвищення продуктивності на виробництві, то в Україні вони стають фундаментальним механізмом психологічного виживання та підтримки операційної стійкості працівників. Компанії, що їх впроваджують, фактично виконують роль служб психологічної та соціальної підтримки для своїх працівників, які перебувають під величезним тиском військової агресії.

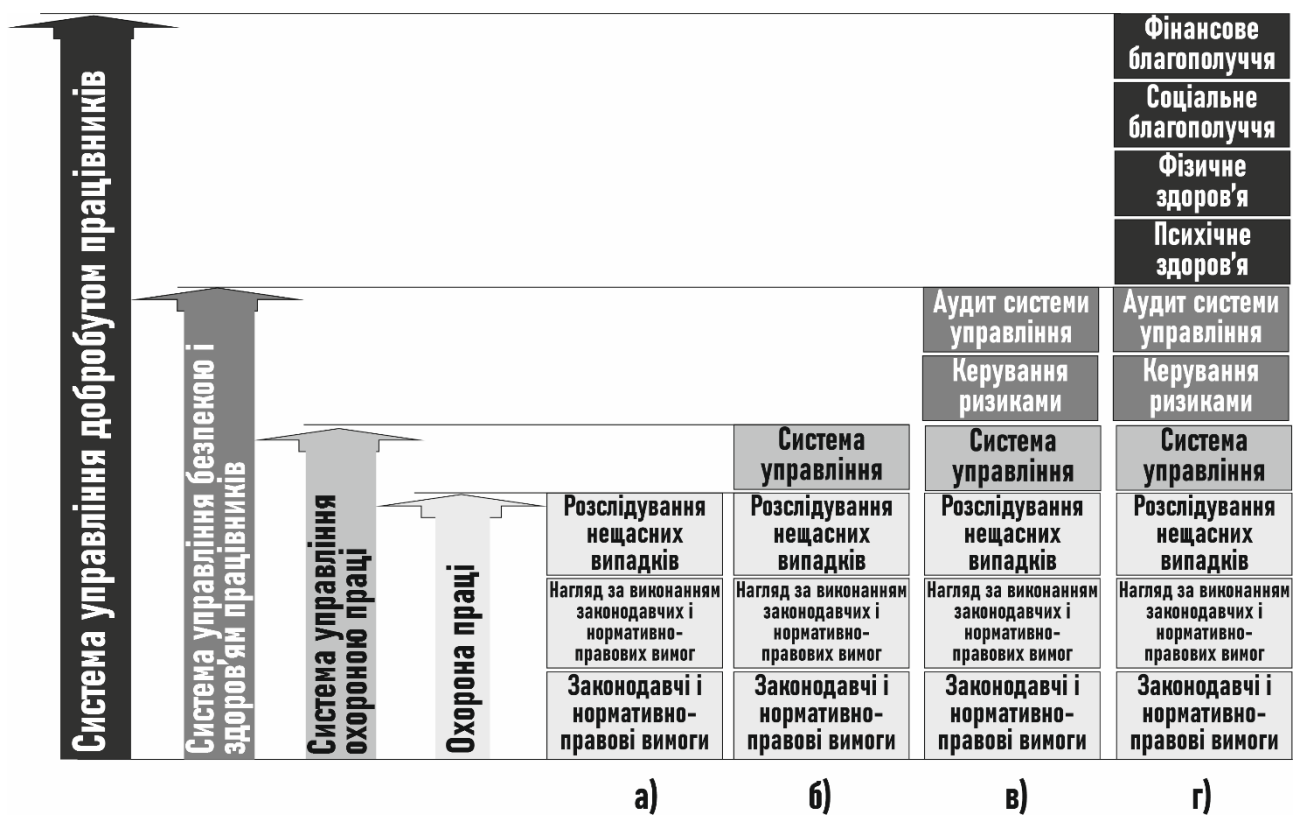


Рисунок 4 – Базові складові концепцій:

- а) “Охорона праці”; б) “Система управління охороною праці”; в) “Система управління безпекою і здоров'ям працівників”; г) “Система добробуту працівників”

Ініціативи приватного сектору у сфері благополуччя працівників мають величезний потенціал для формування майбутньої державної політики. Вони демонструють, що ринок, реагуючи на військовий стан, вже створює дієві моделі підтримки людського капіталу.

У контексті повоєнного відновлення України інтеграція принципів благополуччя, особливо у сфері психічного здоров'я, у національні стратегії безпеки і здоров'я працівників на роботі та соціальну політику буде мати вирішальне значення. Досвід компаній, які вже зараз надають психологічну підтримку працівникам і дбають про їхній добробут, може стати основою для впровадження систем управління безпекою, охороною здоров'я і добробутом працівників на роботі.

Таким чином, приватний сектор не лише випереджає державне регулювання, а й створює потужну нову модель державно-приватного партнерства у сфері відновлення людського капіталу України через побудову і впровадження систем управління безпекою, охороною здоров'я і добробутом працівників на роботі. Подальший розвиток цієї нової концепції “благополуччя” може стати невід'ємною частиною побудови нової, стійкої та незламної України.

Обговорення

Аналіз еволюції підходів до безпеки на робочому місці в Україні демонструє складний, багатоетапний процес трансформації, що відображає ширші історичні та геополітичні зміни в Україні [14, 15]. Україна перебуває в розпалі фундаментального переходу від успадкованої радянської, нормативної та реактивної концепції “охорона праці” до сучасної європейської, ризик-орієнтованої та проактивної концепції “безпека та здоров'я працівників на роботі”. Цей перехід є не лише юридичним зобов'язанням у рамках євроінтеграції, а й глибоким культурним та інституційним викликом [16].

Повномасштабна війна в Україні, розпочата російською федерацією, одночасно і прискорила усвідомлення цінності людського життя і здоров'я, і кардинально ускладнила процес реформ, ввівши нову категорію військових (екзистенційних) ризиків, до яких традиційні системи управління безпеки і здоров'я працівників на роботі не готові [17]. У відповідь на воєнний стан в Україні у приватному секторі зародилася прогресивна концепція “благополуччя на роботі”, що розширює фокус за межі фізичної безпеки до цілісної турботи про психічне, соціальне та фінансове здоров'я працівників, вказуючи на майбутній вектор розвитку. Звідси рекомендуємо запустити масштабну, багаторічну інформаційно-освітню кампанію, яка має включати розробку та поширення спрощених методичних посібників, секторних шаблонів оцінки професійних ризиків, проведення масових тренінгів для інспекторів праці, роботодавців та представників профспілок. Також провести інтеграцію військових ризиків у систему управління безпекою, охороною здоров'я і добробутом працівників на роботі. Для цього розробити спеціальні нормативні акти та рекомендації для роботодавців щодо керування професійними ризиками, пов'язаними із воєнним станом в Україні, що має включати вимоги до облаштування укриттів, протоколи дій під час повітряних тривог та інтеграцію планів цивільного захисту в загальну систему управління безпекою підприємства [18].

Не чекаючи на примус з боку держави, почати впроваджувати ризик-орієнтований підхід, принципи оцінки ризиків на своїх підприємствах, що дозволить не лише підвищити рівень безпеки, а й підготуватися до нових законодавчих вимог. Також поширювати найкращі практики у сфері добробуту, тобто активно обмінюватися досвідом щодо впровадження програм well-being, особливо тих, що спрямовані на подолання психологічних наслідків війни. Усе це сприятиме підвищенню стійкості всього бізнес-середовища [19, 20].

Висновки

1. Проведено аналіз трьох існуючих концепцій та визначено їх сильні сторони, які дозволяють зменшити кількість травматизму, підвищити продуктивність праці та створити умови для всебічного розвитку працівника.

2. Встановлено базові складові кожної концепції з охорони праці, безпеки і здоров'я працівників на роботі та благополуччя працівників на роботі, що стало основою для виявлення ключових ідей для розробки концепції благополуччя працівників на роботі.

3. Запропоновано, на основі аналізу законодавчих вимог щодо охорони праці та сучасних тенденцій щодо розвитку організацій, створення психологічно позитивного та підтримуючого робочого середовища на основі цілісної турботи про здоров'я працівників беручи до уваги майбутній вектор розвитку їх особистості.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Marhavilas, P.K., Pliaki, F., Koulouriotis, D. (2022). International Management System Standards Related to Occupational Safety and Health: An Updated Literature Survey. *Sustainability*, 14(20), 13282. <https://doi.org/10.3390/su142013282>
2. Domínguez, C.R., Guadian, J.E.R., Lona, J.G., Mares, J.I.P. (2023). Hazard identification for risk assessment using the PRA technique in the automotive industry. *Safety Science*, 160, 106041. <https://doi.org/10.1016/j.ssci.2022.106041>
3. Singh, N. (2024). Occupational safety and multiple management systems certifications: The influence of internationalisation of the firm. *Safety Science*, 169, 106324. <https://doi.org/10.1016/j.ssci.2023.106324>
4. Chatzoglou, P.D., Kotzakolios, A.E., Marhavilas, P.K. (2025). Health and Safety Management System (HSMS) and Its Impact on Employee Satisfaction and Performance – A New HSMS Model. *Safety*, 11(2), 52. <https://doi.org/10.3390/safety11020052>
5. Halliday, B., van der Laan, L., Raineri, A. (2024). Prioritizing Work Health, Safety, and Wellbeing in Corporate Strategies: An Indicative Framework. *Safety*, 10, 18. <https://doi.org/10.3390/safety10010018>
6. Roman, G., Demian, C., Love, T., Yousefi-Nooraie, R. (2024). Occupational Safety, Health, and Well-Being Concerns and Solutions for Management Reported by Sign Language Interpreters: A Qualitative Study. *International Journal of Environmental Research and Public Health*, 21, 1400. <https://doi.org/10.3390/ijerph21111400>
7. Mixafenti, S., Moutzouri, A., Karagkouni, A., Sartzetaki, M., Dimitriou, D. (2025). Assessment of Occupational Health and Safety Management: Implications for Corporate Performance in the Secondary Sector. *Safety*, 11, 44. <https://doi.org/10.3390/safety11020044>
8. Yeşilgöz, P., Arga, K.Y. (2025). A Health-Sector-Specific Occupational Health and Safety Management System Model. *Healthcare*, 13, 271. <https://doi.org/10.3390/healthcare13030271>
9. Namazi, S., Kotejoshyer, R., Farr, D., Henning, R.A., Tubbs, D.C., Dugan, A.G., El Ghaziri, M., Cherniack, M. (2021). Development and Implementation of a Total Worker Health® Mentoring Program in a Correctional Workforce. *International Journal of Environmental Research and Public Health*, 18, 8712. <https://doi.org/10.3390/ijerph18168712>
10. Kotejoshyer, R., Gilmer, D.O., Namazi, S., Farr, D., Henning, R.A., Cherniack, M. (2021). Impact of a Total Worker Health® Mentoring Program in a Correctional Workforce. *International Journal of Environmental Research and Public Health*, 18, 8436. <https://doi.org/10.3390/ijerph18168436>
11. Tamers, S.L., Streit, J.M.K., Chosewood, C. (2022). Promising Occupational Safety, Health, and Well-Being Approaches to Explore the Future of Work in the USA: An Editorial. *International Journal of Environmental Research and Public Health*, 19, 1745. <https://doi.org/10.3390/ijerph19031745>
12. Schulte, P.A., Delclos, G., Felknor, S.A., Chosewood, L.C. (2019). Toward an expanded focus for occupational safety and health: A commentary. *International Journal of Environmental Research and Public Health*, 16, 4946. <https://doi.org/10.3390/ijerph16244946>

13. Schulte, P.A., Delclos, G.L., Felknor, S.A., Streit, J.M.K., McDaniel, M., Chosewood, L.C., Newman, L.S., Bhojani, F.A., Pana-Cryan, R., Swanson, N.G. (2022). Expanding the Focus of Occupational Safety and Health: Lessons from a Series of Linked Scientific Meetings. *International Journal of Environmental Research and Public Health*, 19, 15381. <https://doi.org/10.3390/ijerph192215381>
14. Benson C., Obasi I.C., Akinwande D.V., Ile C. (2023). The impact of interventions on health, safety and environment in the process industry. *Heliyon*, 10(1), e23604. <https://doi.org/10.1016/j.heliyon.2023.e23604>
15. Цопа, В.А., Голінько, В.І., Чеберячко, С.І., Дерюгін, О.В. (2024). Взаємозв'язок концепцій «Охорона праці» та «Безпека праці і здоров'я працівників». *Проблеми охорони праці в Україні*, 40(3-4), 24-31. <https://doi.org/10.36804/nndipbop.40-3-4.2024.24-31>
16. Цопа, В., Болібрux, Б., Колесник, В., Чеберячко, С., Дерюгін, О., & Шароватова, О. (2024). Взаємозв'язок між стадіями розвитку організації і рівнем культури безпеки праці. *Social Development and Security*, 14(6), 138-152. <https://doi.org/10.33445/sds.2024.14.6.14>
17. Çalış, S., Büyükakıncı, B.Y. (2019). Occupational Health and Safety Management Systems Applications and A System Planning Model. *Procedia Computer Science*, 158, 1058-1066. <https://doi.org/10.1016/j.procs.2019.09.147>
18. Mtikitiki, N., Madonsela, B.S., Maphanga, T., Shale, K., Grangxabe, X.S., Baloyi, T.M. (2025). Occupational Health and Safety Management System of a South African University Setting. *Safety*, 11(2), 34. <https://doi.org/10.3390/safety11020034>
19. Tejamaya, M., Puspoprodjo, W., Susetyo, H., Modjo, R. (2021). An analysis of pivotal factors in the implementation of occupational health and safety management systems in micro, small and medium enterprises (MSMEs): Literature review. *Gaceta Sanitaria*, 35(2), S348-S359. <https://doi.org/10.1016/j.gaceta.2021.10.050>
20. Gorgenyi-Hegyes, E., Nathan, R.J., Fekete-Farkas, M. (2021). Workplace Health Promotion, Employee Wellbeing and Loyalty during Covid-19 Pandemic—Large Scale Empirical Evidence from Hungary. *Economies*, 9(2), 55. <https://doi.org/10.3390/economies9020055>

References

1. Marhavilas, P.K., Pliaki, F., Koulouriotis, D. (2022). International Management System Standards Related to Occupational Safety and Health: An Updated Literature Survey. *Sustainability*, 14(20), 13282. <https://doi.org/10.3390/su142013282>
2. Domínguez, C.R., Guadian, J.E.R., Lona, J.G., Mares, J.I.P. (2023). Hazard identification for risk assessment using the PRA technique in the automotive industry. *Safety Science*, 160, 106041. <https://doi.org/10.1016/j.ssci.2022.106041>
3. Singh, N. (2024). Occupational safety and multiple management systems certifications: The influence of internationalisation of the firm. *Safety Science*, 169, 106324. <https://doi.org/10.1016/j.ssci.2023.106324>
4. Chatzoglou, P.D., Kotzakolios, A.E., Marhavilas, P.K. (2025). Health and Safety Management System (HSMS) and Its Impact on Employee Satisfaction and Performance – A New HSMS Model. *Safety*, 11(2), 52. <https://doi.org/10.3390/safety11020052>
5. Halliday, B., van der Laan, L., Raineri, A. (2024). Prioritizing Work Health, Safety, and Wellbeing in Corporate Strategies: An Indicative Framework. *Safety*, 10, 18. <https://doi.org/10.3390/safety10010018>
6. Roman, G., Demian, C., Love, T., Yousefi-Nooraie, R. (2024). Occupational Safety, Health, and Well-Being Concerns and Solutions for Management Reported by Sign Language Interpreters: A Qualitative Study. *International Journal of Environmental Research and Public Health*, 21, 1400. <https://doi.org/10.3390/ijerph21111400>

7. Mixafenti, S., Moutzouri, A., Karagkouni, A., Sartzetaki, M., Dimitriou, D. (2025). Assessment of Occupational Health and Safety Management: Implications for Corporate Performance in the Secondary Sector. *Safety*, 11, 44. <https://doi.org/10.3390/safety11020044>
8. Yeşilgöz, P., Arga, K.Y. (2025). A Health-Sector-Specific Occupational Health and Safety Management System Model. *Healthcare*, 13, 271. <https://doi.org/10.3390/healthcare13030271>
9. Namazi, S., Kotejshyer, R., Farr, D., Henning, R.A., Tubbs, D.C., Dugan, A.G., El Ghaziri, M., Cherniack, M. (2021). Development and Implementation of a Total Worker Health® Mentoring Program in a Correctional Workforce. *International Journal of Environmental Research and Public Health*, 18, 8712. <https://doi.org/10.3390/ijerph18168712>
10. Kotejshyer, R., Gilmer, D.O., Namazi, S., Farr, D., Henning, R.A., Cherniack, M. (2021). Impact of a Total Worker Health® Mentoring Program in a Correctional Workforce. *International Journal of Environmental Research and Public Health*, 18, 8436. <https://doi.org/10.3390/ijerph18168436>
11. Tamers, S.L., Streit, J.M.K., Chosewood, C. (2022). Promising Occupational Safety, Health, and Well-Being Approaches to Explore the Future of Work in the USA: An Editorial. *International Journal of Environmental Research and Public Health*, 19, 1745. <https://doi.org/10.3390/ijerph19031745>
12. Schulte, P.A., Delclos, G., Felknor, S.A., Chosewood, L.C. (2019). Toward an expanded focus for occupational safety and health: A commentary. *International Journal of Environmental Research and Public Health*, 16, 4946. <https://doi.org/10.3390/ijerph16244946>
13. Schulte, P.A., Delclos, G.L., Felknor, S.A., Streit, J.M.K., McDaniel, M., Chosewood, L.C., Newman, L.S., Bhojani, F.A., Pana-Cryan, R., Swanson, N.G. (2022). Expanding the Focus of Occupational Safety and Health: Lessons from a Series of Linked Scientific Meetings. *International Journal of Environmental Research and Public Health*, 19, 15381. <https://doi.org/10.3390/ijerph192215381>
14. Benson C., Obasi I.C., Akinwande D.V., Ile C. (2023). The impact of interventions on health, safety and environment in the process industry. *Heliyon*, 10(1), e23604. <https://doi.org/10.1016/j.heliyon.2023.e23604>
15. Цопа, В.А., Голінько, В.І., Чеберячко, С.І., Дерюгін, О.В. (2024). Взаємозв'язок концепцій «Охорона праці» та «Безпека праці і здоров'я працівників». *Проблеми охорони праці в Україні*, 40(3-4), 24-31. <https://doi.org/10.36804/nndipbop.40-3-4.2024.24-31>
16. Цопа, В., Болібрux, Б., Колесник, В., Чеберячко, С., Дерюгін, О., & Шароватова, О. (2024). Взаємозв'язок між стадіями розвитку організації і рівнем культури безпеки праці. *Social Development and Security*, 14(6), 138-152. <https://doi.org/10.33445/sds.2024.14.6.14>
17. Çalış, S., Büyükkakıncı, B.Y. (2019). Occupational Health and Safety Management Systems Applications and A System Planning Model. *Procedia Computer Science*, 158, 1058-1066. <https://doi.org/10.1016/j.procs.2019.09.147>
18. Mtikitiki, N., Madonsela, B.S., Maphanga, T., Shale, K., Grangxabe, X.S., Baloyi, T.M. (2025). Occupational Health and Safety Management System of a South African University Setting. *Safety*, 11(2), 34. <https://doi.org/10.3390/safety11020034>
19. Tejamaya, M., Puspoprodjo, W., Susetyo, H., Modjo, R. (2021). An analysis of pivotal factors in the implementation of occupational health and safety management systems in micro, small and medium enterprises (MSMEs): Literature review. *Gaceta Sanitaria*, 35(2), S348-S359. <https://doi.org/10.1016/j.gaceta.2021.10.050>
20. Gorgenyi-Hegyes, E., Nathan, R.J., Fekete-Farkas, M. (2021). Workplace Health Promotion, Employee Wellbeing and Loyalty during Covid-19 Pandemic—Large Scale Empirical Evidence from Hungary. *Economies*, 9(2), 55. <https://doi.org/10.3390/economies9020055>

Застосування нейронних мереж для вибору інструментів для тестування на проникнення

Application of Neural Networks for Selecting Tools for Penetration Testing

Андріан Піскозуб ^A

Corresponding author: к. тех. Н., доцент кафедри захисту інформації, e-mail: azpiskozub@gmail.com, ORCID: 0000-0002-3582-2835

Анастасія Журавчак ^A

аспірантка, асистентка кафедри захисту інформації, e-mail: anastasiia.y.tolkachova@lpnu.ua, ORCID: 0000-0002-8196-7963

Даниїл Журавчак ^A

доктор філософії, асистент кафедри захисту інформації, e-mail: danyil.y.zhuravchak@lpnu.ua, ORCID: 0000-0003-4989-0203

Юрій Журавчак ^A

магістр, кафедра інформаційних систем та технологій, e-mail: yurii.zhuravchak.mitis.2023@lpnu.ua, ORCID: 0009-0003-2378-5365

Ігор Беляєв ^B

аспірант, асистент кафедри кібербезпеки, e-mail: igor@beliaiev.com, ORCID: 0009-0005-8130-7972

Andriian Piskozub ^A

Corresponding author: PhD. in Engineering, Associate Professor, Department of Information Security, e-mail: azpiskozub@gmail.com, ORCID: 0000-0002-3582-2835

Anastasiia Zhuravchak ^A

PhD student, Associate Assistant, Department of Information Security, e-mail: anastasiia.y.tolkachova@lpnu.ua, ORCID: 0000-0002-8196-7963

Danyil Zhuravchak ^A

PhD, Associate Professor, Department of Information Security, e-mail: danyil.y.zhuravchak@lpnu.ua, ORCID: 0000-0003-4989-0203

Yurii Zhuravchak ^A

Master's Degree, Institute of Computer Science and Information Technology, e-mail: yurii.zhuravchak.mitis.2023@lpnu.ua, ORCID: 0009-0003-2378-5365

Igor Beliaiev ^B

PhD student, Associate Assistant, Department of Cybersecurity, e-mail: igor@beliaiev.com, ORCID: 0009-0005-8130-7972

^A Національний університет "Львівська політехніка", м. Львів, Україна

^B Львівський Національний університет імені Івана Франка, м. Львів, Україна

^A Lviv Polytechnic National University, Lviv, Ukraine

^B Ivan Franko National University of Lviv, Lviv, Ukraine

Received: June 13, 2025 | Revised: August 23, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.12>

Мета роботи. Розробити метод автоматизованого вибору інструментів для тестування на проникнення веб-додатків за допомогою нейронних мереж.

Метод дослідження. Побудова нейронної мережі прямого поширення з навчанням за методом зворотного поширення помилки на основі даних експертів та користувачів, поданих у вигляді матриці характеристик інструментів. Реалізація моделі через веб-сервіс з використанням стеку LAMP і бібліотеки FANN.

Результати дослідження. Створено веб-застосунок, що дозволяє користувачам задавати критерії до інструментів тестування, а система надає відповідні рекомендації. Навчена нейронна мережа демонструє ефективність у виборі утиліт згідно з вхідними параметрами, що підтверджується експериментами з утилітами Acunetix, Nessus та Nexpose. Система враховує як експертні дані, так і користувацький зворотний зв'язок, що забезпечує її динамічну адаптацію.

Теоретична цінність дослідження. Обґрунтовано ефективність застосування нейромереж для автоматизованого підбору інструментів у сфері кібербезпеки, що відкриває нові підходи до інтеграції машинного навчання у процеси тестування на проникнення.

Практична цінність дослідження. Розроблений веб-сервіс може використовуватись як допоміжний інструмент тестувальниками безпеки, зокрема початківцями, для швидкого та обґрунтованого вибору засобів тестування.

Цінність дослідження. Дослідження демонструє, що застосування нейромереж дозволяє підвищити ефективність вибору інструментів та спростити процес прийняття рішень при тестуванні веб-додатків.

Майбутні дослідження. Удосконалення архітектури моделі, пояснюваність рішень нейромережі, масштабування системи на більші обсяги даних та розширення спектра інструментів.

Тип статті. Прикладне дослідження.

Purpose. To develop a method for the automated selection of penetration testing tools for web applications using neural networks.

Method. Construction of a feedforward neural network trained with the backpropagation algorithm using expert and user data represented as a matrix of tool characteristics. Implementation of the model through a web service using the LAMP stack and FANN library.

Findings. A web application was developed that allows users to specify criteria for testing tools, and the system provides appropriate recommendations. The trained neural network demonstrates effectiveness in selecting utilities based on input vectors, confirmed by experiments with Acunetix, Nessus, and Nexpose. The system incorporates both expert data and user feedback, ensuring its dynamic adaptation.

Theoretical implications. The study substantiates the effectiveness of neural networks for the automated selection of tools in cybersecurity, paving the way for new approaches to integrating machine learning into penetration testing processes.

Practical implications. The developed web service can be used as an auxiliary tool by security testers, especially beginners, for fast and justified selection of testing tools.

Value. The study shows that the application of neural networks increases the efficiency of tool selection and simplifies decision-making during web application testing.

Future research. Improving the model architecture, explainability of neural network decisions, scaling the system to larger datasets, and expanding the toolset.

Paper type. Applied study.

Ключові слова: штучний інтелект, тестування на проникнення, інструменти безпеки, нейронні мережі, автоматизація, машинне навчання.

Key words: artificial intelligence, penetration testing, security tools, neural networks, automation, machine learning.

Вступ

У даній науковій статті розглядається актуальна проблема вибору інструментальних засобів для проведення тестування на проникнення веб-додатків. Тестування на проникнення спрямоване на виявлення та усунення вразливостей, а використання інструментальних засобів дозволяє автоматизувати рутинні операції. Однак, тестувальники, особливо початківці, стикаються зі складнощами у виборі найбільш підходящих утиліт для конкретних завдань безпеки, оскільки існує багато схожих інструментів. Стаття починається з аналізу проблематики вибору утиліт для тестування безпеки, зокрема процесів формування власних наборів інструментів досвідченими тестувальниками. Автори пропонують метод вирішення цієї проблеми за допомогою створення веб-сервісу, що використовує нейромережу для аналізу критеріїв вибору та рекомендацій інструментів. Нейромережу навчають на основі даних, зібраних експертами з тестування безпеки, у вигляді матриці утиліт та їхніх характеристик. Користувач сервісу може зазначити критерії для пошуку інструментів, а система надасть кілька найвідповідніших варіантів. Також враховується можливість коригування вибору користувачем, що дозволяє розширювати базу навчальних даних. Запропонований підхід включає створення двох моделей нейромереж: одна навчається виключно на даних експертів, а інша враховує також дані користувачів. Це забезпечує динамічну адаптацію системи до нових вимог і зворотного зв'язку. Результати дослідження демонструють, що використання нейромереж для вибору інструментів дозволяє підвищити ефективність тестування безпеки. Запропонований метод може бути застосований не лише для вибору засобів тестування веб-додатків, а й для інших сфер програмного забезпечення.

Теоретичні основи дослідження

Сьогодні широкого використання набули інструменти для автоматизації тестування на проникнення. Вони дозволяють зменшити обсяг рутинних завдань і підвищити ефективність роботи. Водночас різноманітність таких інструментів і їхніх функціональних можливостей створює проблему вибору оптимального рішення для конкретних завдань. Наприклад, одні сканери чудово знаходять вразливості, пов'язані з конфігурацією серверів, але пропускають помилки логіки застосунку. Інші можуть мати високий відсоток хибнопозитивних спрацювань [1]. Таким чином, вибір інструментів залишається критичною точкою в проведенні тестувань, який потребує значного часу на аналіз доступних рішень та їхнє порівняння. Використання нейромереж може стати вирішенням цієї проблеми. Вони здатні обробляти великі обсяги даних та підбирати найкращий інструмент для тестування. Нейромережі також можуть допомагати в класифікації вразливостей, прогнозуванні можливих атак і покращенні ефективності використання існуючих інструментів [2]. У сучасних умовах проблема вибору ефективних інструментів для тестування набуває дедалі більшої актуальності. Існуючі рішення часто мають обмежену сферу застосування, а їхній вибір потребує значних витрат часу та експертних знань. Водночас автоматизація цього процесу із застосуванням методів нейромереж залишається недостатньо дослідженою, що стримує її впровадження у практику.

Головною проблемою, що стоїть перед дослідниками, є недостатня адаптованість нейромереж до змінюваних умов і завдань пентесту. Також залишається відкритим питання інтеграції таких рішень у процес пентесту без втрати ефективності та точності. Ці виклики потребують комплексного аналізу та пошуку інноваційних рішень, що дозволять значно покращити якість тестування на проникнення.

Постановка проблеми

У сучасних умовах кіберзагроз тестування на проникнення (penetration testing) стало ключовим елементом забезпечення безпеки веб-додатків. Одним із критичних аспектів цього

процесу є правильний вибір інструментів для виявлення вразливостей, адже від нього залежить як повнота, так і точність аналізу. Ринок пропонує велику кількість утиліт, що мають схожі функціональні можливості, однак різну ефективність у залежності від типу атак, що ускладнює вибір, особливо для початківців.

У роботі [2] P. Gallus та ін. досліджується застосування генеративних нейронних мереж, таких як ChatGPT, для автоматизації процесів тестування на проникнення веб-додатків. Основну увагу приділено використанню цих моделей для генерації сценаріїв атак і автоматичного виявлення вразливостей у популярних платформах, зокрема WordPress. Авторами підкреслено ефективність таких підходів у підвищенні швидкості аналізу безпеки та зниженні вимог до експертних знань тестувальників. Однак, робота обмежується розглядом лише генеративних моделей і не охоплює їх інтеграцію з іншими методами тестування на проникнення, такими як аналіз поведінкових моделей або розширення до багатокomпонентних архітектур.

У дослідженні [3] K. Pozdniakov та ін. запропоновано підхід до автоматизації аудиту безпеки з використанням методів підкріплюючого навчання у поєднанні з глибокими нейронними мережами. Основна ідея роботи полягає у застосуванні алгоритму Q-навчання для визначення оптимальних стратегій тестування, що дозволяє автоматично адаптуватися до різних систем і середовищ. Авторами відзначено значний потенціал запропонованого підходу в підвищенні ефективності тестування на проникнення, зокрема у складних і динамічних середовищах. Однак, у статті відсутній глибокий аналіз обмежень, пов'язаних із продуктивністю моделі, коли вона застосовується до великомасштабних корпоративних систем або середовищ із високим рівнем варіативності вразливостей.

У роботі [4] M. Pawlicki та ін. представлено детальний огляд викликів та можливостей використання штучних нейронних мереж у сфері кібербезпеки, зокрема для систем виявлення вторгнень (IDS). У статті розглянуто проблеми налаштування гіперпараметрів, забезпечення збалансованості датасетів і захисту моделей від атак. Додатково автори акцентують увагу на нетехнічних аспектах, таких як етичні, правові та суспільні виклики, що виникають при впровадженні цих технологій. У роботі також наведено приклади реальних впроваджень, які підтверджують ефективність нейронних мереж у виявленні аномалій і загроз. Однак, ключовою проблемою, відзначеною авторами, є обмежена інтерпретованість моделей, що може ускладнювати їх прийняття у практичних сценаріях.

Підсумовуючи ці дослідження, можна зазначити, що сучасні підходи до застосування нейронних мереж у тестуванні на проникнення демонструють значний потенціал у підвищенні ефективності та автоматизації процесів кібербезпеки. Генеративні моделі, такі як ChatGPT [5], дозволяють створювати сценарії атак, а методи підкріплюючого навчання сприяють адаптації систем до динамічних середовищ і складних системних архітектур. Водночас систематичні огляди підкреслюють необхідність вирішення таких викликів, як налаштування гіперпараметрів, збалансування даних та забезпечення захисту самих моделей від атак.

Таким чином, можна помітити існуючу необхідність у подальших дослідженнях для забезпечення інтеграції цих методів у реальних корпоративних середовищах. Зокрема, потребує розвитку питання пояснюваності моделей, розширення наборів даних для різноманітних сценаріїв атак, а також створення комплексних рішень, що об'єднують різні підходи, такі як генеративні нейромережі, підкріплююче навчання та традиційні методи кібербезпеки.

Методологія

Навчання нейромережі відбувається на основі даних, отриманих від експертів у сфері тестування на проникнення. У загальному вигляді дані можуть бути описані таким чином.

$$M = \begin{cases} m_{11}, m_{12}, \dots, m_{1n}, \\ m_{21}, m_{22}, \dots, m_{2n}, \\ m_{k1}, m_{k2}, \dots, m_{kn}, \end{cases} \quad (1)$$

де M – матриця значень критеріїв інструментальних засобів;
 m – значення критерію засобу;
 k – розмір множини критеріїв;
 n – розмір множини утиліт.

Фрагмент даних, які можуть бути використані для навчання наведено в таблиці 1. Ці дані було отримано в результаті перевірки кількох сканерів на тестовому майданчику. За допомогою сканерів перевіряли характерні для Web-додатків вектори атак.

Таблиця 1 – Дані для перевірки сканерів у тестовому середовищі

Критерії	Acunetix	Nexpose	Nessus
Server-Side Template Injection	1	1	0
Stored Cross Site Scripting	1	1	1
Reflect Cross Site Scripting	1	0	0
Cross Site Request Forgery	1	0	0
Weak CORS	1	1	1
HTML injection	0	1	0
CSS Injection	0	1	0
Host Header Injection	1	1	1
Server-Side Request Forgery	1	0	0
XML Injection	1	1	1
HTTP Splitting Smuggling	1	0	0
HTTP Incoming Requests	1	0	1
XPath Injection	0	0	1
SQL Injection	1	1	0
SSI Injection	1	0	0

Як зазначалося раніше, множину навчальних прикладів можна розширити, враховуючи думки користувачів щодо відповідності вектора вимог та утиліт, які були запропоновані як найбільш відповідні за заданим вектором. Такі дані не можна використовувати без попередньої перевірки на наявність суперечностей. Під суперечностями розуміється відповідність однакових наборів вхідних даних різним наборам вихідних даних. Під час навчання на суперечливих прикладах результат роботи нейромережі буде непередбачуваним. Для вирішення поставленого завдання використовується нейромережа прямого поширення, а для навчання з учителем застосовується метод зворотного поширення помилки [6].

Архітектура веб-сервісу. Для реалізації завдання вибору інструментів для тестування на проникнення пропонується створити веб-сервіс, основною частиною логіки якого на серверній стороні буде нейронна мережа. Розроблений сайт допомагатиме початківцям у тестуванні на проникнення обирати інструменти. Для реалізації нейронної мережі пропонується використовувати бібліотеку FANN (Fast Artificial Neural Network) [7] у поєднанні з традиційним програмним стеком LAMP для веб-застосунків (Linux + Apache + MySQL + PHP). Усі використані технології є безкоштовними. Загальний вигляд архітектури веб-застосунку наведено на рисунку 1.

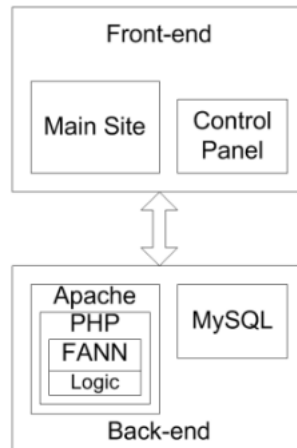


Рисунок 1 – Короткий опис архітектури

Основна частина сайту доступна всім користувачам, і за її допомогою користувач відповідатиме на запитання, формуючи таким чином вектор вимог для пошуку інструментів. Панель управління є закритою та доступна лише адміністратору сайту. За допомогою панелі управління адміністратор виконує такі дії:

1. Додавання нових інструментів у систему.

Технології розвиваються, з'являються нові уразливості та нові напрями атак. Інструменти для виявлення цих уразливостей також повинні оновлюватися, щоб ідентифікувати актуальні проблеми безпеки веб-застосунків. Якщо випускається новий інструмент, якого ще немає в системі, адміністратор може додати його до списку інструментів.

2. Додавання нових характеристик інструментів.

Кожен інструмент визначається певним набором характеристик. Якщо новий інструмент має унікальні характеристики, адміністратор може додати їх до загального списку характеристик.

3. Визначення значень характеристик інструментів.

На основі таблиці вхідних даних адміністратор вводить відповідні значення для кожної характеристики кожного інструмента.

Інформація про інструменти та їх характеристики зберігається у базі даних. Ці дані використовуються для навчання нейронної мережі. Крім того, результати вибору інструментів користувачами також зберігаються у базі даних. Це дозволяє користувачам зберігати результати свого вибору, якщо їхній вибір відрізняється від запропонованого.

Приклад реалізації нейронної мережі

Розглянемо приклад створення нейронної мережі та її навчання на даних, наведених у таблиці 1. Параметри нейронної мережі:

кількість вхідних нейронів – 15 (відповідає кількості критеріїв утиліт);

кількість вихідних нейронів – 3 (відповідає кількості утиліт);

кількість прихованих шарів – 2;

кількість нейронів у прихованих шарах – 9 і 6 відповідно.

Немає суворих правил для вибору кількості нейронів у прихованих шарах, зазначені вище значення отримані за допомогою правила геометричної піраміди.

Результати

У таблиці 2 наведено декілька прикладів вхідних даних та результат роботи нейронної мережі. Результат складається з трьох чисел, що відповідають трьом утилітам. Чим ближче значення

до одиниці, тим більша впевненість нейронної мережі в тому, що утиліта відповідає заданому вектору вимог.

Таблиця 2 – Результати роботи нейромережі

#	Вхідні дані	Результат
1	1; 1; 1; 1; 1; 0; 0; 1; 1; 1; 1; 1; 0; 1; 1	0.978; 0.234; 0.002
2	1; 1; 0; 0; 1; 1; 1; 1; 0; 1; 0; 0; 0; 1; 0	0.923; 0.124; -0.078
3	0; 1; 0; 0; 1; 0; 0; 1; 0; 1; 0; 1; 1; 0; 0	0.854; 0.000; 0.612

У першому прикладі нейронна мережа обрала лише першу (0.978) і другу (0.234) утиліти, оскільки їхні результати є додатними. Третя утиліта (0.002) не була обрана, оскільки її значення є нижчим за поріг прийняття рішення. Вхідний вектор: (1; 1; 1; 1; 1; 0; 0; 1; 1; 1; 1; 1; 0; 1; 1).

У другому прикладі нейронна мережа обрала лише першу утиліту (0.923), оскільки результати для другої (-0.124) і третьої (-0.078) утиліт були негативними. Це вказує на те, що заданий вектор (1; 1; 0; 0; 1; 1; 1; 1; 0; 1; 0; 0; 0; 1; 0) відповідав лише першій утиліті.

У третьому прикладі нейронна мережа обрала першу (0.854) і третю (0.612) утиліти. Друга утиліта (0.000) не була обрана через відсутність позитивного значення. Вхідний вектор: (0; 1; 0; 0; 1; 0; 1; 0; 1; 1; 0; 1; 0; 0; 0). Для практичного використання нейронна мережа повинна бути навчена на даних про 50-100 утиліт. Наведений вище приклад є лише демонстрацією її можливостей.

Обговорення

У ході дослідження авторами запропоновано метод вирішення завдання вибору інструментальних засобів для тестування веб-застосунків на проникнення. Описано вхідні дані для створення веб-сервісу, що реалізує запропонований метод.

Перевага використання нейронних мереж полягає в простоті реалізації порівняно з детермінованими алгоритмами; як метрика використовується кількість рядків коду. До недоліків можна віднести необхідність експериментального підбору параметрів нейронної мережі. Додатковою складністю є пошук даних для навчання через високі вимоги до експертів, які надають навчальні дані для нейронної мережі.

Напрямок подальших досліджень полягає у вивченні впливу параметрів нейронної мережі на результати її роботи.

Висновки

У результаті дослідження запропоновано метод автоматизованого вибору інструментів для тестування на проникнення веб-додатків, що базується на використанні нейронних мереж. Метод дозволяє ефективно аналізувати критерії вибору інструментів та надавати рекомендації, зважаючи на дані, отримані від експертів та користувачів. Основними перевагами підходу є простота реалізації та можливість динамічної адаптації до змін у вимогах тестування безпеки. Запропонований метод забезпечує підвищення ефективності процесу вибору інструментів, зменшуючи час і складність завдання для користувачів. Проте дослідження виявило ряд викликів, зокрема:

- необхідність експериментального налаштування параметрів нейронної мережі;
- складність у зборі якісних навчальних даних через високі вимоги до експертних знань.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Tolkachova, A., & Piskozub, A. (2024). Methods for testing the security of web applications. *Cybersecurity: Education, Science, Technique*, 2(26), 115–122. <https://doi.org/10.28925/2663-4023.2024.26.668>
2. Chowdhary, A., Jha, K., & Zhao, M. (2023). Generative adversarial network (GAN)-based autonomous penetration testing for web applications. *Sensors*, 23(18), 8014. <https://doi.org/10.3390/s23188014>
3. Pozdniakov, K., Alonso, E., Stankovic, V., Tam, K., & Jones, K. (2020, June 15–19). Smart security audit: Reinforcement learning with a deep neural network approximator. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–8). IEEE. <https://doi.org/10.1109/CyberSA49311.2020.9139683>
4. Pawlicki, M., Kozik, R., & Choraś, M. (2022, June). A survey on neural networks for (cyber-)security and (cyber-) security of neural networks. *Neurocomputing*. <https://doi.org/10.1016/j.neucom.2022.06.002>
5. Aljanabi, M., & ChatGPT. (2023, January). ChatGPT: Future directions and open possibilities. *Mesopotamian Journal of Cyber Security*, 16–17. <https://doi.org/10.58496/mjcs/2023/003>
6. Yam, Y. F., & Chow, T. W. S. (1993). Extended backpropagation algorithm. *Electronics Letters*, 29(19), 1701–1702. <https://doi.org/10.1049/el:19931131>
7. Wicht, B., Fischer, A., & Hennebert, J. (2018). DLL: A fast deep neural network library. In *Artificial Neural Networks in Pattern Recognition* (pp. 54–65). Springer International Publishing. https://doi.org/10.1007/978-3-319-99978-4_4

References

1. Tolkachova, A., & Piskozub, A. (2024). Methods for testing the security of web applications. *Cybersecurity: Education, Science, Technique*, 2(26), 115–122. <https://doi.org/10.28925/2663-4023.2024.26.668>
2. Chowdhary, A., Jha, K., & Zhao, M. (2023). Generative adversarial network (GAN)-based autonomous penetration testing for web applications. *Sensors*, 23(18), 8014. <https://doi.org/10.3390/s23188014>
3. Pozdniakov, K., Alonso, E., Stankovic, V., Tam, K., & Jones, K. (2020, June 15–19). Smart security audit: Reinforcement learning with a deep neural network approximator. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–8). IEEE. <https://doi.org/10.1109/CyberSA49311.2020.9139683>
4. Pawlicki, M., Kozik, R., & Choraś, M. (2022, June). A survey on neural networks for (cyber-)security and (cyber-) security of neural networks. *Neurocomputing*. <https://doi.org/10.1016/j.neucom.2022.06.002>
5. Aljanabi, M., & ChatGPT. (2023, January). ChatGPT: Future directions and open possibilities. *Mesopotamian Journal of Cyber Security*, 16–17. <https://doi.org/10.58496/mjcs/2023/003>
6. Yam, Y. F., & Chow, T. W. S. (1993). Extended backpropagation algorithm. *Electronics Letters*, 29(19), 1701–1702. <https://doi.org/10.1049/el:19931131>
7. Wicht, B., Fischer, A., & Hennebert, J. (2018). DLL: A fast deep neural network library. In *Artificial Neural Networks in Pattern Recognition* (pp. 54–65). Springer International Publishing. https://doi.org/10.1007/978-3-319-99978-4_4

Вибір організаційних форм метрологічного забезпечення цифрових ІТ-проектів

Selection of Organizational Forms for Metrological Support of Digital it Projects

Віталій Яровий ^A

Corresponding author: доктор філософії, начальник кафедри, e-mail: vitalii.yaroviy@viti.edu.ua, ORCID: 0000-0002-8239-1150

Оксана Андриєнко ^A

начальник навчально-лабораторного комплексу кафедри, e-mail: oksana.andriienko@viti.edu.ua, ORCID: 0009-0002-5488-1432

Віктор Гудима ^B

к. тех. н., доцент кафедри, e-mail: viktor.gud77@gmail.com, ORCID: 0000-0003-4722-0601

Vitalii Yarovyi ^A

Corresponding author: PhD, Head of the Department, e-mail: vitalii.yaroviy@viti.edu.ua, ORCID: 0000-0002-8239-1150

Oksana Andriienko ^A

Head of the Educational and Laboratory Complex of the Department, e-mail: oksana.andriienko@viti.edu.ua, ORCID: 0009-0002-5488-1432

Viktor Hudyma ^B

Candidate of Technical Sciences, Associate Professor of the Department, e-mail: viktor.gud77@gmail.com, ORCID: 0000-0003-4722-0601

^A Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

^B Національний університет оборони України, м. Київ, Україна

^A Heroes of Kruty Military Institute of Telecommunications and Informatization, Kyiv, Ukraine

^B National Defence University of Ukraine, Kyiv, Ukraine

Received: July 12, 2025 | Revised: August 13, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.13>

Мета роботи. Визначення варіанту організаційної форми метрологічного забезпечення цифрових ІТ-проектів при створенні єдиної інформаційно-аналітичної системи цифрових проектів.

Метод дослідження. методи системного аналізу, порівняльного аналізу, концептуального моделювання, узагальнення, а також експертно-аналітичний підхід.

Результати дослідження. Досліджено організаційні форми метрологічного забезпечення цифрових ІТ-проектів, що покликані створити єдину інформаційно-аналітичну платформу для безперервного моніторингу якості програмного забезпечення.

Теоретична цінність дослідження. Теоретичні положення, висновки та рекомендації, викладені в роботі, можуть стати основою для подальших наукових досліджень й дискусій з питань удосконалення метрологічного забезпечення цифрових ІТ-проектів.

Практична цінність дослідження. Реалізація рекомендацій і пропозицій, обґрунтованих у роботі, які спрямовані на розвиток інтегрованих підходів до метрологічного забезпечення цифрових проектів. Це дозволить внести вклад у розширення наявних знань та практик в сфері метрологічного забезпечення цифрових ІТ-проектів, інтегруючи метрологію з загальною концепцією стратегічного управління цифровими проектами.

Оригінальність дослідження. В даному дослідженні проведено аналіз специфічних чинників, що впливають на функціонування всієї вертикалі органів управління та виконання заходів метрологічного забезпечення, що не були предметом комплексного наукового дослідження.

Тип статті. Теоретичний з практичними рекомендаціями.

Purpose. Determination of the organizational form option for metrological support of digital IT projects during the development of a unified information and analytical system for digital projects.

Method. Methods of systems analysis, comparative analysis, conceptual modeling, generalization, and an expert-analytical approach.

Findings. The organizational forms of metrological support for digital IT projects have been examined, aimed at creating a unified information and analytical platform for continuous monitoring of software quality.

Theoretical implications. The theoretical principles, conclusions, and recommendations presented in the paper may serve as a foundation for further scientific research and discussions on improving metrological support for digital IT projects.

Practical implications. The implementation of the recommendations and proposals substantiated in the paper is aimed at developing integrated approaches to metrological support of digital projects. This will contribute to expanding existing knowledge and practices in the field of metrological support for digital IT projects by integrating metrology into the overall concept of strategic management of digital projects.

Originality of the study. This research analyzes specific factors influencing the functioning of the entire vertical structure of management bodies and the implementation of metrological support measures, which have not previously been the subject of comprehensive scientific investigation.

Paper type. Theoretical with practical recommendations.

Ключові слова: метрологічне забезпечення, цифрові ІТ-проекти, метрики програмного забезпечення, Metering as a Service, організаційні форми.

Key words: метрологічне забезпечення, цифрові ІТ-проекти, метрики програмного забезпечення, Metering as a Service, організаційні форми.

Вступ

В статті в якості основного об'єкта дослідження розглядаються цифрові проекти – проекти, метою яких є створення програмних засобів як основи сучасних ІТ-продуктів. Основний ракурс дослідження – проєкції, що описують різні аспекти екосистеми, в межах якої реалізуються ключові процеси створення і розвитку програмних засобів. Ці проєкції складають основу інформаційно-аналітичного середовища, яке формує і забезпечує оптимальні умови для реалізації ключового процесу – процесу розробки якісного програмного забезпечення (ПЗ) і його подальший розвиток при імплементації в сферу практичного використання.

Предметом дослідження в статті виступає один із ключових видів базового забезпечення цифрових – метрологічне забезпечення (МЗ) цифрових проєктів (ЦП). Роль процесів МЗ в структурі інформаційно-аналітичного забезпечення ЦП постійно зростає, особливо з переходом на принципи і засоби сучасних data driven технологій. Як відомо, на таких ЦП ключові рішення щодо властивостей ПЗ здійснюються на основі даних аналітики, яка безперервно проводиться в процесі розробки і розвитку ПЗ. У свою чергу, якість таких даних, їх повнота, достовірність і релевантність суттєво залежить від правильного вибору і застосування ключових метрик і вимірювань як нормативних властивостей ПЗ, так і факторів впливу зовнішнього і внутрішнього середовищ програмних проєктів. Тому правильно побудована система метрологічного забезпечення ЦП є невід’ємною складовою і важливою задачею управління ЦП.

Теоретичні основи дослідження

Аналізуючи сучасні джерела, стандарти та наукові публікації щодо програмних проєктів та їх метрологічного забезпечення [6-12], можна констатувати наступне. Концепція дослідження, яка орієнтована на створення та оптимізацію інфраструктурних середовищ цифрових проєктів знаходиться на перетині споріднених предметних областей. Проте в інформаційних джерелах та стандартах частіше метрологічне забезпечення розглядається через призму вимірювань характеристик програмних засобів, а не як задача комплексного метрологічного забезпечення внутрішнього середовища проєктів [1-5].

Найближчими аналогами, що відповідають частині змісту досліджень, є стандарти, які прямо визначають метрологію ПЗ як предметну область із чіткими методологічними, технологічними та організаційними аспектами:

ISO/IEC 25023:2016 визначає систематичний підхід до вимірювання якості програмних продуктів;

ISO/IEC 15939:2017 описує процес вимірювання для інженерії програмних систем;

ДСТУ 7363:2013 визначає технічні вимоги до програмного забезпечення засобів вимірювальної техніки.

Проте, ці документи не фокусуються на формуванні саме стратегічних внутрішніх середовищ проєкту, а скоріше розглядають метрологію ПЗ через безпосередні вимірювальні процеси та метрики.

Сучасні дослідження і стандарти чітко фіксують метрологію ПЗ як окрему науково-прикладну дисципліну, що успадковує ключові риси загальної метрології, але з унікальними особливостями, пов’язаними з природою програмного забезпечення:

абстрактність об’єктів вимірювання: нематеріальні характеристики програмних продуктів;

відсутність єдиної фізичної шкали: метрики програмного забезпечення залежать від конкретних умов та середовища;

автоматизація: вимірювання переважно здійснюються автоматизовано за допомогою програмних засобів;

контекстна залежність: всі вимірювання та оцінки суттєво залежать від конкретних умов проєкту.

динамічність: об’єкти вимірювання еволюціонують у процесі життєвого циклу програмного проєкту.

Постановка проблеми

В дослідженнях проведених автором постановка задачі є більш широкою і стратегічною, ніж традиційні практики метрології ПЗ. В них включені задачі створення і використання внутрішніх інфраструктурних середовищ, які не лише забезпечують вимірювання характеристик ПЗ, але й безпосередньо сприяють досягненню стратегічних цілей проєкту. Такий підхід може

розглядатися як розширення традиційної предметної області метрології ПЗ, яка обмежена більш локальними задачами вимірювання, аналізу і оцінювання якості ПЗ.

На думку автора таке, дослідження містить елементи наукової новизни, оскільки воно не лише розширює традиційну область метрологічного забезпечення ПЗ, але й інтегрує метрологію у загальний контекст стратегічного управління ЦП. Саме концепція створення видів забезпечень як інфраструктурних внутрішніх середовищ проекту є новим порівняно з наявними стандартами і типовими публікаціями, які зосереджуються більше на метрологічних аспектах, а не на стратегічному інтегрованому середовищі проекту.

Таким чином, можна констатувати, що запропонований підхід до постановки задачі є достатньо оригінальним та має практичну цінність для розвитку інтегрованих підходів до метрологічного забезпечення цифрових проєктів. Це дозволить внести вклад у розширення наявних знань та практик в цій сфері, інтегруючи метрологію з загальною концепцією стратегічного управління ЦП.

Метою статті є визначення варіанту організаційної форми метрологічного забезпечення цифрових ІТ-проєктів при створенні єдиної інформаційно-аналітичної системи цифрових проєктів.

Результати

Метрологічне забезпечення цифрових проєктів, як відносно нова гілка знань предметної області “Метрологія” є певною спеціалізацією цієї предметної області через застосування основних її концептів і принципів до одного із сегментів предметної області “Інженерія програмного забезпечення”. Цей сегмент об’єднує сферу знань і їх практичне застосування до ключових об’єктів програмної інженерії – цифрових проєктів. Останні, в свою чергу є звуженням поняття проєкту створення програмного забезпечення до рівня розгляду проєктів, головною метою яких є створення програмного забезпечення як основи цифрових ІТ-продуктів. Саме тому в статті з метою релевантного і системного застосування понять і концепцій предметної області “Метрологічне забезпечення цифрових проєктів” використаний відомий принцип успадкування об’єктно-орієнтованого проєктування (ООП). Нижче наведені базові положення, які розкривають сутність базових понять і принципів метрологічного забезпечення цифрових проєктів через застосування принципу успадкування ООП.

Розглядаючи предметну область “Метрологія” як батьківський клас “Метрологія” визначимо ті концепти і розділи (базові концепти) предметної області, які є спільними для всіх його похідних класів (включно з “Метрологічним забезпеченням ЦП”):

Теоретичні основи та методологія вимірювань – поняття величини, міри, еталона, похибки та класифікація методів і підходів до оцінки величин.

Моделювання та оцінка точності – концепти абсолютної й відносної похибки, калібрування, верифікації, процедур повірки й валідації.

Засоби вимірювань – класифікація приладів і систем (фізичні стенди, автоматизовані системи збору даних тощо) та принципи їх побудови й застосування.

Стандартизація та регламентація – ієрархія нормативних документів (ISO, ГОСТ, ДСТУ), правила сертифікації й підтвердження відповідності

Системи управління якістю – процеси контролю, метрологічного нагляду, управління ризиками та впровадження моделей якості (Six Sigma, TQM, SPICE тощо).

Прикладна спрямованість – аналітичні та оптимізаційні застосування результатів вимірювань, прогнозування й оцінка ризиків у різних галузях

Ці шість атрибутів-концептів формують ядро предметної області “Метрологія” й забезпечують успадкування всіх ключових розділів у похідних класах, зокрема в “Метрологічне забезпечення цифрових проєктів”. Адаптацію зазначеного ядра батьківського класу до

специфіки основного об'єкту предметної області “Програмне забезпечення” приводить до наступних дефініції цих понять.

1. Теоретичні основи та методологія вимірювань.

Для ПЗ це сукупність понять “об'єкт вимірювання” (характеристики коду та системи: продуктивність, надійність, складність тощо) і “системи одиниць” (метрики: LOC, функціональні точки, цикломатичність) разом із методами їх отримання та інтерпретації.

2. Моделювання та оцінка точності.

Процеси калібрування (підгонка інструментів аналізу коду під еталони), верифікації (перевірка відповідності зразкам) і аналізу похибок (різниця між очікуваними й фактичними значеннями метрик) для забезпечення достовірності вимірювань властивостей ПЗ.

3. Засоби вимірювань.

Програмні інструменти та платформи для автоматизованого збору, обробки й візуалізації метрик ПЗ: аналізатори статичного коду (SonarQube, CodeClimate), профайлери, навантажувальні тестери тощо.

4. Стандартизація та регламентація.

Комплекс міжнародних і національних норм щодо якості ПЗ: ISO/IEC 25010, ISO/IEC 9126, ДСТУ 7363, СММІ, а також процедури сертифікації, оцінки відповідності та формування технічної документації.

5. Системи управління якістю.

Підходи до контролю й вдосконалення процесів розробки та вимірювань ПЗ із використанням моделей Six Sigma, TQM, ISO/IEC 15504 (SPICE) тощо; визначення метрик-гейтів, аудити якості й безперервне поліпшення процесів.

6. Прикладна спрямованість.

Застосування результатів метрологічного аналізу ПЗ для оптимізації процесів розробки (скорочення витрат часу, прогнозування ризиків дефектів, планування ресурсів), аналітики продуктивності та ухвалення рішень у проектах “Метрологія ПЗ”.

Якщо методами предметної області “Метрологія” вважати базові принципи і підходи, яких необхідно дотримуватися при організації метрологічного забезпечення в інженерії, то такі “методи-принципи” можуть бути сформульовані для батьківського класу наступним чином.

Вимірювання – процес отримання значення фізичної величини (об'єкта вимірювань) за допомогою метрологічних засобів і методів. Забезпечує збір вхідних даних для подальшого аналізу точності й відповідності стандартам.

Калібрування – встановлення відповідності показників вимірювального приладу (або засобу) відомим значенням еталонної величини. Гарантує коректність подальших вимірювань шляхом налаштування інструментів під еталони.

Повірка – офіційна процедура перевірки, чи відповідають метрологічні засоби (прилади, методи) встановленим нормативним вимогам і технічним специфікаціям. Застосовується для підтвердження придатності засобів вимірювання до експлуатації.

Аналіз похибок – виявлення, кількісна оцінка та класифікація похибок вимірювань. Мета – мінімізувати вплив систематичних та випадкових відхилень, підвищити достовірність отриманих результатів.

Ці чотири базові методи-принципи можуть бути перевизначені для дочірнього класу “Метрологічне забезпечення цифрових проєктів” наступним чином.

Вимірювання – збір і фіксація значень метрик ПЗ: показників продуктивності (час відгуку, пропускна здатність), надійності (кількість дефектів, середній час безвідмовної роботи), складності (цикломатична складність, кількість рядків коду), ефективності тестового покриття тощо. Використовує автоматизовані інструменти (профайлер, навантажувальні тести, статичний аналіз) для отримання достовірних даних про поточний стан системи.

Калібрування – налаштування та узгодження інструментів збору метрик із відомими еталонними проектами або зразками коду. Передбачає порівняння результатів тестового заміру на контрольному проекті зі “зразковими” значеннями, корекцію порогів спрацьовувань аналізаторів, валідацію конфігурацій профайлерів та засобів статичного аналізу.

Повірка – формальна перевірка придатності та коректності програмних засобів вимірювань. Включає проведення верифікації аналітичних скриптів, аудит точності плагінів до CI/CD-пайплайнів, порівняння отриманих метрик із зовнішніми джерелами (наприклад, незалежними дослідженнями) та оформлення звіту про відповідність встановленим стандартам якості ПЗ.

Аналіз похибок – виявлення та кількісна оцінка відхилень метрик ПЗ від очікуваних або еталонних значень. Розрізняє систематичні похибки (зумовлені конфігурацією інструментів або особливостями середовища виконання) і випадкові (зумовлені нерепрезентативністю тестових сценаріїв). Мета — скорегувати процеси збору даних, виключити упередження у звітах і підвищити довіру до результатів метрологічного забезпечення ПЗ.

Кожен із цих методів у “Метрологічному забезпеченні ЦП” може бути реалізований як набір скриптів, плагінів та процедур в рамках пайплайнів DevOps/MLOps, що гарантує автоматизований і відтворюваний процес метрологічного контролю цифрових проєктів.

Успадковані від батьківського класу концепти, принципи метрології в дочірньому класі доповнюються концептами і принципами, які визначають спеціалізацію цього класу, орієнтованого на метрологічне забезпечення цифрових проєктів. Наступна група понять і принципів (методів) розкривають сутність такої спеціалізації.

Розглядаючи метрологію ПЗ, як основу для створення підсистеми метрологічного забезпечення цифрових (data driven) проєктів, можна дати наступне визначення такої підсистеми.

Підсистема метрологічного забезпечення цифрових (data-driven) проєктів – одна із ключових підсистем інформаційно-аналітичної підтримки цифрових проєктів, яка створюється для забезпечення достовірності, точності і відтворюваності усіх ключових метрик і аналітичних показників у цифрових проєктах, що базуються на даних, шляхом інтеграції засад метрології ПЗ як невід’ємної складової конвеєра розробки, тестування та експлуатації ПЗ.

Задекларована у визначенні мета підсистеми метрологічного забезпечення ПЗ реалізується через досягнення наступних її цілей.

1. Визначення та стандартизація метрик.

Вибір і формалізація набору базових показників (продуктивність, якість даних, надійність алгоритмів, точність моделей тощо) з прив’язкою до галузевих та внутрішніх стандартів.

2. Інтеграція засобів збору метрик у DataOps/DevOps-пайплайн.

Розгортання автоматизованих скриптів та плагінів для безперервного моніторингу й збору даних у кожному етапі конвеєра: від попередньої обробки даних і тренування моделей до їх розгортання й експлуатації.

3. Калібрування та валідація інструментів.

Налаштування інструментів збору й аналізу метрик на контрольних (еталонних) наборах даних і моделях, регулярна перевірка їх відповідності заданим порогам точності та пропускну здатності.

4. Повірка та аудит якості вимірювань.

Проведення формальної перевірки коректності скриптів і сервісів збору метрик, документування результатів перевірок, виконання періодичних аудитів конфігурацій інструментів.

5. Аналіз похибок і адаптація процесів.

Ідентифікація джерел систематичних і випадкових похибок у метриках (наприклад, не репрезентативність вхідних даних, недоліки конфігурації середовища), коригування процесів збору й обробки з метою мінімізації спотворення результатів.

6. Забезпечення відтворюваності та трасованості.

Фіксація версій вихідних даних, моделей, налаштувань інструментів та скриптів; створення детальних логів кожного вимірювання для подальшого відтворення й аналізу.

7. Підтримка ухвалення рішень і управління ризиками.

Формування регулярних звітів з агрегованими метриками для стейкхолдерів, розроблення дашбордів, які демонструють тренди, показники SLA/SLI, ризики відхилень і рекомендовані коригувальні дії.

8. Постійне вдосконалення.

Налагодження зворотного зв'язку між результатами метрологічного аналізу й процесами розробки, впровадження покращення в інструменти, методики та нормативні документи підсистеми на основі накопиченого досвіду й нових технологічних трендів.

Важлива роль у досягненні поставлених цілей відводиться правильному вибору організаційних форм метрологічного забезпечення цифрових проєктів. Виходячи із існуючих практик програмної інженерії можливі наступні організаційні форми метрологічного забезпечення цифрових проєктів.

1. Централізований метрологічний центр

Структура:

окрема функціональна “служба метрології” на рівні всієї організації.

єдиний набір інструментів, процесів, стандартів.

усі команди звертаються в центр за підтримкою, аудитом та звітністю.

Ключові ролі:

керівник метрології: відповідає за політику, нормативи та стандарти.

аналітик-метролог: налаштовує й контролює інструменти збору метрик для всіх проєктів.

аудитор якості: проводить періодичні перевірки.

Переваги:

повна уніфікація підходів і найвищий рівень контролю.

централізована експертиза та накопичення знань.

Виклики:

низька гнучкість, “вузьке горло” – усі запити проходять через центр.

може відставати від швидких потреб окремих команд.

2. Федеративна модель (“hub-and-spoke”)

Структура:

є центральний метрологічний “хаб” (як у варіанті 1) + “спок” – метрологи в кожній продуктивній або DevOps-команді.

хаб задає стандарти, споки – локалізують їх під конкретні проєкти.

Ключові ролі:

головний метролог (хаб): управляє методологією.

метролог-представник (спок): впроваджує процеси й інструменти в команді.

Переваги:

баланс між уніфікацією та адаптацією під потреби команди.

швидший зворотний зв'язок і підтримка на місцях.

Виклики:

потребує добре налагодженої комунікації та синхронізації між хабом і споками.

ризик “розбіжності” в тлумаченні стандартів.

3. Вбудована модель у DevOps/DataOps-команді

Структура:

кожна крос-функціональна команда сама відповідає за весь цикл метрології (від збору до аналізу).

метрологія інтегрована безпосередньо у CI/CD та DataOps-конвеєр.

Ключові ролі:

DevOps-інженер: налаштовує збір метрик у пайплайні.

Data-інженер: стежить за якістю метаданих і джерелом істини.

QA-інженер/автоматизатор: додає вимірювання в тести.

Переваги:

Максимальна швидкість та гнучкість.

“Метрика” йде разом із кодом і конфігурацією, гарантуючи відтворюваність.

Виклики:

потрібен високий рівень компетенцій у кожному інженері.

ризик непослідовності метрик між різними командами.

4. Платформна/сервісна модель (Metering as a Service)

Структура:

усі інструменти та API метрології винесені у внутрішню платформу-сервіс.

команди підключаються через чітко задокументовані REST-/gRPC-інтерфейси.

Ключові ролі:

платформ-інженери: розробляють і підтримують сам сервіс.

споживачі-розробники: інтегрують SDK і API в свої продукти.

Переваги:

висока масштабованість і однаковий інтерфейс для всіх команд.

легко розгортати оновлення без “болісних” змін у клієнтах.

Виклики:

потребує інвестицій у розробку та підтримку платформи.

додаткова складність взаємодії через мережеві виклики й аутентифікацію.

5. Модель “Спільнота практик” (Community of Practice)

Структура:

метрологічні заходи – не частина жодної формальної ієрархії, а засновані на добровільній участі.

регулярні зустрічі, воркшопи й обмін шаблонами/плагінами.

Ключові ролі:

координатор спільноти: організовує зустрічі та фасилітує обмін досвідом.

ентузіасты-метрологи: діляться реалізаціями, кейсами, скриптами.

Переваги:

швидкий обмін ідеями та найкращими практиками.

гнучкість і мінімальні бюрократичні бар’єри.

Виклики:

відсутність формальної відповідальності може призвести до нерівномірної участі.

складніше домогтися єдиних стандартів.

В таблиці 1 показані відповідності цілей-завдань метрологічного забезпечення цифрових проєктів п’яти розглянутим варіантам їх системної організації. У перетині ставиться “+”, якщо відповідна ціль досягається у цьому варіанті найкраще.

Вибір оптимального варіанта організаційних форм:

1. Малі проєкти/стартапи – зазвичай достатньо моделі № 3 або № 5.

2. Середні за розміром організації – компромісна федеративна модель № 2.

3. Великі корпорації з високими вимогами до регулювання – варто розглянути варіанти № 1 або № 4 з централізованою платформою.

Таблиця 1 – Порівняльний аналіз організаційних форм метрологічного забезпечення цифрових проєктів

Цілі-завдання	Централізований метрологічний центр	Федеративна модель	Вбудована в DevOps/DataOps	Платформна (Metering as a Service)	Спільнота практик
Визначення та стандартизація метрик	+			+	
Інтеграція збору метрик у пайплайн			+	+	
Калібрування і валідація інструментів	+	+			
Повірка та аудит якості вимірювань	+	+			
Аналіз похибок і адаптація процесів			+	+	
Забезпечення відтворюваності й трасованості					
Підтримка ухвалення рішень і управління ризиками	+			+	
Постійне вдосконалення		+			+

Пояснення до вибору організаційної структури:

1. Централізований центр ідеально підходить для уніфікації політик, перевірки й аудитів, стандартизації метрик і підтримки управління ризиками.

2. Федеративна модель забезпечує баланс: сильну методологічну підтримку хабом і локальну адаптацію, що корисно для калібрування, валідації, аналізу похибок і безперервного вдосконалення.

3. Вбудована модель максимально інтегрує збір метрик і трасованість у DevOps/DataOps-пайплайн, що сприяє швидкому аналізу похибок та відтворюваності.

4. Платформна модель дає єдиний API для всіх команд і найкраще підходить для стандартизації метрик, їх інтеграції та забезпечення відтворюваності, а також підтримки ухвалення рішень.

5. Спільнота практик стимулює постійне вдосконалення через обмін досвідом і накопичення кращих практик.

Висновки

При створенні єдиної інформаційно-аналітичної системи цифрових проєктів в якості організаційної форми метрологічного забезпечення більш за все підходить варіант 4 – Платформна/сервісна модель (Metering as a Service). Таке рішення пояснюється наступними причинами.

Уніфіковані API – всі команди та сервіси підключаються через єдиний, стандартизований інтерфейс (REST/gRPC), що спрощує інтеграцію з аналітичним шаром, BI-дашбордами та іншими компонентами єдиного інформаційного ландшафту.

Централізоване зберігання та обробка – метрики й логи потрапляють у спільне сховище – це гарантує консистентність даних, полегшує їх агрегацію, крос-проектний аналіз і побудову єдиної візуалізації.

Масштабованість та гнучкість – платформа може розростатися незалежно від окремих команд і підлаштовуватися під зростання навантаження, при цьому клієнти продовжують користуватися незмінними API.

Розмежування відповідальностей – platform team відповідає за ядро метрології та аналітики, а продукт-команди фокусуються на своїй доменній логіці, просто споживаючи дані “з-під капота”.

Підтримка DevOps/DataOps-конвеєра – платформа легко вбудовується у CI/CD та DataOps-пайплайни, даючи змогу тригерити метрики, калібрування й валідацію автоматично в процесах розробки й розгортання.

Завдяки цим властивостям платформа-сервіс забезпечує найвищий рівень інтеграції, уніфікації та масштабованості в рамках єдиної інформаційно-аналітичної системи цифрових проєктів.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Закон України «Про метрологію та метрологічну діяльність» / Верховна Рада України // Відомості Верховної Ради України. – 2003. – № 27. – Ст. 190.
2. Державна система забезпечення єдності вимірювань: ДСТУ ISO/IEC 17025:2011 / Держстандарт України. – К., 2011.
3. ISO/IEC 25023:2016 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of system and software product quality. – Geneva: ISO, 2016.
4. ISO/IEC 15939:2017 Systems and software engineering — Measurement process. – Geneva: ISO, 2017.
5. IEEE Std 1061-1998 IEEE Standard for a Software Quality Metrics Methodology. – New York: IEEE, 1998.
6. Кузнецов І. Б., Мацько О. Й., Гудима В. П., Ярошенко О. В. Організація метрологічного забезпечення військ (сил). У 2-х ч. Ч. 1 : навч. посіб. – К.: Нац. ун-т оборони України імені Івана Черняхівського, 2020. – 268 с.
7. Тарасова В. В., Малиновський А. С., Рибак М. Ф. Метрологія, стандартизація і сертифікація : підруч. / за заг. ред. В. В. Тарасової. – К.: Центр навч. літ., 2006. – 264 с.
8. Коренець Ю. М. Стандартизація, сертифікація і метрологія : навч. посіб. – Кривий Ріг: ДонНУЕТ, 2023. – 90 с.
9. Метрологія, стандартизація, сертифікація та управління якістю в системах зв'язку / Л. В. Коломієць, П. П. Воробієнко, М. Т. Козаченко, М. Б. Налісний, В. Л. Серебрін, Л. О. Козаченко, О. В. Грабовський, Л. О. Лебединська. – Одеса: ТОВ «ВМВ», 2009. – 376 с.
10. Гудима В., Червоняк В. Аналіз факторів впливу на систему метрологічного забезпечення військових частин Збройних Сил України на основі досвіду російсько-української війни

// *Social Development and Security*. – 2025. – T. 15, № 1. – C. 76–87.
<https://doi.org/10.33445/sds.2025.15.1.7>

11. Fenton N., Pfleeger S. L. *Software Metrics: A Rigorous and Practical Approach*. – Boca Raton: CRC Press, 1998. – 448 p.
12. Kan S. H. *Metrics and Models in Software Quality Engineering*. – Boston: Addison-Wesley, 2002. – 560 p.

References

1. Verkhovna Rada of Ukraine. (2003). *Law of Ukraine “On metrology and metrological activity”*. *Vidomosti Verkhovnoi Rady Ukrainy*, (27), Article 190.
2. State Standard of Ukraine. (2011). *National system for ensuring the uniformity of measurements: DSTU ISO/IEC 17025:2011*. Kyiv: Derzhstandart Ukrainy.
3. International Organization for Standardization. (2016). *ISO/IEC 25023:2016 Systems and software engineering — Systems and software quality requirements and evaluation (SQuaRE) — Measurement of system and software product quality*. Geneva: ISO.
4. International Organization for Standardization. (2017). *ISO/IEC 15939:2017 Systems and software engineering — Measurement process*. Geneva: ISO.
5. Institute of Electrical and Electronics Engineers. (1998). *IEEE Std 1061-1998 IEEE Standard for a Software Quality Metrics Methodology*. New York: IEEE.
6. Kuznetsov, I. B., Matsko, O. Y., Hudyma, V. P., & Yaroshenko, O. V. (2020). *Organization of metrological support of the troops (forces). Part 1* (Textbook). Kyiv: National Defence University of Ukraine named after Ivan Cherniakhovskyi.
7. Tarasova, V. V., Malynovskyi, A. S., & Rybak, M. F. (2006). *Metrology, standardization and certification* (V. V. Tarasova, Ed.). Kyiv: Center for Educational Literature.
8. Korenets, Y. M. (2023). *Standardization, certification and metrology* (Textbook). Kryvyi Rih: DonNUET.
9. Kolomiiets, L. V., Vorobiyenko, P. P., Kozachenko, M. T., Nalisnyi, M. B., Serebrin, V. L., Kozachenko, L. O., Hrabovskyi, O. V., & Lebedynska, L. O. (2009). *Metrology, standardization, certification and quality management in communication systems*. Odesa: VMV.
10. Hudyma, V., & Chervoniak, V. (2025). Analysis of factors influencing the system of metrological support of military units of the Armed Forces of Ukraine based on the experience of the Russian-Ukrainian war. *Social Development and Security*, 15(1), 76–87.
<https://doi.org/10.33445/sds.2025.15.1.7>
11. Fenton, N., & Pfleeger, S. L. (1998). *Software metrics: A rigorous and practical approach*. Boca Raton: CRC Press.
12. Kan, S. H. (2002). *Metrics and models in software quality engineering*. Boston: Addison-Wesley.

A Framework to Secure Business Assets Against Social Engineering Attacks in State Corporations in Kenya

Структура захисту бізнес-активів від атак соціальної інженерії в державних корпораціях Кенії

John Maiyo ^A

Corresponding author: Postgraduate Student, Department of Information Technology, School of Computing and Informatics, e-mail: lomezjay@gmail.com, ORCID: 0009-0007-9847-4034

Satwinder Singh Rupra ^A

Dr., Senior Lecturer, Department of Information Technology, School of Computing and Informatics, e-mail: dotanga@mmust.ac.ke, ORCID: 0000-0003-3695-196X

Daniel Otanga ^A

Dr., Senior Lecturer and Dean, Department of Information Technology, School of Computing and Informatics, e-mail: ssingh@mmust.ac.ke, ORCID: 0000-0001-7212-1088

Джон Маййоа ^A

Corresponding author: аспірант, кафедра інформаційних технологій, Школа обчислювальної техніки та інформатики, e-mail: lomezjay@gmail.com, ORCID: 0009-0007-9847-4034

Сатвіндер Сінгх Рупраб ^A

Доктор, старший викладач, кафедра інформаційних технологій, Школа обчислювальної техніки та інформатики, e-mail: dotanga@mmust.ac.ke, ORCID: 0000-0003-3695-196X

Даніель Отангак ^A

Доктор, старший викладач і декан, кафедра інформаційних технологій, Школа обчислювальної техніки та інформатики, e-mail: ssingh@mmust.ac.ke, ORCID: 0000-0001-7212-1088

^A Masinde Muliro University of Science and Technology, Kakamega, Kenya

^A Університет науки і технологій Масінде Муліро, Какемеге, Кенія

Received: June 21, 2025 | Revised: August 01, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.14>

Purpose. To develop a framework for securing business assets against social engineering attacks in state corporations in Kenya.

Method: Mixed methods.

Findings. The study found a rise in social engineering (SE) attacks, with phishing being the most common. Employee awareness and training were identified as the most critical factors in managing SE threats, supported by awareness programs, reporting practices, and integration with other training initiatives.

Theoretical Implications. A lack of tailored frameworks and methods for addressing SE attacks in Kenyan state corporations was identified, underscoring the need for an effective cybersecurity framework.

Practical implications. The study provides insights for cybersecurity professionals to better prevent, detect, and respond to SE attacks, while helping state corporations strengthen security, promote cybersecurity culture, and improve policy and governance.

Value. It highlights the importance of employee compliance with security policies and skills in mitigating SE threats to business assets.

Future Research. Further work should focus on advanced detection techniques, such as machine learning, and the impact of emerging technologies like AI chatbots on SE methods.

Paper type. Empirical.

Мета дослідження. Розробити рамкову модель для захисту бізнес-активів від атак соціальної інженерії у державних корпораціях Кенії.

Метод дослідження. Застосовано змішаний підхід.

Результати дослідження. Встановлено зростання атак соціальної інженерії, серед яких найпоширенішим є фішинг. Ключову роль у протидії відіграє рівень обізнаності та навчання персоналу з питань інформаційної безпеки.

Теоретичне значення. Виявлено брак спеціалізованих фреймворків та методик для протидії атакам соціальної інженерії у держкорпораціях Кенії, що підкреслює потребу у створенні ефективної моделі кіберзахисту.

Практичне значення. Результати корисні для фахівців з кібербезпеки та державних корпорацій у посиленні захисту, формуванні культури кібербезпеки та вдосконаленні політики інформаційної безпеки.

Цінність дослідження. Дослідження допомагає краще зрозуміти рівень захищеності організацій та наголошує на важливості дотримання політик і процедур безпеки працівниками.

Подальші дослідження. Доцільно розвивати сучасні методи виявлення атак, зокрема на основі машинного навчання, а також аналізувати вплив нових технологій, таких як чат-боти зі штучним інтелектом.

Тип статт.: Емпірична.

Key words: Social Engineering attacks, cybersecurity, State Corporations, phishing, business assets.

Ключові слова: Атаки соціальної інженерії, кібербезпека, державні корпорації, фішинг, бізнес-активи.

Introduction

State corporations in Kenya increasingly rely on information technology to operate and manage their assets. However, this reliance has made them vulnerable to a range of cyber threats, among which social engineering attacks have emerged as a significant concern. Social engineering is defined by [1] as tactics that exploit human weaknesses and persuade individuals to violate established security processes and protocols. According to [2], the effectiveness of social engineering attacks stems from the fact that they target people, who are the most vulnerable component of any security framework. Unlike technological flaws, which can be identified and corrected, human behavior is unpredictable and easily manipulated. In today's digital age, social engineering poses a substantial

threat to both informational and economic security. This is largely due to the growing complexity of information and technological systems. Additionally, [3] found that social engineers attempt to exploit the weakest element in a security architecture by convincing individuals and organizations to disclose essential, sensitive, and confidential information belonging to the organization. Similarly, the principle of persuasion, as highlighted by [4], suggests that humans are more likely to accept and act upon a message if it is presented in a way that appears authentic. According to [5], the focus of social engineering has shifted from targeting individual users to exploiting the entire social network within an organization. Moreover, [6] observed that phishing and other social engineering tactics have evolved significantly. This evolution has been fueled by the development of collaborative systems and practices such as BYOD (bring your own device), which provide avenues for threats like phishing, email fraud, and other malicious communication tools, thereby increasing the risks of network intrusions, especially through counterfeit websites or phishing emails. Recent cybersecurity incidents have revealed such vulnerabilities, for example, the attack on the eCitizen platform in 2023 by the Anonymous Sudan group, which caused major disruptions to critical government services. In this attack, private-sector entities were also affected, including mobile payment providers and ticketing services operated by SGR, as discussed by [7] and [8]. The aim of this research was to develop a framework to secure business assets against social engineering attacks. This framework is intended to provide valuable insights for policymakers in state corporations and researchers seeking to advance knowledge in the field of social engineering. To achieve this, state corporations from four different cities were surveyed through questionnaires and strategic interviews that focused on various aspects of social engineering and cybersecurity threats. The quantitative data were analyzed using descriptive statistics, which were applied to organize and present the findings in the form of tables, graphs, percentages, and frequencies. Thematic analysis was employed to interpret the qualitative data. Data analysis was conducted using the latest version of the Statistical Package for the Social Sciences (SPSS, version 30.0).

Data and methods

This study reviewed frameworks within the cybersecurity domain, with a particular emphasis on social engineering (SE) threats, drawing insights from extensive literature on securing business assets against such attacks in state corporations in Kenya. The literature search encompassed peer-reviewed journal articles, case studies in government agencies, conference proceedings related to social engineering and cybersecurity attacks, and documented best practices in cybersecurity. The review was limited to articles published within the last 10 to 15 years to capture recent findings and advancements. The databases consulted included ACM Digital Library, JSTOR, Google Scholar, Scopus, IEEE Xplore, Web of Science, the Directory of Open Access Journals (DOAJ), and ScienceDirect. Additionally, databases specializing in social engineering and cybersecurity attacks were used for specific case studies.

1. Research Design

According to [9], research design is a structured approach employed to gather reliable responses to questions concerning a research topic. It provides a detailed guide on how to define parameters, collect data, conduct measurements, and analyze the information obtained. The study adopted a mixed-methods design, combining both quantitative and qualitative approaches. Research tools, including questionnaires, interviews, and observations, were also used to provide a comprehensive understanding of the study. The quantitative design enabled the researchers to measure the population required for statistical investigation, offering valuable indicators regarding which variables were most suitable for quantitative testing. [10] emphasized that qualitative research helps evaluate data systematically by using common expressions to draw appropriate conclusions and recommendations in a social context, reflecting the perspectives of the individuals studied.

2. Location of the Study

The primary focus of this study was the cities of Nairobi, Kisumu, Mombasa, and Nakuru. These four cities were selected because they are major centers of state corporations that rely heavily on IT for day-to-day operations. Additionally, their excellent internet connectivity promotes higher adoption rates of IT technologies compared to other towns in Kenya, making them ideal locations for examining the protection of business assets against social engineering attacks. Respondents in these state corporations were chosen using purposive sampling to ensure that the study focused on the most relevant participants.

3. Population of the Study

[11] defines a target population as the entire set of individuals or entities toward which research aims to generalize its findings. [12] supports this view by describing population as a collective of entities, objects, or individuals that share specific homogeneous characteristics. This homogeneity allows results obtained from sampled subsets to accurately reflect the features of the entire group. The study selected 30 state corporations, involving CEOs, Directors, Deputy Directors, CFOs, System Administrators, Network Administrators, Database Administrators, Computer Technologists, system end users, and employees from HR and Procurement departments, yielding a target population of 153 respondents. Purposive sampling was employed to determine the sample sizes for each city, as summarized in Table 1 below.

Table 1 – Sampling setting

City	No. of respondents
Nairobi	105
Mombasa	26
Kisumu	13
Nakuru	9
Total	153

Source: <Author (2025)>

4. The Sample Size and Sampling Procedure

Purposive and stratified random sampling methods were employed to select participants from four cities in Kenya. According to [13], purposive sampling is an appropriate approach when certain groups of people have unique characteristics and can provide more insightful information compared to other groups within the same population. In this study, purposive sampling was used because individuals with essential knowledge were intentionally selected to provide information that could not be obtained from other sources. Stratified random sampling was also employed, as it ensures that every employee has an equal chance of being selected within their respective strata and allows participants to be chosen in proportion to their representation in the general population, as emphasized by [14].

Purposive sampling was applied to select 153 individuals with IT expertise and key system users—specifically those handling sensitive, confidential, and critical data requiring secure privacy measures and the use of IT resources for daily operations. The decision to use purposive sampling is supported by [15], who argues that individuals are intentionally chosen for the valuable information they can provide, which cannot be obtained elsewhere. In total, 153 individuals were purposively selected from 30 state corporations to participate in the study. Consequently, the overall sample size for this study was 153 respondents, as shown in the distribution detailed in Table 2 below.

Table 2 –Members of State Corporation Engaging in the Survey

Section/Users	No. of participants
CEO/Directors/Deputy Directors	10
CFOs	10
System admins/ Network Admins/ IT Technicians/ Database Admins/ Computer Technologists	40
Human Resource Department	20
Procurement Department	25
Other End Users/ Other System Users	48
Total	153

Source: <Author (2025)>

5. Reliability and Validity Analysis

According to [16], the validity of a tool is defined as its ability to accurately measure what it is intended to measure. Similarly, [14] noted that validity refers to how effectively the chosen instrument assesses the variables under study. Additionally, [17] defines reliability as the stability of outcomes across time or among different respondents. In this study, reliability refers to the internal consistency of the instrument, which evaluates the consistency of responses related to an underlying variable. Incorporating feedback from experts and participants ensured that both validity and reliability were thoroughly addressed, thereby strengthening the study's credibility. In this research, validity was assessed through content validity, which determines how effectively the survey instruments captured the variables outlined in the study. Furthermore, credibility was examined by conducting suitability tests on the research data, including the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity. Internal validity was evaluated for each subscale, as presented in Table 3 below.

Table 3 –Test of internal validity

KMO Index		Bartlett's Test	
	Approx. Chi-Square	df	Sig.
0.869	5290.936	150	0.000

Source: <Research Data (2025), SPSS Analysis>

Table 3 shows that all subscales of the questionnaire yielded a significant value of less than 0.0001 ($p \leq 0.001$) on Bartlett's test of sphericity. Moreover, the KMO index was 0.869, which is above the minimum threshold of 0.8 for internal validity. According to [18], a significant KMO index combined with a Bartlett's test value exceeding 0.6 indicates that the conditions for sufficient internal validity are met.

The data obtained were used to calculate the Cronbach's alpha coefficient (α) as a measure of the internal consistency of the respondents' data, derived from how closely related the data sets are. A high level of reliability is indicated by the Cronbach's alpha value of 0.93, leading to the conclusion that the instrument demonstrated "good" reliability. Additionally, [19] confirms that the instrument was considered reliable, since the reliability coefficient of the variables was 0.93, as shown in Table 4 below.

Table 4 –Test of reliability

Cronbach's Alpha Coefficient (α)	Cronbach's Alpha coefficient (α) standardized Items	N of Items
.928	.935	17

Source: <Research Data (2025), SPSS Analysis>

Results and Discussion

1. The types of SE attacks

The study evaluated the different forms of SE threats affecting state corporations in Kenya. Participants were asked to indicate the extent to which they had been affected by various types of SE attacks. They were instructed to specify their responses using the following categories: no level, little level, moderate level, great level, and very great level. The prevalence of SE attacks was assessed using a five-point Likert scale ranging from 1: No Level (NL), 2: Little Level (LL), 3: Moderate Level (ML), 4: Great Level (GL), to 5: Very Great Level (VGL), and the results were analyzed as percentages. The respondents' views are summarized in Table 5 below.

Table 5 –Respondents' views on the types of social engineering attacks

Item	NL	LL	ML	GL	VGL
	Frequency	Frequency	Frequency	Frequency	Frequency
Ransomware Attacks	46	25	34	31	14
Reverse Social Engineering Attacks	48	34	30	24	14
Pretexting Attacks	36	41	29	18	26
Phone/Email Scam Attacks	33	19	37	38	23
Phishing Attacks	16	26	26	42	40

Source: <Research Data (2025)>

Table 5 highlights that phishing attacks (68.5%) have emerged as the most prevalent and highly effective cybersecurity threat. In these schemes, attackers use deceptive e-mails, web pages, websites, or text messages designed to mislead individuals into revealing confidential information such as login credentials, credit card details, or other private data. Frequently, attackers impersonate legitimate entities through sophisticated social engineering techniques. Because phishing is one of the most common ways attackers gain initial access, it represents a significant threat, paving the way for additional malicious activities such as phone or email scams (59.9%), which pose serious risks to both individuals and government agencies.

The findings also indicated that 49.6% of respondents had not been affected by reverse social engineering attacks. Table 5 further suggests that 31.5% of state corporations in Kenya lack adequate protection for access to and use of their information systems. Consequently, these corporations do not sufficiently train or raise awareness among employees about the types of social engineering attacks that affect daily operations. As a result, business assets remain vulnerable, and the extent of this vulnerability is substantial enough to warrant attention. The findings of this study are consistent with [20] and [21], who emphasized that major concerns within government agencies are linked to threats such as phishing, which has emerged as the most prevalent type of SE attack in Kenyan state corporations.

2. Current Security Measures

The study aimed to identify the current security measures in use within state corporations. Respondents were asked to rate the extent of implementation as follows: no level, little level, moderate level, great level, or very great level, across different types of security measures applied in their organizations. The status of these security measures was assessed using a five-point Likert scale ranging from 1: No Level (NL), 2: Little Level (LL), 3: Moderate Level (ML), 4: Great Level (GL), to 5: Very Great Level (VGL), and was analyzed in percentages.

Findings from Table 6 reveal that 70.9% of state corporations have implemented corporate endpoint security, while 29.1% have not yet done so. Endpoint security, along with access controls for data and systems, is crucial for ensuring the security of information systems. Moreover, 72.7% of state corporations enforce strong password policies effectively, while 27.3% have not done so adequately. The respondents' views are summarized in Table 6 below.

Table 6 –Respondents' views on the current security measures

Item	NL	LL	ML	GL	VGL
	Frequency	Frequency	Frequency	Frequency	Frequency
What is the level of implementation of corporate endpoint security in the state corporation	4	28	38	42	38
What is the level of implementation of control access to data and systems assets in the state corporation	6	19	29	50	46
To what extent to have strong passwords been enforced in the state corporation	7	25	38	29	51
To what extent is scanning of malware on your PC performed	13	19	39	45	34

Source: <Research Data (2025)>

Table 6 also shows that 69.1% of respondents agreed that malware scanning on PCs is performed effectively, while 30.9% of state corporations reported that it is not performed efficiently. The results further indicate that 74.8% of state corporations in Kenya do not effectively control access to data and system assets, while only 25.2% manage access control effectively. These findings are consistent with [22], who noted that levels of access control in computing environments should be carefully considered by institutions. [22] also emphasizes that access to assets and systems is typically secured through mechanisms such as physical controls, firewalls, access lists, and privileged access, thereby strengthening access control practices. Supporting the study's findings, [23] evaluated information systems and concluded that controlled access to data, systems, assets, and other computing resources is a vital component of information security. Furthermore, the study's results corroborate those of [24], which pointed out that the availability of resources in information systems within Kenyan state corporations is influenced not only by data loss incidents but also by cybersecurity attacks.

3. Level of employee information security awareness and training

The study examined the level of employee information security awareness and training available and in use within state corporations. Awareness and training levels were assessed using a five-point Likert scale ranging from 1: No Level (NL), 2: Little Level (LL), 3: Moderate Level (ML), 4: Great Level (GL), to 5: Very Great Level (VGL), and were analyzed as percentages. Table 7 indicates that participants agreed that all employees, regardless of their position, are informed about cybersecurity and available training programs for online work, and that they undergo regular

training to report security incidents (61.1%). The views of respondents were recorded and are presented in Table 7 below.

Table 7 –Respondents’ views on the level of employee information security awareness and training

Item	NL	LL	ML	GL	VGL
	Frequency	Frequency	Frequency	Frequency	Frequency
To what degree has the state corporation implemented initiatives focused on cybersecurity education and training for staff working online and remotely?	10	37	41	59	3
To what extent has the state corporation established continuous improvement programs	6	48	54	32	10
To what extent has the state corporation implemented effective security training programs	19	33	47	45	6
What is the extent of integration of other training programs with information security programs	15	33	59	33	10

Source: <Research Data (2025)>

Notwithstanding this progress, 41.3% of respondents indicated that the integration of information security with other training programs has not been implemented in state corporations, while 58.7% stated that such integration has been achieved. Moreover, 58.1% of participants reported that employees across different levels are provided with appropriate cybersecurity awareness and training on social engineering attacks. Similarly, 58.9% of respondents confirmed that their state corporation has established continuous improvement programs in cybersecurity.

These results align with the research conducted by [25], which highlights that such attacks exploit employees’ lack of cybersecurity knowledge, leading them at times to unknowingly expose sensitive data or install malicious software. Additionally, [26] recommend that education and training programs should aim to raise awareness among all employees about the different types of SE attacks, the methods or tactics used by attackers, and the consequences of a successful attack within the organization. Moreover, [26] propose the use of effective simulations of social engineering attack scenarios, allowing employees to practice responding in a controlled and safe environment. According to [27], user engagement or gamification can be employed as a means of enhancing awareness among employees. To increase attention and commitment during training, [27] suggests using interactive and engaging training materials, which is supported by the findings of this study.

It is therefore clear that cultivating a cybersecurity culture within state corporations is essential, and that organizational leadership must actively support and promote this culture.

4. Organizational Culture and Policies

The study aimed to identify the different organizational cultures and policies in use within state corporations. The status of organizational culture and policies was evaluated using a five-point Likert scale ranging from 1: No Level (NL), 2: Little Level (LL), 3: Moderate Level (ML), 4: Great Level (GL), to 5: Very Great Level (VGL), and was analyzed based on percentages. The views of the respondents were recorded and are presented in Table 8 below.

Table 8 –Respondents’ views on organizational culture and policies

Item	NL	LL	ML	GL	VGL
	Frequency	Frequency	Frequency	Frequency	Frequency
To what extent has the information security policy be implemented in the state corporation	3	35	35	60	17
What is the level of incident response in relation to the organizational culture	10	40	40	38	22
To what extent has the state corporation adopted risk management framework	10	28	45	54	13
To what extent has the state corporation defined collaboration between departments	3	40	49	40	18

Source: Research Data (2025)

Table 8 shows that 67.1 percent of state corporations in Kenya have implemented an information security (IS) policy. However, 32.9 percent of respondents reported that they either do not have such a policy or have not engaged with it in their organizations. This indicates that nearly one-third of state corporations lack sufficient safeguards for controlling access to and use of their information systems. Such a high proportion of corporations without an IS policy represents a significant issue that must be addressed. This finding contradicts [28], which describes an IS policy as a comprehensive document typically linked to executive leadership that defines goals and constraints for the use of information systems and should therefore be an integral part of every state corporation, accessible to all users of information systems.

The findings of this study diverge from previous research that characterized the IS policy as a management document prohibiting risky computing behaviors and practices, thereby enhancing the security of organizational systems. Additionally, Table 8 reveals that 64.3 percent of respondents stated that a risk management framework has been adopted and implemented in their corporations and effectively guides the actions of individuals using information systems. By contrast, 35.7 percent indicated that the framework has not been implemented and therefore does not adequately guide user behavior. This aligns with [29], who stated that the foundation of a robust information security framework lies in the IS policy. Similarly, [30] emphasized that a risk management framework includes effective risk assessment strategies that help identify weaknesses in information security and guide the implementation of stronger protective measures.

Furthermore, 62.9 percent of respondents reported that they were not aware of incident response practices related to organizational culture, while only 37.1 percent were sensitized to such practices and safe computing behavior. According to [31], IT security can be enhanced by establishing IS policies and incident response mechanisms that include staff training and awareness. It was also observed that 64 percent of respondents agreed that no formal collaboration between departments had been established in their corporations, while 36 percent confirmed that such collaboration had been implemented. Therefore, the insufficient execution of IS policies can be linked to the growing number of system breaches occurring within Kenyan state corporations.

Conclusion

The frequency and severity of SE attacks have been increasing, causing significant emotional distress among employees and severe financial damage to organizations. These attacks have become a serious concern, particularly when carried out without direct technical methods. Nevertheless, technical attacks remain more common than non-technical ones. Therefore, there is an urgent need for innovative methods of threat detection and preventive measures, along with cybersecurity

initiatives aimed at educating employees. State corporations must allocate resources to cybersecurity education and training in order to cultivate skilled and well-prepared staff.

The study found that phishing attacks (68.5%) are the most prevalent type of social engineering attack and represent a highly effective cybercrime tactic in state corporations. This threat paves the way for further malicious activities, such as ransomware attacks (52.3%). Moreover, the categories of SE threats identified in the study include Phone or Email Scams, Reverse Social Engineering, and Pretexting attacks.

The study also revealed that although various critical security measures are in place, employee understanding of information security and training practices (61.1%) plays a more crucial role in the overall management of social engineering in state corporations in Kenya. This includes cybersecurity training and awareness programs, continuous improvement initiatives, cybersecurity awareness campaigns, reporting of suspicious activity, and the integration of information security into other training programs.

In terms of current security measures, the actions implemented include multi-factor authentication (MFA), two-factor authentication (2FA), access controls, strong password policies, IT security standards and frameworks, regular security audits, periodic scanning of users' PCs, phishing simulation exercises, the use of secure communication protocols such as HTTPS, and the deployment of security software such as antivirus and other anti-malware programs. Organizational culture and policies primarily consist of implemented information security policies, clear IT security procedures, incident response mechanisms, the adoption of a risk management framework, and defined collaboration between departments. The study's observations highlight that state corporations remain vulnerable if any of these social engineering techniques are employed during an actual attack.

Finally, employee compliance with established security policies, practices, and procedures, together with adequate user skills, plays a vital role in mitigating social engineering attacks on business assets. The types of social engineering attacks, the current security measures, the level of employee information security awareness and training, as well as organizational culture and policies, are all crucial factors in securing business assets against social engineering attacks in Kenyan state corporations.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

1. ENISA (2021). Social Engineering: Exploiting the weakest links. Enisa.europa.eu. Retrieved from: <http://www.enisa.europa.eu/publications/archive/social-engineering>. Retrieved on: 14/06/2024.
2. Jamshed, & Jahangir (2021). Cultural Implications of China Pakistan Economic Corridor. Vol. 2. no. 4.
3. Carey, B. (2017). Protect or disclose? Confidential information in the Cayman Islands. Trusts and Trustees. ttw229. doi:10.1093.
4. Garcia-Alfaro, J., & Navarro-Arribas, G. (2009). A Survey on Cross-Site Scripting Attacks. Retrieved from: <http://arxiv.org/abs/0905.4850>.

5. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Vol. 22. Journal of Information Security and Applications. <https://doi.org/10.1016/j.jisa.2014.09.005>.
6. Pathak et. al (2014). E-governance, Corruption and Public Service Delivery: A Comparative Study of Fiji and Ethiopia. Joaag, vol. 3. no. 1.
7. Cheruiyot, K. (2023). CS Owalo admits cyberattack on eCitizen portal insists data secure. Daily Nation. Retrieved from: <https://www.nation.africa>.
8. Gooding, M. (2023). Anonymous Sudan DDoS cyberattacks cripple Kenya's new e-Citizen digital infrastructure. Retrieved from <https://techmonitor.ai/technology/cybersecurity/anonymous-sudan-kenya-ddos-cyberattack-ecitizen>.
9. Matthews, B., & Ross, L. (2014). Research methods. Pearson Higher Ed.
10. Berg, B. (2009). Qualitative Research Methods. 7 ed. Boston: Allyn and Bacon.
11. Cooper, C. R., & Schindler, P. S. (2008). Business Research Methods. 10 ed. McGraw-Hill.
12. Kombo, D. K., & Tromp, D. L. (2006). Proposal and thesis writing: An introduction. Nairobi: Paulines Publications Africa. pp10-45.
13. Tongco, M. D. (2007). Purposive sampling as a tool for informant selection. vol. 5. Ethnobotany Research and applications.
14. Mugenda, O. & Mugenda, A. (2019). Research methods: quantitative and qualitative approaches.
15. Padgett, D. K. (2016). Qualitative methods in social work research. Sage Publications vol. 36.
16. Anastasiadou, S. D. (2011). Reliability and Validity Testing of a New Scale for Measuring Attitudes Toward Learning Statistics with Technology. Acta Didactica Napocensia. vol. 4. no. 1. pp 1–10.
17. Fienberg, S. E. (2012). Statistics for Social and Behavioral.
18. Creswell, J. W. & Clark, V. P. (2007). Designing and conducting mixed methods research.
19. Nunnally, J. (1978). Psychometric theory. New York: McGraw-Hill 2nd ed.
20. Miryala, N., & Gupta, D. (2022). Data Security Challenges and Industry Trends. International Journal of Advanced Research in Computer and Communication Engineering. <https://doi.org/10.17148/ijarccce.2022.111160>.
21. Mphatheni, M., & Maluleke, W. (2022). Cybersecurity as a Response to Combating Cybercrime. International Journal of Research in Business and Social Science.
22. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.
23. Mitnick, K., & Simon, W. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley, New York.
24. Mang'ira, R. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.
25. Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity Threats in Fintech: A Systematic Review. Expert Systems with Applications. 241, Article ID: 122697.
26. Aldawood, H., & Skinner, G. (2020). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. 26th International Conference on Systems Engineering. Sydney, 8-20 December, 1-6. <https://doi.org/10.1109/ICSENG.2018.8638166>.
27. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers and Security. vol. 98. Retrieved from: <https://doi.org/10.1016/j.cose.2020.102003>.
28. Kimwele, M. M. (2011). Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs). Int. J. Comput. Sci. Secur. vol. 5.

29. Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*. Vol. 14. no. 2. pp 37-49.
30. Hu, Q. D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*. vol 43. no. 4. pp 615-660.
31. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

Список використаних джерел

1. ENISA (2021). Social Engineering: Exploiting the weakest links. *Enisa.europa.eu*. Retrieved from: <http://www.enisa.europa.eu/publications/archive/social-engineering>. Retrieved on: 14/06/2024.
2. Jamshed, & Jahangir (2021). Cultural Implications of China Pakistan Economic Corridor. Vol. 2. no. 4.
3. Carey, B. (2017). Protect or disclose? Confidential information in the Cayman Islands. *Trusts and Trustees*. ttw229. doi:10.1093.
4. Garcia-Alfaro, J., & Navarro-Arribas, G. (2009). A Survey on Cross-Site Scripting Attacks. Retrieved from: <http://arxiv.org/abs/0905.4850>.
5. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Vol. 22. *Journal of Information Security and Applications*. <https://doi.org/10.1016/j.jisa.2014.09.005>.
6. Pathak et. al (2014). E-governance, Corruption and Public Service Delivery: A Comparative Study of Fiji and Ethiopia. *Joaag*, vol. 3. no. 1.
7. Cheruiyot, K. (2023). CS Owalo admits cyberattack on eCitizen portal insists data secure. *Daily Nation*. Retrieved from: <https://www.nation.africa>.
8. Gooding, M. (2023). Anonymous Sudan DDoS cyberattacks cripple Kenya's new e-Citizen digital infrastructure. Retrieved from <https://techmonitor.ai/technology/cybersecurity/anonymous-sudan-kenya-ddos-cyberattack-ecitizen>.
9. Matthews, B., & Ross, L. (2014). *Research methods*. Pearson Higher Ed.
10. Berg, B. (2009). *Qualitative Research Methods*. 7 ed. Boston: Allyn and Bacon.
11. Cooper, C. R., & Schindler, P. S. (2008). *Business Research Methods*. 10 ed. McGraw-Hill.
12. Kombo, D. K., & Tromp, D. L. (2006). *Proposal and thesis writing: An introduction*. Nairobi: Paulines Publications Africa. pp10-45.
13. Tongco, M. D. (2007). Purposive sampling as a tool for informant selection. vol. 5. *Ethnobotany Research and applications*.
14. Mugenda, O. & Mugenda, A. (2019). *Research methods: quantitative and qualitative approaches*.
15. Padgett, D. K. (2016). *Qualitative methods in social work research*. Sage Publications vol. 36.
16. Anastasiadou, S. D. (2011). Reliability and Validity Testing of a New Scale for Measuring Attitudes Toward Learning Statistics with Technology. *Acta Didactica Napocensia*. vol. 4. no. 1. pp 1–10.
17. Fienberg, S. E. (2012). *Statistics for Social and Behavioral*.
18. Creswell, J. W. & Clark, V. P. (2007). *Designing and conducting mixed methods research*.
19. Nunnally, J. (1978). *Psychometric theory*. New York: McGraw-Hill 2nd ed.
20. Miryala, N., & Gupta, D. (2022). Data Security Challenges and Industry Trends. *International Journal of Advanced Research in Computer and Communication Engineering*. <https://doi.org/10.17148/ijarcce.2022.111160>.

21. Mphatheni, M., & Maluleke, W. (2022). Cybersecurity as a Response to Combating Cybercrime. *International Journal of Research in Business and Social Science*.
22. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.
23. Mitnick, K., & Simon, W. (2011). *The Art of Deception: Controlling the Human Element of Security*. Wiley, New York.
24. Mang'ira, R. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.
25. Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity Threats in Fintech: A Systematic Review. *Expert Systems with Applications*. 241, Article ID: 122697.
26. Aldawood, H., & Skinner, G. (2020). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. 26th International Conference on Systems Engineering. Sydney, 8-20 December, 1-6. <https://doi.org/10.1109/ICSENG.2018.8638166>.
27. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers and Security*. vol. 98. Retrieved from: <https://doi.org/10.1016/j.cose.2020.102003>.
28. Kimwele, M. M. (2011). Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs). *Int. J. Comput. Sci. Secur.* vol. 5.
29. Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*. Vol. 14. no. 2. pp 37-49.
30. Hu, Q. D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*. vol 43. no. 4. pp 615-660.
31. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

Захисна пошарова модель багатокомпонентної архітектурно-компонованої структури оптоелектронного каналу витоку інформації

Protective Layered Model of a Multi-Component Architectural-Composite Structure of an Optoelectronic Information Leakage Channel

Назарій Дзяний

Nazarii Dzyanyy

доктор філософії, доцент кафедри захисту інформації, e-mail: azpiskozub@gmail.com, nazarii.r.dzianyiy@lpnu.ua, ORCID: 0000-0001-9101-3701

Doctor of Philosophy, Associate Professor of the Department Information Protection, e-mail: nazarii.r.dzianyiy@lpnu.ua, ORCID: 0000-0001-9101-3701

Національний університет "Львівська політехніка", м. Львів, Україна

Lviv Polytechnic National University, Lviv, Ukraine

Received: June 21, 2025 | Revised: August 01, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.15>

Мета роботи. Розробка захисної моделі багатокомпонентної архітектурно-компонованої структури оптоелектронного каналу витоку інформації, яка, на відміну від існуючих підходів, враховує складну взаємодію пошарових елементів та дозволяє більш точно оцінити та мінімізувати ризики витоку мовної інформації.

Метод дослідження. Теоретичне узагальнення та практичне моделювання на основі результатів попередніх емпіричних досліджень.

Результати дослідження. Побудовано захисну модель багатокомпонентної архітектурно-компонованої структури оптоелектронного каналу витоку інформації, яка враховує комбінацію пошарових елементів, відгук від проходження лазерного променя в середину приміщень і у зворотному напрямку та розгортається на рівні агрегатної та комплексної моделі. Розроблено математичну модель, що описує мінімізацію втрат інформації через оптоелектронний канал витоку від лазерними системами акустичної розвідки (ЛСАР), дозволяє визначити оптимальну величину зменшення ризику для кожного гіпотетичного шару вихідного матеріалу, що, в свою чергу, відповідає максимальному ступеню захищеності приміщення.

Теоретична цінність дослідження. Дослідження розвиває теоретичні засади захисту інформації, пропонуючи комплексну модель оптоелектронного каналу витоку, яка враховує складні процеси взаємодії лазерного випромінювання з багатопшаровими структурами.

Практична цінність дослідження. Дослідження надає наукову основу для проектування та оптимізації захисних систем, дозволяючи досягти найбільш ефективної протидії лазерним системам акустичної розвідки шляхом цілеспрямованого впливу на фізичні властивості багатопшарових архітектурних компонентів. Результати дослідження можуть бути використані для модернізації існуючих систем захисту інформації, наприклад, шляхом розробки нових типів захисних плівок або покриттів для вікон.

Цінність дослідження. Дослідження демонструє, що розроблена модель та отримані результати можуть бути використані для створення більш ефективних засобів захисту, що сприятиме підвищенню безпеки інформаційних систем і об'єктів та стимулює подальші міждисциплінарні дослідження у цій важливій галузі.

Тип статті. Теоретичне узагальнення та практичне моделювання на основі результатів попередніх емпіричних досліджень.

Purpose. Development of a protective model of a multi-component architectural-composite structure of an optoelectronic information leakage channel, which, unlike existing approaches, takes into account the complex interaction of layered elements and allows for a more accurate assessment and minimization of the risks of speech information leakage.

Method. Theoretical generalization and practical modeling based on the results of previous empirical studies.

Findings. A protective model of a multi-component architecturally-composed structure of an optoelectronic information leakage channel has been constructed, which takes into account the combination of layered elements, the response from the passage of a laser beam into the interior of the premises and in the opposite direction, and is deployed at the level of an aggregate and complex model. A mathematical model has been developed that describes the minimization of information loss through the optoelectronic information leakage channel from the Laser Acoustic Reconnaissance Systems, allowing to determine the optimal amount of risk reduction for each hypothetical layer of the source material, which, in turn, corresponds to the maximum degree of security of the premises.

Theoretical implications. The study develops the theoretical foundations of information protection by proposing a complex model of the optoelectronic leakage channel, which takes into account the complex processes of interaction of laser radiation with multilayer structures.

Practical implications. The research provides a scientific basis for the design and optimization of protective systems, allowing to achieve the most effective counteraction to laser acoustic reconnaissance systems by targeted influence on the physical properties of multilayer architectural components. The results of the research can be used to modernize existing information protection systems, for example, by developing new types of protective films or coatings for windows.

Value. The study demonstrates that the developed model and the obtained results can be used to create more effective protection tools, which will contribute to increasing the security of information systems and objects and stimulate further interdisciplinary research in this important field.

Paper type. Theoretical generalization and practical modeling based on the results of previous empirical research.

Ключові слова: мовна інформація, оптоелектронний канал витоку інформації, лазерні системи акустичної розвідки, захист інформації, пошарова модель.

Key words: language information, optoelectronic information leakage channel, laser acoustic reconnaissance systems, information protection, layered model.

Вступ

Мовна інформація часто містить державні та комерційні таємниці, особисті дані або стратегічні плани. Витік такої інформації може призвести до значних фінансових втрат, репутаційних ризиків, юридичної відповідальності або навіть загрози національній безпеці. Моделювання та мінімізація втрат через оптоелектронний канал витоку є прямою відповіддю на цю загрозу.

Витік конфіденційної інформації залишається однією з найсерйозніших проблем у сфері забезпечення національної безпеки. Лазерно-локаційне зондування віконних шибок та інших відбиваючих поверхонь робить можливим відтворення розмови, що ведеться під час конфіденційних переговорів, виступів тощо. Протягом останніх десятиліть розроблялись численні методи захисту інформації від витоку різними каналами. Одним із ключових напрямків забезпечення інформаційної безпеки є виявлення та локалізація можливих технічних каналів витоку акустичної інформації. В цій галузі було досліджено багато методів, включаючи як активні, так і пасивні методи захисту мовної інформації з використанням спеціальних приладів, магнітостатики та електростатики, оптичних властивостей.

Одним з найактуальніших та найперспективніших напрямків пасивного захисту мовної інформації на даний час є розробка спеціальних покриттів та плівок, застосування яких може суттєво знизити ризик витоку конфіденційної інформації за рахунок: поглинання або розсіювання лазерного випромінювання, що використовується для зондування; зниження амплітуди вібрацій відбивних поверхонь, що ускладнює відтворення звуку та комбінації пошарових елементів, що відповідає максимальному ступеню захищеності приміщення. Захищеність приміщень від зняття мовної інформації лазерними системами акустичної розвідки (ЛСАР) має складну залежність, що формується багатьма взаємопов'язаними величинами. Це завдання вимагає комплексного підходу, який враховує властивості матеріалів (скла, захисних плівок), їх пошарові комбінації, взаємодію лазерного променя з поверхнями. Розробка математичної моделі, яка враховує всі ці фактори, є критично важливою для створення ефективних рішень.

Теоретичні основи дослідження

У закритих приміщеннях акустична інформація може бути перехоплена, оскільки будівельні конструкції (стіни, підлога, стеля, вікна, труби, закриті двері) по суті є акустичними мембранами і добре передають звукові коливання. З будь-якого приміщення через стіни, підлогу або стелю можна перехоплювати акустичний сигнал за допомогою віброперетворювача і підсилювача.

Здалеку акустичний сигнал від закритих вікон можна зняти, спрямувавши лазерне випромінювання на скло або використовуючи спрямований мікрофон. Акустична інформація також може бути знята з побутової техніки, апаратури зв'язку. Вібруючі тіла і механізми, що коливаються, такі як рухомі елементи машин, телефонні апарати, звукопідсилюючі системи, голосові зв'язки людини і т.д. є джерелом утворення акустичного каналу витоку інформації.

При розповсюдженні акустичної хвилі, частинки повітря, якщо на їх шляху немає перешкод, утворюють пружну хвилю, що коливається, розповсюджуючись у всі сторони. В межах приміщень або інших закритих просторів на шляху поширення звукових хвиль виникає багато перешкод, на які акустичні хвилі чинять тиск (двері, вікна, стіни, стеля, підлога і т.п.), заставляючи їх коливатися. Така дія акустичних хвиль являється причиною утворення акустичного каналу витоку інформації.

Акустичні канали витоку інформації утворюються шляхом (рис. 1.) [1]:
поширення акустичних коливань у вільному повітряному просторі;
впливу звукових коливань на елементи та будівельні конструкції;
впливу звукових коливань на технічні засоби обробки інформації.



Рисунок 1 – Утворення акустичних каналів витоку інформації

Залежно від середовища розповсюдження голосових сигналів і способів їх перехоплення, технічні канали витоку інформації можна розділити на: акустичні, вібраційні, електроакустичні, оптоелектронні та параметричні.

Процес обміну інформацією за допомогою акустичного сигналу ґрунтується на його поширенні в навколишньому середовищі. Відповідно, акустичні сигнали можуть поширюватись у будь-якому середовищі, за винятком вакууму. Саме цей факт обумовлює можливість проходження акустичного сигналу через складові будівельних конструкцій, скло та зняття його лазерними системами акустичної розвідки (ЛСАР).

Структура каналу витоку інформації через скло зображена на рисунку 2.

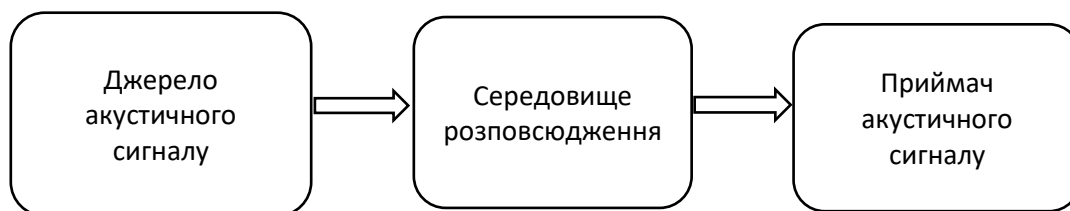


Рисунок 2 – Структура акустичного каналу витоку інформації

Акустичні канали витоку інформації є одними із найнебезпечніших, де серед усіх видів акустичних сигналів-носіїв значну частину становить мовна інформація, яка отримується у режимі реального часу.

Лазерні системи акустичної розвідки є одними із високотехнологічних інструментів, що дозволяють знімати акустичну інформацію дистанційно, використовуючи вібрації поверхонь (наприклад, віконного скла), спричинені звуковими хвилями. Це робить їх надзвичайно небезпечними для будь-яких приміщень, де обговорюється конфіденційна інформація.

Оптоелектронний (лазерний) канал витоку інформації широко використовується в інформаційній розвідці та є досить простим у використанні, оскільки здебільшого зняття інформації відбувається з вібруючого скла. Крім того, використання лазерного мікрофону не потребує його безпосередньої присутності на об'єкті [2].

Оптоелектронний канал витоку інформації формується при опроміненні лазерним променем тонких відбивних поверхонь (скла, вікон, картин, дзеркал тощо), що коливаються в акустичному полі. Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється

по амплітуді та фазі і приймається приймачем оптичного випромінювання, яке демодулюється для вивільнення голосової інформації.

Сутність оптоелектронних каналів витоку інформації полягає в тому, що на об'єкті інформаційної діяльності, де озвучується інформація, під впливом небезпечного акустичного сигналу знаходяться усі предмети. Ті предмети, що мають оптичні властивості віддзеркалення, вібрують. Вібрація таких предметів пов'язана з коливанням їх поверхні. Якщо на поверхню цих предметів спрямувати лазерний промінь, то він віддзеркалиться від поверхні у вигляді променя, модульованого тремтінням від сигналу вібрації і розповсюджуватиметься далі (Рис. 3.) [3].

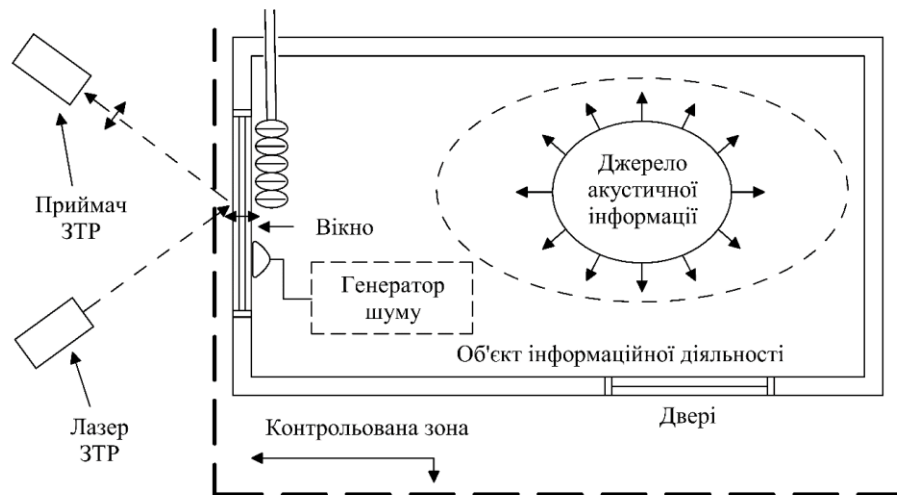


Рисунок 3 – Акустооптоелектронний (лазерний акустичний) канал витоку інформації

Віддзеркалений промінь може бути перехоплений противником, здійснена його демодуляція і відновлений смисл початкового інформаційного мовного сигналу.

Запобігання витоку інформації акустооптоелектронним каналом можна досягти наступними способами:

- використання вакуумних та інших захищених вікон, матування зовнішньої поверхні скла;
- використання щодо вікон та інших предметів віддзеркалення вібраційного зашумлення.

Захист мовної інформації – це комплекс заходів, спрямованих на запобігання несанкціонованому доступу, використанню, поширенню або зміні мовної інформації.

У роботах [4–8] вітчизняні науковці розглядають питання захисту мовної інформації від витоку за допомогою оптоелектронного каналу. Запропоновані методи пасивного захисту з використанням сонцезахисних плівок не дають бажаного ефекту як антилазерні.

Плівки на основі сполук міді, які захищають вікна від випромінювання в ультрафіолетовому та видимому інфрачервоному діапазонах, як описано в [9], працюють найбільш ефективно в діапазоні 500 нм, який не може забезпечити бажаний захист від сканування, оскільки лазери працюють в робочому діапазоні 650 – 3000 нм.

Зарубіжними авторами в роботі [10] проаналізовано варіанти для зменшення вібрації скла та запобігання лазерному прослуховуванню. Враховано вплив конструкції склопакета на захисні властивості від ЛСАР. Результати дослідження показують, що лише 1% коливань скла передається віконними рамами, а решта – віконним склом.

Вплив антилазерних аерозолів на інтенсивність акустичних сигналів розглянуто в роботі [11]. Було встановлено, що оптимальна сила сигналу відповідає кількості абляційного

матеріалу. Це дозволяє відповідним чином регулювати лазерний фокус під час відбору зразків для оптимальної абляції на основі інтенсивності акустичного сигналу.

При дистанційній лазерній зйомці голосу, проаналізовані характеристики зворотного розсіювання об'єктів [12]. Результати показали, що відновлена амплітуда мовного сигналу поступово зменшується зі збільшенням шорсткості поверхні. Крім того, відновлена амплітуда акустичного сигналу збільшується зі збільшенням коефіцієнта ослаблення металу.

На основі надрешіток з фотонних кристалів та наноматеріалів, розроблені багаточастотні багат шарові плівки та покриття з матеріалів [13]. Ці матеріали забезпечують фільтрацію певних довжин хвилі світла, зберігаючи прозорість у іншому спектрі.

Аналізування праць зарубіжних та вітчизняних вчених дає підстави стверджувати, що захист мовних даних від можливого витоку технічними каналами є одним з важливих завдань забезпечення інформаційної безпеки, як у державних, так і бізнес-структурах.

Будь-який канал витоку інформації формується на основі трьох складових: передавач (джерело небезпечного сигналу), середовище розповсюдження небезпечного сигналу, приймач (пристрій знімання інформації). Оптико-електронний канал – не виняток. Небезпечним сигналом в даному випадку є мова співрозмовників, тобто обговорювана вголос закрита інформація. Середовищем поширення небезпечного сигналу, в нашому випадку, можуть бути вікна, картини, дзеркала, та інші предмети побуту, що знаходяться у приміщенні. Ці конструкції мають властивості мембрани і піддаються сильному впливу звукових коливань [14].

Таким чином, для використання оптоелектронного каналу витоку інформації зловмиснику немає необхідності проникати в приміщення, достатньо лише отримати доступ до суміжних будівель та встановити там пристрої знімання інформації, що перетворюють коливання конструкцій контрольованої зони в електричні.

Захист мовної інформації може відбуватися у двох напрямках. По-перше, захистити переговори, які відбуваються в закритих приміщеннях або на контрольованій території. Другий аспект – захистити мовну інформацію в каналах зв'язку.

Постановка проблеми

Існуючі архітектурні та будівельні рішення, що застосовуються при будівництві або модернізації приміщень, не завжди забезпечують належний рівень захисту мовної інформації від ЛСАР. Це зумовлено тим, що принципи функціонування ЛСАР ґрунтуються на дистанційному зчитуванні мікровібрацій поверхонь (наприклад, віконного скла), що виникають під впливом звукових хвиль усередині приміщення. Навіть незначні вібрації можуть бути перетворені назад у мовну інформацію з використанням чутливого оптичного обладнання.

Захист від ЛСАР є надзвичайно складним, багатофакторним заданням, що залежить від значної кількості взаємопов'язаних параметрів. Це включає в себе характеристики матеріалів (особливо скла), їхню товщину, кількість шарів, наявність і властивості спеціальних покриттів, а також динаміку та архітектуру взаємодії лазерного променя з цими елементами.

Відсутність комплексних та науково обґрунтованих моделей, які б враховували комбінацію пошарових елементів та відгук від проходження лазерного променя в обох напрямках (у приміщення та у зворотному напрямку), ускладнює проектування дійсно захищених об'єктів. Це призводить до того, що заходи безпеки часто є недостатніми, неефективними або надмірно витратними без досягнення бажаного рівня захисту.

Необхідність мінімізації втрат інформації через оптоелектронний канал витоку вимагає не просто блокування сигналу, а оптимізації захисних характеристик кожного елемента архітектурної композиції. Це дозволяє досягти максимального ступеня захищеності приміщення з урахуванням усіх аспектів взаємодії.

Таким чином, актуальною науково-технічною проблемою є розробка та впровадження ефективної моделі, яка дозволить кількісно оцінювати, прогнозувати та мінімізувати ризики

витоку мовної інформації через оптоелектронний канал від ЛСАР, забезпечуючи максимальну захищеність приміщень у сучасних умовах загроз інформаційній безпеці.

Методологія

Методологія даного дослідження опирається на комплексну методику вивчення параметрів захищеності оптоелектронного каналу витоку інформації, яка дає змогу дослідити пошарову взаємозалежність та вплив захисних оптичних шарів і внутрішньої будови скла на його захисні характеристики від ЛСАР. Зокрема, на основі оцінювання захищеності скла та плівкових покриттів від лазерних систем розвідки, що здійснювалося за допомогою рентгенофлуоресцентного і спектрального аналізу та симплекс-решітчатого планування при моделюванні характеристик скла, можна узагальнити, що застосовані методи, розроблені на їхній основі методики та експериментальні дослідження становлять таку методологію, що повністю довершує поставлені завдання.

Для побудови захисної пошарової моделі багатокомпонентної архітектурно компонованої структури оптоелектронного каналу витоку інформації використовувалися отримані нами результати попередніх досліджень.

Зокрема, проведені дослідження захисних можливостей скла від лазерного зондування залежно від його елементного складу, зокрема щодо впливу елементного складу листового скла на коефіцієнти відбивання та поглинання зондуючого випромінювання. Систематизація елементного та кількісного складу досліджуваного віконного скла за періодами та групами періодичної системи хімічних елементів, дала змогу побачити залежність між електронною будовою хімічних елементів і захисними властивостями скла. Отримані результати показали, що коефіцієнти відбивання та поглинання змінюються відповідно до зміни хімічного складу досліджуваного скла, що дає можливість прогнозувати властивості та моделювати хімічний склад скла із заданими захисними властивостями [15].

На основі дослідження коефіцієнту відбивання скла з напиленням одношаровим покриттям діоксиду гафнію за допомогою спектральних характеристик, нами запропоновано використання захисних плівок з високою відбиваючою здатністю, що ускладнює або робить неможливим зняття інформації оптичним методом. Обґрунтовано можливі переваги використання діелектричних плівок діоксиду гафнію, так як коефіцієнт відбивання скла з напиленою плівкою значно вищий в порівнянні з чистим склом, що в разі підвищує захисні характеристики скла від витоку мовної інформації. Крім того, затрати на виготовлення та нанесення таких покриттів є суттєво меншими, ніж затрати на розробку та виробництво будь-яких активних засобів захисту у сучасному світі, що підтверджує переваги пасивних методів захисту мовної інформації від зчитування оптоелектронним каналом [16].

Проведені також дослідження та оцінка ефективності застосування захисної напівпровідникової плівки BaCuTeF , запропоновано спосіб одержання вдосконаленої структури аморфної електропровідної захисної плівки з подальшим отриманням кристалічної структури за допомогою проведення відпалу в атмосфері аргону, що за різних температур може значно покращити властивості пропускання видимого світла, збільшити потужність відбитого лазерного променя та більшою мірою поглинати потужність лазерного випромінювання у порівнянні з простими металізованими плівками. Дане дослідження дозволило зробити висновок, що встановлення такої захисної плівки у поєднанні з шаром барвника з високою відбивною здатністю на зовнішньому віконному склі будівлі знижує або повністю виключає ефективність лазерних засобів перехоплення голосової інформації, в основному через різке падіння потужності відбитого або поглиненого сигналу зовнішнім шаром скла з плівковим покриттям [17].

Аналізуючи результати дослідження, де авторами описана методика напилення одношарового покриття діоксиду гафнію з подальшим дослідженням коефіцієнту відбивання

скла з напиленою плівкою, та роботи [18], в якій було проведено дослідження захисних характеристик напилених на скло рельєфних плівок, ми дійшли висновку, що зміна кута нахилу склопакету та використання рельєфних плівок із зовнішнього боку скла суттєво впливають на коефіцієнт відбивання, що може ефективно та з мінімальними витратами забезпечити захист мовної інформації від ЛСАР.

На основі аналізу та узагальнення результатів попередніх досліджень стало можливим побудувати комплексну модель багатокомпонентної архітектурно-компонованої структури оптоелектронного каналу витоку інформації.

Результати

Складений оптоелектронний канал витоку інформації утворюється шляхом знімання інформації лазерним променем в ІЧ-діапазоні (ЛСАР) з плоскої поверхні скла, що коливається під дією акустичної хвилі з інформацією. Якщо ж брати за основу класичну структуру оптоелектронного каналу витоку інформації, то можемо констатувати, що джерелами акустичного сигналу в приміщенні може бути, в першу чергу, сама людина в процесі розмови і відбиті джерела сигналів. У нашому випадку – це віконне скло у відповідному розташуванні, встановленого хімічного складу, з використанням різноманітних напилень і плівок, яке з середовища розповсюдження стає також джерелом вібраційних коливань, тобто в залежності від кількості захисних шарів на склі, воно може послаблювати або посилювати джерела сигналів для зняття ЛСАР.

Разом з тим, на основі проведених експериментів і досліджень, можемо зазначити, що поширення вібрацій відрізняється в залежності від компонування матеріалів перешкоди (скла та ін. огорожувальних об'єктів), якою вони поширюються, та попередньої відповіді на скануючу дію лазерного променя.

Отже, структуру оптоелектронного каналу витоку інформації пропонуємо представити у вигляді пошарової моделі (Рис. 4.).

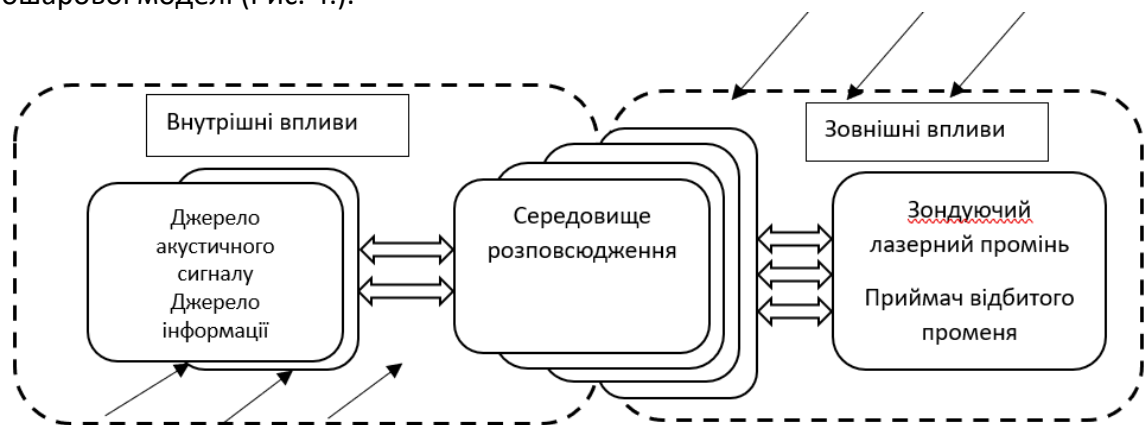


Рисунок 4 – Захисна пошарова модель багатокомпонентної архітектурно компонованої структури оптоелектронного каналу витоку інформації

Як видно з рисунка, поряд з джерелом вібраційних коливань прямої дії формується також відгук від проходження лазерного променя в середину приміщення і у зворотному напрямку.

Отже, захищеність приміщень від зняття мовної інформації системами лазерної розвідки має достатньо складну залежність і формується компонуванням багатьох взаємопов'язаних величин:

K_1 – якісний коефіцієнт захисту (елементний склад скла);

K_2 – кількісний коефіцієнт захисту (стехіометрія елементів скла);

K_3 – коефіцієнт захисних покриттів (плівки);

- K_4 – кутовий коефіцієнт (кут нахилу склопакету);
 K_5 – кутовий коефіцієнт (кут падіння лазерного променя);
 K_6 – «сендвіч» коефіцієнт (компонування захисних шарів);
 K_7 – коефіцієнт технічних характеристик приладів;
 K_n – n -ий коефіцієнт захисту.

Математична модель описує мінімізацію втрат інформації через оптоелектронний канал витоку від ЛСАР, що відповідає максимальному ступеню захищеності приміщення. Загальні або сумарні втрати інформації складаються з декількох складових, які пошарово компонуються на вихідному матеріалі (склі). Для кожного гіпотетичного шару існує повна (оптимальна) величина зменшення ризику витоку інформації оптоелектронним каналом від ЛСАР, який відповідає мінімуму. Цей мінімум втрат корелює з реальною чисельною характеристикою $K_{min}^{лсар}$, яка враховує компонування пошарових елементів, їх комбінацію, що беруть участь у вирішенні питання безпеки приміщення. У загальному випадку кінцева множина $K_{min}^{лсар}$ складається з n захисних шарів, тобто:

$$K_{min}^{лсар} = \sum_{i=1}^n K_n$$

де $K_{min}^{лсар}$ – коефіцієнт мінімальних втрат мовної інформації;
 K_n – коефіцієнт мінімальних втрат мовної інформації n -м захисним шаром.

Можемо припустити, що пошарова модель багатокомпонентної архітектурно компонованої структури оптоелектронного каналу витоку інформації розгортається на рівні агрегатної та комплексної моделі.

Агрегатна модель складної (пошарової) системи буде складатись з окремих підсистем та опису їх взаємодії (за класичною схемою). При вивченні цієї моделі підсистеми представлені окремими рівняннями, що пов'язують вихідні сигнали з вхідними сигналами та з параметрами підсистеми. Агрегатна модель буде подаватись системою цих рівнянь:

$$\begin{cases} K_1 = f_1(x_1, x_2, x_n \dots) \\ K_2 = f_2(x_1, x_2, x_n \dots) \\ K_n = f_n(x_1, x_2, x_n \dots) \end{cases}$$

Взаємодія підсистем (скло, напилення, захисні плівки, компонування та ін.) полягає в тому, що вихідні сигнали однієї підсистеми є вхідними для іншої і мають однакове позначення в агрегатній моделі. Вихідні сигнали однієї підсистеми вводяться в іншу і мають однакові назви в агрегатній моделі.

Комплексна (системна) модель розглядає джерело (середовище розповсюдження) в цілому, не розділяючи його на підсистеми і окремі внутрішні процеси. Коефіцієнт захисту можна представити у вигляді:

$$K_{зах} = f K_n$$

Разом з тим, комплексна модель при вирішенні конкретних завдань, може теж бути отримана і представлена у вигляді сумарної агрегатної моделі, шляхом зведення системи рівнянь до одного виразу, що пов'язує вхідні і вихідні сигнали системи, методом підстановки, в залежності від компонування складових захисту інформації від витоку оптоелектронним каналом.

Переваги цих підходів полягають в тому, що в залежності від завдань, які стоять перед системою і вихідних характеристик елементів, ми можемо довільно компоувати роботу системи в цілому, з готових компонентів з визначеними параметрами або критеріями і без

дослідження внутрішньої структури, опираючись тільки на потрібний результат. Очевидно, що представлена модель дозволить використовувати обидва підходи як для проведення експериментальних досліджень пошарових елементів, так і прогнозування теоретичних можливостей цілої системи захисту мовної інформації від ЛСАР.

Висновки

У результаті проведеного дослідження побудовано захисну модель багатокомпонентної архітектурно-компонованої структури оптоелектронного каналу витоку інформації, яка враховує комбінацію пошарових елементів, відгук від проходження лазерного променя в середину приміщень і у зворотному напрямку та розгортається на рівні агрегатної та комплексної моделі.

Встановлено, що **захищеність приміщень від зняття мовної інформації ЛСАР не є лінійною функцією, а формується складною комбінацією взаємопов'язаних параметрів**, включаючи відгук від проходження лазерного променя крізь багат шарові елементи будівельних конструкцій (наприклад, скло, захисні плівки та ін.).

Розроблена математична модель, що описує мінімізацію втрат інформації через оптоелектронний канал витоку від ЛСАР, дозволяє визначити **оптимальну величину зменшення ризику** для кожного гіпотетичного шару вихідного матеріалу, що, в свою чергу, відповідає **максимальному ступеню захищеності приміщення**.

Концепція “мінімуму втрат” відображає реальну чисельну характеристику ефективності комбінації пошарових елементів, які формують систему забезпечення безпеки приміщення. Таким чином, дослідження надає **наукову основу для проектування та оптимізації захисних систем**, дозволяючи досягти найбільш ефективної протидії лазерним системам акустичної розвідки шляхом цілеспрямованого впливу на фізичні властивості багат шарових архітектурних компонентів.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Іванченко, С. О., Гавриленко, О. В., Липський, О. А., & Шевцов, А. С. (2016). *Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навч. посіб.* ІСЗІ НТУУ «КПІ».
2. Горбенко, І., & Ковальчук, Ю. (2008). Оцінка характеристик лазерного каналу витоку мовної інформації з урахуванням багатомодового випромінювання лазера. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, (2), 83-88.
3. Громико, І. О. (2006). Загальна парадигма захисту інформації: визначення термінів від носіїв до каналів витоку інформації. *Системи обробки інформації*, 9(58), 3-9.
4. Дудикевич, В. Б., Собчук, І. С., Ракобовчук, В. О., & Лич, С. В. (2015). Дослідження властивостей плівок на основі діоксиду гафнію для захисту інформації від лазерного зондування. *Захист інформації і безпека інформаційних систем: матеріали IV міжнародної науково-технічної конференції* (С. 185–186).
5. Дудикевич, В. Б., Ракобовчук, В. О., Гаранюк, П. І., & Дей, В. А. (2014). Вплив діелектричного покриття на захисні властивості скла від витоку інформації через оптико-електронний

- канал. *Проблеми створення, розвитку та застосування високотехнічних систем спеціального призначення: Тези доповідей 20 Всеукр. наук.-практ. конф.*, 196-197.
6. Катаєв, В., & Яремчук, Ю. (2019). Метод активного захисту інформації від зняття лазерними системами акустичної розвідки. *Захист інформації*, 21(1), 34-39. <https://doi.org/10.18372/2410-7840.21.13545>
7. Abramov, P. I., Kuznetsov, E. V., & Skvortsov, L. A. (2017). Prospects of using quantum-cascade lasers in optoelectronic countermeasure systems: review. *J. Opt. Technol.*, 84, 331-341.
8. Horev, A., & Savin, A. (2021). Efficiency Research of Sun Protection Window Films for Speech Information Protection from LEAKAGE by Optoelectronic Channel. *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering* (pp. 2335-2339). <https://doi.org/10.1109/ElConRus51938.2021.9396253>
9. Klochko, N. P., Barbash, V. A., Klepikova, K. S., Kopach, V. R., Tyukhov, I. I., Yashchenko, O. V., Zhadan, D. O., Petrushenko, S. I., Dukarov, S. V., Sukhov, V. M., & Khrypunova, A. L. (2021). Biodegradable flexible transparent films with copper iodide and biomass-derived nanocellulose for ultraviolet and high-energy visible light protection. *Solar Energy*, 220, 852-863. <https://doi.org/10.1016/j.solener.2021.04.014>
10. Zeng, U., Pan, B., Cao, Y., & Ai, H. (2021). Test and analysis of window vibration for anti-laser-eavesdropping. *Applied Acoustics*, 176, 107871. <https://doi.org/10.1016/j.apacoust.2020.107871>
11. Kradolfer, S., Heutschi, K., Koch, J., & Gunther, D. (2021). Listening with curiosity—tracking the acoustic response of portable laser ablation. *Chimia*, 75(4), 300-304. <https://doi.org/10.2533/Chimia.2021.300>
12. Li, L., Zeng, H., Zhang, Y., Kong, Q., Zhou, Y., & Liu, Y. (2014). Analysis of backscattering characteristics of objects for remote laser voice acquisition. *Appl. Opt.*, 53, 971-978.
13. Zhang, W., Zhang, L., Liang, X., et al. (2017). Unconventional High-Performance Laser Protection System Based on Dichroic Dye-Doped Cholesteric Liquid Crystals. *Sci Rep*, 7, 42955. <https://doi.org/10.1038/srep42955>
14. Катаєв, В., & Яремчук, Ю. (2019). Метод активного захисту інформації від зняття лазерними системами акустичної розвідки. *Захист інформації*, 21(1), 34-39. <https://doi.org/10.18372/2410-7840.21.13545>
15. Dzianyi, N., Dudykevych, V., Opirskyy, I., Rakobovcuk, L., & Haraniuk, P. (2022). Investigation of the protective capabilities of glass from laser sounding depending on its elemental composition. *Eureka: Physics and Engineering*, (5), 162–174. <https://doi.org/10.21303/2461-4262.2022.002527>
16. Rakobovcuk, L., Dzianyi, N., Antonevych, M. (2023). Захисні характеристики плівок від лазерних систем акустичної розвідки на прикладі одношарового відбиваючого покриття діоксиду гафнію. *Ukrainian Scientific Journal of Information Security*, 29(1), 32-40. <http://infosecurity.nau.edu.ua>; <https://doi.org/10.18372/2225-5036.29.17550>
17. Dzianyi, N.R. (2019). Електропровідна плівка на вікна для захисту інформації від витoku оптоелектронним каналом. *Актуальні питання забезпечення кібербезпеки та захисту інформації: тези доповідей учасників IV Міжнар. наук.-практ. конф.* (С. 54-59). Видавництво Європейського університету.
18. Пархуць, Л. Т., Совин, Я. Р., & Ракобовчук, Л. М. (2024). Вплив інтер'єру приміщення на протидію лазерним системам акустичної розвідки. *Кібербезпека: освіта, наука, техніка*, 3(23), 246-257.

References

1. Ivanchenko, S. O., Havrylenko, O. V., Lyps'kyy, O. A., & Shevtsov, A. S. (2016). *Tekhnichni kanaly vy-toku informatsiyi. Poryadok stvorenniya kompleksiv tekhnichnoho zakhystu informatsiyi:*

- Navch. posib.* [Technical channels of information leakage. The procedure for creating complexes of technical information protection: Tutorial]. ISZZI NTUU «KPI».
2. Horbenko, I., & Kovalchuk, Y. (2008). Otsinka kharakterystyk lazernoho kanalu vy-toku movnoyi informatsiyi z urakhuvannyam bahatomodovoho vy-prominyuvannya lazera [Evaluation of the characteristics of the laser channel of speech information leakage taking into account multimode laser radiation]. *Pravove, normatyvne ta metrolohichne zabezpechennya systemy zakhystu informatsiyi v Ukraini*, (2), 83-88.
 3. Hromyko, I. O. (2006). Zahal'na paradyhma zakhystu informatsiyi: vyznachennya terminiv vid nosiyiv do kanaliv vy-toku informatsiyi [General paradigm of information security: Definition of terms from media to information leakage channels]. *Systemy obrobky informatsiyi*, 9(58), 3-9.
 4. Dudykevych, V. B., Sobchuk, I. S., Rakobovchuk, V. O., & Lych, S. V. (2015). Doslidzhennya vlastyvostry plivok na osnovi dioksydu hafniyu dlya zakhystu informatsiyi vid lazernoho zonduvannya [Investigation of the properties of hafnium dioxide-based films for information protection against laser sounding]. *Zakhyst informatsiyi i bezpeka informatsiynykh system: materialy IV mizhnarodnoyi naukovo-tekhnichnoyi konferentsiyi* (pp. 185–186).
 5. Dudykevych, V. B., Rakobovchuk, V. O., Haranyuk, P. I., & Dey, V. A. (2014). Vplyv dielektrychnoho pokryttya na zakhysni vlastyvostry skla vid vy-toku informatsiyi cherez optyko-elektronnyy kanal [The effect of dielectric coating on the protective properties of glass against information leakage through the optoelectronic channel]. *Problemy stvorenniya, rozvytku ta zastosuvannya vysokotekhnichnykh system spetsial'noho pryznachennya: Tezy dopovidey 20 Vseukr. nauk.-prakt. konf.*, 196-197.
 6. Katayev, V., & Yaremchuk, Y. (2019). Metod aktyvnoho zakhystu informatsiyi vid znyattya lazernymy systemamy akustychnoyi rozvidky [Method of active information protection against removal by laser systems of acoustic reconnaissance]. *Zakhyst informatsiyi*, 21(1), 34-39. <https://doi.org/10.18372/2410-7840.21.13545>
 7. Abramov, P. I., Kuznetsov, E. V., & Skvortsov, L. A. (2017). Prospects of using quantum-cascade lasers in optoelectronic countermeasure systems: review. *J. Opt. Technol.*, 84, 331-341.
 8. Horev, A., & Savin, A. (2021). Efficiency Research of Sun Protection Window Films for Speech Information Protection from LEAKAGE by Optoelectronic Channel. *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering* (pp. 2335-2339). <https://doi.org/10.1109/ElConRus51938.2021.9396253>
 9. Klochko, N. P., Barbash, V. A., Klepikova, K. S., Kopach, V. R., Tyukhov, I. I., Yashchenko, O. V., Zhadan, D. O., Petrushenko, S. I., Dukarov, S. V., Sukhov, V. M., & Khrypunova, A. L. (2021). Biodegradable flexible transparent films with copper iodide and biomass-derived nanocellulose for ultraviolet and high-energy visible light protection. *Solar Energy*, 220, 852-863. <https://doi.org/10.1016/j.solener.2021.04.014>
 10. Zeng, U., Pan, B., Cao, Y., & Ai, H. (2021). Test and analysis of window vibration for anti-laser-eavesdropping. *Applied Acoustics*, 176, 107871. <https://doi.org/10.1016/j.apacoust.2020.107871>
 11. Kradolfer, S., Heutschi, K., Koch, J., & Gunther, D. (2021). Listening with curiosity—tracking the acoustic response of portable laser ablation. *Chimia*, 75(4), 300-304. <https://doi.org/10.2533/Chimia.2021.300>
 12. Li, L., Zeng, H., Zhang, Y., Kong, Q., Zhou, Y., & Liu, Y. (2014). Analysis of backscattering characteristics of objects for remote laser voice acquisition. *Appl. Opt.*, 53, 971-978.
 13. Zhang, W., Zhang, L., Liang, X., et al. (2017). Unconventional High-Performance Laser Protection System Based on Dichroic Dye-Doped Cholesteric Liquid Crystals. *Sci Rep*, 7, 42955. <https://doi.org/10.1038/srep42955>
 14. Katayev, V., & Yaremchuk, Y. (2019). Metod aktyvnoho zakhystu informatsiyi vid znyattya lazernymy systemamy akustychnoyi rozvidky [Method of active information protection

- against removal by laser systems of acoustic reconnaissance]. *Zakhyst informatsiyi*, 21(1), 34-39. <https://doi.org/10.18372/2410-7840.21.13545>
15. Dzianyi, N., Dudykevych, V., Opirskyy, I., Rakobovcuk, L., & Haraniuk, P. (2022). Investigation of the protective capabilities of glass from laser sounding depending on its elemental composition. *Eureka: Physics and Engineering*, (5), 162–174. <https://doi.org/10.21303/2461-4262.2022.002527>
16. Rakobovcuk, L., Dzianyi, N., Antonevych, M. (2023). Захисні характеристики плівок від лазерних систем акустичної розвідки на прикладі одношарового відбиваючого покриття діоксиду гафнію [Protective characteristics of films from laser acoustic reconnaissance systems on the example of a single-layer reflective coating of hafnium dioxide]. *Ukrainian Scientific Journal of Information Security*, 29(1), 32-40. <http://infosecurity.nau.edu.ua>; <https://doi.org/10.18372/2225-5036.29.17550>
17. Dzianyi, N.R. (2019). Електропровідна плівка на вікна для захисту інформації від витоку оптоелектронним каналом [Electrically conductive film on windows for protecting information from leakage by optoelectronic channel]. *Aktual'ni pytannya zabezpechennya kiberbezpeky ta zakhystu informatsiyi: tezy dopovidey uchasnykiv IV Mizhnar. nauk.-prakt. konf.* (pp. 54-59). Vydavnytstvo Yevropeys'koho universytetu.
18. Parkhuts', L. T., Sovyn, Y. R., & Rakobovchuk, L. M. (2024). Vplyv inter'yeru primishchennya na protydyu lazernym systemam akustychnoyi rozvidky [The influence of the room interior on countering laser acoustic reconnaissance systems]. *Kiberbezpeka: osvita, nauka, tekhnika*, 3(23), 246-257.

Автоматизована система розпізнавання повітряних цілей за допомогою згорткових нейронних мереж

Automated system for recognizing air targets using convolutional neural networks

Олег Лавров

Corresponding author: к. тех. н., заступник начальника науково-дослідного відділу, e-mail: lavrov1107@gmail.com, ORCID: 0000-0003-1292-5986

Андрій Лавров

старший науковий співробітник науково-дослідного відділу, e-mail: andriy.lavrov@gmail.com, ORCID: 0009-0004-1138-2945

Oleg Lavrov

Corresponding author: PhD in Technical Sciences, Deputy Head of the Research Department, e-mail: lavrov1107@gmail.com, ORCID: 0000-0003-1292-5986

Andrii Lavrov

Senior Researcher in the Research Department, e-mail: andriy.lavrov@gmail.com, ORCID: 0009-0004-1138-2945

Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків, Україна

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

Received: August 13, 2025 | Revised: August 29, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.16>

Мета роботи. Підвищення ефективності і точності систем протиповітряної оборони шляхом розробки та впровадження автоматизованої системи розпізнавання повітряних цілей із використанням методів глибокого навчання, зокрема згорткових нейронних мереж.

Метод дослідження. Застосовано кількісний підхід із використанням публічного набору даних Drone Image Classification Dataset, що містить чотири класи зображень (три типи дронів та негативний клас).

Результати дослідження. Розроблена модель показала високу точність класифікації повітряних цілей у тестових умовах, забезпечивши надійну ідентифікацію дронів та стійкість до фонових перешкод.

Теоретична цінність дослідження. Поглиблено наукове розуміння можливостей використання згорткових нейронних мереж у завданнях реального часу з розпізнавання повітряних об'єктів, що сприяє розвитку теорії комп'ютерного зору у сфері безпілотних літальних апаратів.

Практична цінність дослідження. Отримані результати можуть бути використані для розробки та вдосконалення систем ППО, охорони стратегічних об'єктів та захисту критичної інфраструктури.

Оригінальність дослідження. Запропоновано ефективну архітектуру CNN для багатокласової класифікації повітряних цілей із використанням публічного датасету, що враховує негативний клас для підвищення стійкості системи.

Обмеження дослідження. Модель тестувалася на статичних зображеннях; для підвищення її ефективності в реальних умовах доцільно дослідити роботу з відеопотоками та застосування методів оптимізації обчислювальних ресурсів для вбудованих систем.

Тип статті. Прикладне дослідження.

Purpose. To enhance the efficiency and accuracy of air defense systems through the development and implementation of an automated air target recognition system based on deep learning methods, specifically convolutional neural networks (CNNs).

Method. A quantitative approach was applied using the public Drone Image Classification Dataset containing four image classes (three types of drones and a negative class).

Findings. The developed model demonstrated high classification accuracy of air targets under test conditions, ensuring reliable drone identification and robustness against background noise.

Theoretical implications. The research deepens the scientific understanding of applying convolutional neural networks to real-time air object recognition tasks, contributing to the advancement of computer vision theory in the field of unmanned aerial vehicles.

Practical implications. The obtained results can be utilized for the development and improvement of air defense systems, strategic facility protection, and critical infrastructure security.

Originality of the study. An effective CNN architecture for multi-class air target classification using a public dataset has been proposed, incorporating a negative class to improve system robustness.

Research limitations. The model was tested on static images; to improve its real-world performance, further research should address video stream processing and computational optimization methods for embedded systems.

Paper type. Applied research.

Ключові слова: згорткова нейронна мережа, дрони, розпізнавання повітряних цілей, обробка зображень, автоматизована система.

Key words: convolutional neural network, drones, air target recognition, image processing, automated system.

Вступ

Сучасні виклики у сфері забезпечення безпеки повітряного простору обумовлюють нагальну потребу у створенні високотехнологічних автоматизованих систем розпізнавання повітряних цілей.

Швидкий розвиток безпілотних літальних апаратів (БПЛА, дронів) різних класів, а також складних типів бойових літаків, а також загроза їх несанкціонованого використання роблять завдання ідентифікації повітряних об'єктів особливо актуальним для оборонної галузі.

Водночас традиційні методи класифікації та моніторингу повітряних об'єктів часто поступаються сучасним підходам штучного інтелекту у швидкості обробки великих обсягів даних та точності прогнозування. Особливої уваги потребують малі повітряні цілі, такі як комерційні та саморобні дрони, які все частіше використовуються у військових і цивільних конфліктах.

Теоретичні основи дослідження

Patil та інші (2025) запропонували оригінальний підхід до класифікації форм на основі акустичного розсіювання із використанням нейронних мереж, натренованих на синтетично згенерованих даних. Результати показали, що навіть за наявності обмеженої кількості експериментальних спостережень мережа здатна досягати високих показників точності при розпізнаванні складних контурів об'єктів. Це особливо важливо для задач пасивного виявлення дронів за допомогою акустичних сенсорів у реальному середовищі, де сигнал часто спотворюється шумом і перешкодами.

У свою чергу Chen та інші (2024) зосередили увагу на мультифідельному підході оптимізації аеродинамічних форм із використанням глибинних нейронних мереж та знання-орієнтованого вибору зразків. Вони довели, що їхній метод дозволяє зменшити обсяг дорогих високоточних симуляцій, водночас зберігаючи якість оптимізації. Це напряму співвідноситься з потребами дронобудування: оптимізація форми БПЛА під конкретні задачі (наприклад, максимальна дальність чи маневреність) може суттєво виграти від таких гібридних моделей.

Lee та інші (2025) представили підхід до детекції структурних пошкоджень за акустичними емісіями у реальному часі. Вони розробили глибоку CNN, яка у поєднанні з алгоритмами виділення спектральних ознак досягла точності класифікації понад 95% при ідентифікації тріщин і мікродефектів у складних структурах. Для безпілотних систем це відкриває можливість безперервного моніторингу технічного стану елементів каркасу під час польоту.

Водночас Ahmed та інші (2024) у своїй роботі зосередилися на гібридних архітектурах, що поєднують CNN із рекурентними мережами (RNN). Їхній підхід до діагностики несправностей обертових механізмів довів, що комбінація просторової та часової обробки сигналів дозволяє досягти точності діагностики понад 98% навіть за шумних виробничих умов. Це особливо цінно для розпізнавання дронів, що можуть мати обертові частини, наприклад, багатогвинтові системи.

Дослідження Wang та інші (2025) висвітлює перспективи інтеграції фізичних обмежень у структуру нейронних мереж для розв'язання обернених задач у структурній динаміці. Їхня фізично-обґрунтована модель (PINN) дозволила значно зменшити похибки між симульованими і фактичними результатами, що критично важливо для завдань моделювання аеродинамічної поведінки дронів у мінливих погодних умовах або при виявленні їх у складних фонів.

У дослідженні Kumar та інших (2024) представлена ансамблева архітектура глибинних моделей для виявлення дефектів у підшипниках. Вони показали, що поєднання кількох нейронних мереж дозволяє досягти точності понад 99% у складних робочих умовах. Це демонструє потенціал використання ансамблевих підходів у класифікації повітряних цілей, де може знадобитися обробка даних з різних сенсорів — відео, акустики, радіолокації.

Li та інші (2024) запропонували метод ідентифікації пошкоджень балкових конструкцій за допомогою автоенкодерів, що дозволяє працювати з великими обсягами неструктурованих даних. Їхній метод показав ефективне виявлення прихованих дефектів навіть у разі низької інтенсивності сигналу, що близько до задач виявлення малопомітних дронів серед складного фону.

У роботі Zhang та інших (2025) CNN моделі використовувались для прогнозування втомного ресурсу металевих матеріалів. Автори досягли зниження середньоквадратичної похибки на понад 15% у порівнянні з традиційними підходами, що особливо важливо для

визначення залишкового ресурсу конструкцій безпілотників, які можуть працювати у жорстких умовах експлуатації.

Park та інші (2024) зосередилися на визначенні ударних навантажень у композитних структурах за допомогою CNN. Їхній метод дозволяє відслідковувати локальні пошкодження в режимі реального часу, що прямо відповідає вимогам до оцінки бойової готовності БПЛА після експлуатації у складних умовах.

Nguyen та інші (2024) реалізували фреймворк глибинного навчання для моніторингу мостів у реальному часі з використанням даних прискорень. Вони досягли точності понад 95% у прогнозуванні стану конструкцій при навантаженні. Аналогія з БПЛА очевидна: моделі з онлайн-моніторингом можуть забезпечувати оцінку стану дронів під час виконання польотів, що підвищує надійність їх використання.

Zhao та інші (2025) акцентували увагу на застосуванні трансферного навчання для виявлення пошкоджень за обмежених даних. Вони показали, що перенавчання моделей дозволяє підвищити точність прогнозування на 12% у порівнянні зі стандартними моделями. Це напряму пов'язано з практичним викликом розпізнавання нових типів дронів у реальних умовах, коли обсяг навчальних даних обмежений.

Liu та інші (2025) запропонували комбінацію глибинних мереж із вейвлет-перетворенням, що дозволяє виділяти дрібномасштабні ознаки ушкоджень у складних конструкціях. Їхня модель досягла точності понад 96% при мінімальній кількості попередньої обробки сигналу. Wang та співавт. (2025) успішно продемонстрували застосування CNN для моніторингу мостів під навантаженням рухомого транспорту, досягнувши стабільності прогнозу у режимі реального часу з точністю понад 97%. Це ще раз підкреслює можливість CNN працювати у динамічних умовах та обробляти великі потоки даних.

Постановка проблеми

Узагальнення представлених результатів свідчить про високий потенціал глибинних нейронних мереж у різних галузях моніторингу складних технічних об'єктів. Однак при цьому більшість досліджень не зосереджується безпосередньо на розпізнаванні малогабаритних повітряних цілей, зокрема дронів, у складних середовищах з високим рівнем шуму або мінливими погодними умовами. Це визначає актуальність запропонованої розробки, що спрямована на створення гнучкої та масштабованої CNN-системи для автоматизованого розпізнавання дронів із можливістю подальшої адаптації до різних сценаріїв застосування.

Метою роботи є розробка та апробація автоматизованої системи розпізнавання повітряних цілей, зокрема безпілотних літальних апаратів (дронів) із використанням згорткових нейронних мереж, яка забезпечує класифікацію типів повітряних об'єктів, передусім різних типів дронів, у реальному або наближеному до реального часу. Запропонована система має продемонструвати стійкість до різних умов знімання, бути придатною для інтеграції у практичні комплекси спостереження та протиповітряної оборони, а також мати архітектуру, що легко масштабується для подальшого донавчання під специфічні типи цілей.

Методологія дослідження

Для того щоб обґрунтувати працездатність запропонованого підходу та перевірити можливість ефективної класифікації типів повітряних об'єктів у режимі, наближеному до реального часу, було проведено серію експериментів із використанням згорткової нейронної мережі (CNN). Головною метою було продемонструвати, що навіть порівняно проста архітектура CNN здатна вирішувати завдання розпізнавання дронів різних типів у змінних умовах знімання та відокремлювати їх від фонових сцен, у яких об'єкт відсутній.

У якості навчальної та тестової вибірки використано відкритий Drone Image Classification Dataset, що спеціально сформований для задач класифікації цивільних безпілотних літальних апаратів за візуальними ознаками. Цей датасет охоплює чотири окремі класи: DJI Inspire, DJI Mavic, DJI Phantom та No Drone. Три перші класи відповідають різним комерційним моделям дронів, що на практиці відрізняються за габаритами, формами, конфігураціями гвинтів і конструктивними особливостями, що створює різноманітність у вигляді контурів та характерних ознак на зображеннях. Четвертий клас No Drone сформовано як негативний, він містить зображення типових фонових сцен — фрагментів неба, міського або природного середовища без присутності будь-яких повітряних об'єктів. Наявність такої контрольної групи особливо важлива для підготовки моделі, яка має не лише розпізнавати присутність дрона, але й з високою достовірністю ідентифікувати його відсутність, мінімізуючи хибнопозитивні спрацювання у реальних умовах експлуатації.

Дані у межах кожного класу підібрані так, щоб максимально врахувати варіативність зовнішніх факторів. Зокрема, зображення включають різні кути зйомки — як фронтальні, так і з верхніх, бічних і діагональних перспектив. Це дозволяє моделі навчитися виділяти стабільні контурні та текстурні ознаки незалежно від положення дрона у кадрі, що є критично важливим для систем, які працюють у режимі безперервного моніторингу. Окрім різних ракурсів, у вибірці представлені зображення з різною якістю освітлення: зйомки вдень при яасному небі, у хмарних умовах та при частковому затемненні об'єкта. Таке різноманіття забезпечує підвищення стійкості моделі до змін зовнішнього середовища, які є типовими для реального театру спостереження повітряного простору.

З технічної точки зору датасет структуровано за принципом розподілу на дві логічні частини: навчальну (train) та валідаційну (val). Це відповідає кращим практикам машинного навчання, де навчальна підмножина використовується для оптимізації параметрів мережі, а валідаційна дозволяє об'єктивно оцінювати узагальнюючу здатність моделі на прикладах, які не використовувалися під час навчання. Кожен підрозділ організовано у вигляді ієрархії директорій за назвами класів, що спрощує завантаження даних через генератори ImageDataGenerator у середовищі TensorFlow/Keras та полегшує процес аугментації, масштабування й нормалізації зображень.

Додатковим аргументом на користь вибору саме цього датасету є його висока якість та достатній обсяг, що дозволяє уникнути переобучення при збереженні відносно компактної архітектури моделі. Формат зображень дозволяє легко підлаштовувати їх під стандартизовані вхідні розміри CNN, а наявність чітких класів без перетинів мінімізує ймовірність семантичних помилок під час навчання. При цьому клас No Drone виконує роль потужного засобу формування так званої фонової чутливості — здатності моделі диференціювати релевантні об'єкти від шумових та нефункціональних даних.

Обраний датасет не лише відповідає технічним вимогам до збалансованості та різноманітності вибірки, але й імітує реалістичні умови, що наближає процес тестування до умов реальної експлуатації автоматизованих систем протиповітряного спостереження. Це робить Drone Image Classification Dataset доцільною та виправданою основою для побудови й апробації експериментальної моделі.

Результати

Для вирішення поставленої задачі було реалізовано згорткову нейронну мережу, яка складається з трьох основних блоків згорткових шарів з функціями активації ReLU, шарів підвибірки (MaxPooling) та повнозв'язної частини з додатковим шаром Dropout для запобігання перенавчанню (див. фрагмент коду у файлі main.py). Вихідний шар має чотири нейрони, що відповідають кількості класів, і використовує функцію активації softmax для багатокласової класифікації. Архітектура моделі обрана так, щоб балансувати між достатньою

глибиною для виділення інформативних ознак та низькою обчислювальною складністю, що дозволяє використовувати модель у сценаріях з обмеженими ресурсами, наприклад, на вбудованих обчислювальних модулях дронів чи ППО.

Математично робота CNN ґрунтується на згортковій операції, що описується виразом:

$$Z_{i,j}^{(k)} = (X * K^{(k)})_{i,j} + b^{(k)}, \quad (1)$$

де X – вхідне зображення або ознакові карти попереднього шару;
 $K^{(k)}$ – ядро згортки для k -го фільтра;
 $*$ – операція згортки (підхід до застосування CNN для ідентифікації силових впливів у композитних структурах побудованих на основі [9]).

На виході застосовується функція активації ReLU:

$$f(x) = \max(0, x), \quad (2)$$

що забезпечує нелінійність та сприяє кращому наближенню складних залежностей (підхід до застосування ReLU в архітектурі для задач моніторингу в реальному часі побудований на основі [3]). Завдяки таким обчислювальним блокам модель послідовно перетворює вихідні піксельні дані у набір високорівневих ознак, які в подальшому класифікуються у відповідні типи повітряних цілей.

Обрана структура та принципи функціонування дозволяють запропонованій системі демонструвати гнучкість при роботі з різними типами даних та спрощують інтеграцію моделі у реальні комплекси автоматизованого спостереження за повітряним простором.

Для реалізації поставленої мети було розроблено повноцінний експериментальний цикл, що включає етапи підготовки даних, побудови архітектури згорткової нейронної мережі, процесу навчання, оцінювання якості роботи моделі та організації візуалізації результатів.

На першому етапі було здійснено підключення та первинну обробку даних. Було використано можливості стандартного генератора зображень ImageDataGenerator з бібліотеки TensorFlow Keras, що дозволило виконати масштабування піксельних значень до діапазону [0; 1] для уніфікації шкали ознак та зниження ризику нестабільності градієнтів під час навчання. Усі зображення було приведено до єдиного розміру 150 × 150 пікселів, що забезпечує баланс між збереженням інформативності та швидкістю обробки даних у процесі згортки. Розмір пакету (batch size) було встановлено рівним 32, що дало змогу забезпечити оптимальний компроміс між стабільністю оптимізації та використанням пам'яті відеокарти.

На другому етапі було реалізовано послідовну архітектуру моделі (Sequential API). Було передбачено три каскади згорткових шарів (Conv2D) з функціями активації ReLU, кожен з яких супроводжується шарами підвибірки (MaxPooling2D). Зокрема, було налаштовано:

перший згортковий блок із 32 фільтрами та ядром 3×3,

другий — із 64 фільтрами,

третій — із 128 фільтрами, що дозволило моделі послідовно виділяти як базові, так і високорівневі ознаки.

Після каскаду згортки було здійснено розгортання багатовимірного тензора у вектор (Flatten), який передавався до повнозв'язного шару (Dense) з 128 нейронів та активацією ReLU. Для запобігання перенавчанню було впроваджено шар Dropout із коефіцієнтом 0.5, що вимикає 50% нейронів на кожній ітерації навчання. Вихідний шар було спроектовано як багатокласовий softmax з 4 нейронами, що відповідають кількості класів у вибірці (DJI Inspire, DJI Mavic, DJI Phantom, No Drone).

Для оптимізації параметрів моделі було застосовано алгоритм Adam, що забезпечує адаптивну швидкість навчання та стабільність сходження. В якості функції втрат було обрано

категоріальну крос-ентропію, що є стандартною для багатокласової класифікації. Тривалість навчання було обмежено 10 епохами для демонстраційних цілей, однак структура дозволяє масштабувати цей параметр для підвищення точності у подальших експериментах.

Логіка функціонування запропонованої програми наведена на рис. 1.

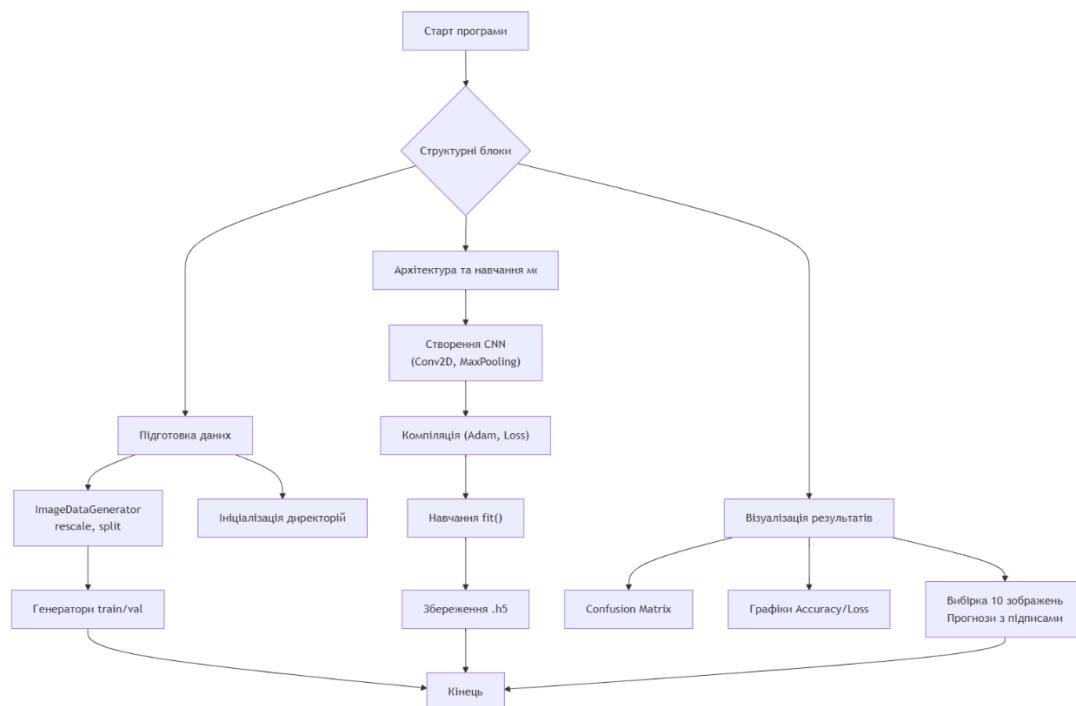


Рисунок 1 – Логічна структура роботи автоматизованої системи розпізнавання повітряних цілей

Джерело: побудовано автором

На основі розробленого коду було реалізовано послідовний алгоритм роботи, що включає такі ключові етапи:

1. Було ініціалізовано службові директорії `models/` і `results/` для збереження моделі та проміжних артефактів.

2. Було сформовано генератори потоків даних із автоматичною подачею батчів, масштабуванням та перетворенням зображень у тензорний формат.

3. Було здійснено повний цикл навчання моделі, під час якого ваги мережі оптимізувалися за допомогою зворотного поширення помилки та градієнтного спуску.

4. Після завершення навчання модель було серіалізовано у форматі HDF5 (.h5), що дозволяє зберегти архітектуру та ваги для повторного використання без необхідності повторного тренування.

5. Для контролю якості було побудовано графіки зміни точності (accuracy) та функції втрат (loss) на кожній епісі.

6. Було розраховано та візуалізовано матрицю змішування (confusion matrix), що демонструє співвідношення правильних і хибних класифікацій для кожного класу.

7. Для валідації наочної працездатності мережі було сформовано підсумкове вікно з випадково відібраними 10 зображеннями, для кожного з яких модель здійснила прогноз із виведенням передбаченого класу та рівня впевненості.

Було розроблено компактну, але функціонально достатню архітектуру згорткової нейронної мережі, що може застосовуватися як базова структура для подальшого

нарощування складності та інтеграції у практичні системи моніторингу повітряного простору з акцентом на автоматизоване розпізнавання дронів.

Для перевірки працездатності розробленої згорткової нейронної мережі було проведено серію експериментів, результати яких демонструють відповідність моделі поставленим вимогам з точки зору точності класифікації, стійкості роботи у змінних умовах та здатності ідентифікувати об'єкти малої розмірності.

У першу чергу було здійснено кількісний аналіз зміни функції втрат (loss) протягом 10 епох навчання. Як видно з графіка (рис. 2), крива функції втрат для навчальної вибірки демонструє стабільне зниження від початкового значення близько 0,52 до рівня близько 0,03, що вказує на ефективне навчання моделі без значних коливань чи ознак дивергенції. Для валідаційної вибірки значення втрат протягом навчання зберігаються у межах від 0,18 до 0,1, що свідчить про відсутність значного перенавчання та достатню узагальнюючу здатність моделі.

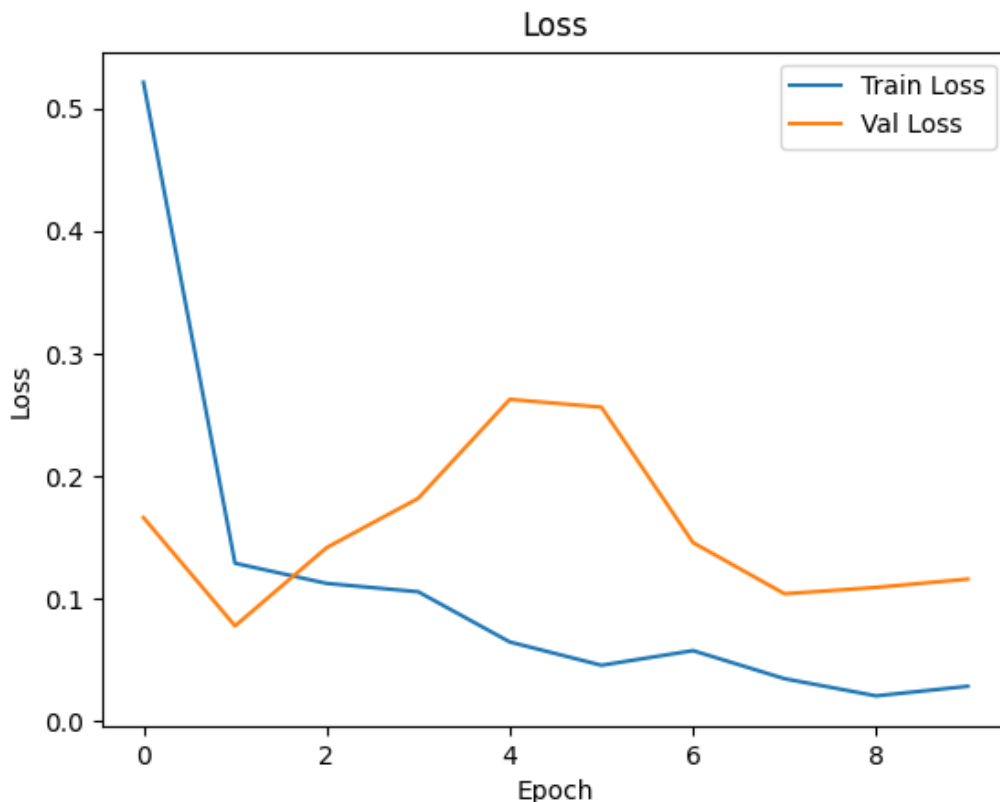


Рисунок 2 – Динаміка функції втрат під час навчання та валідації

Джерело: побудовано програмним рішенням, розробленим автором

Додатково було оцінено динаміку точності класифікації (accuracy) на кожній епосі. Згідно з отриманими даними (рис. 3), точність на навчальній множині зростає з близько 80 % у першій ітерації до понад 99 % наприкінці циклу, що демонструє ефективне засвоєння ключових ознак дронів і фонових сцен. Точність на валідаційній множині зберігається на рівні 97–98 % протягом останніх епох, що підтверджує стійкість моделі до невідомих даних.

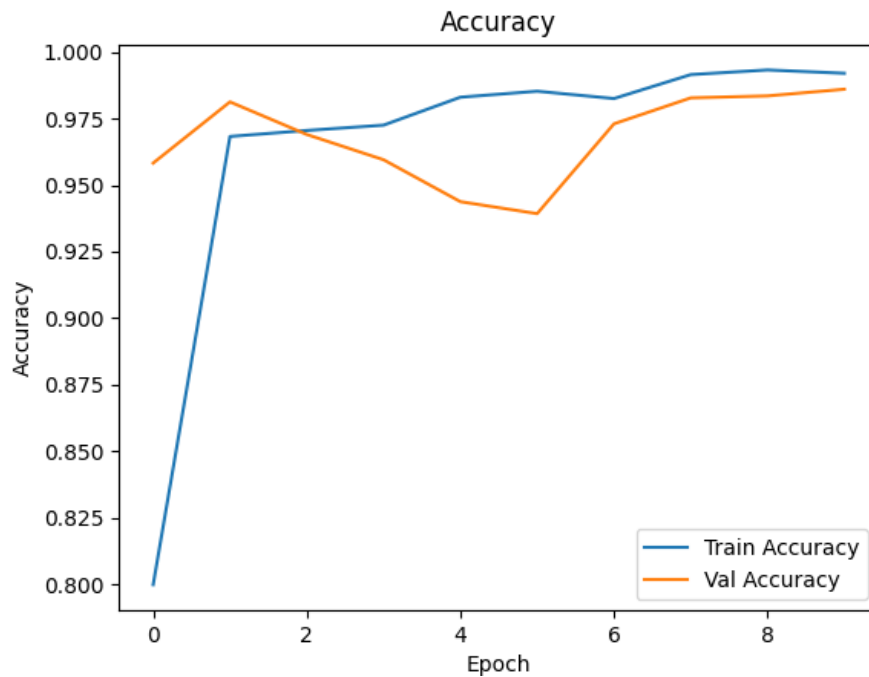


Рисунок 3 – Динаміка точності класифікації під час навчання та валідації

Джерело: побудовано програмним рішенням, розробленим автором

Одним з ключових доказів працездатності є побудова матриці змішування (confusion matrix), яка дозволяє деталізувати розподіл правильних та хибних передбачень по кожному класу (рис. 4). Аналіз матриці свідчить про надзвичайно високу точність класифікації: більшість зображень кожного класу правильно ідентифікуються з незначною кількістю помилок між суміжними класами. Наприклад, для класу DJI Inspire правильно класифіковано 979 випадків із 1000, для DJI Mavic – 992 випадки, що відповідає рівню точності вище 99 %. Клас No Drone також демонструє стабільне розпізнавання з мінімальною кількістю хибнопозитивних спрацювань, що підтверджує спроможність моделі адекватно працювати з фоновими сценами.

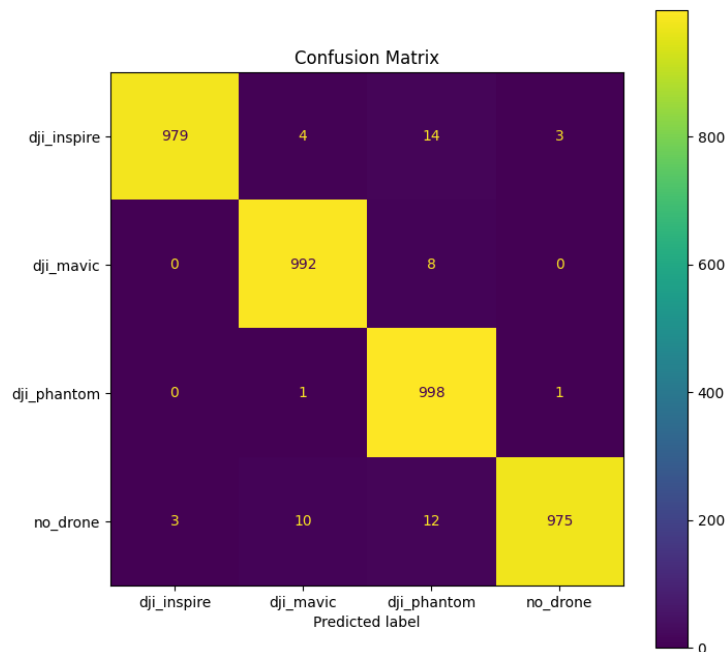


Рисунок 4 – Матриця змішування результатів класифікації для чотирьох класів

Джерело: побудовано програмним рішенням, розробленим автором

Окрім кількісних метрик, було проведено візуальний аналіз роботи моделі на реальних зображеннях, що не входили до навчальної множини. Для цього було випадково обрано 10 зображень із усіх класів і виконано передбачення типу об'єкта разом з розрахунком рівня впевненості (рис. 5). Як видно з прикладів, модель із високою ймовірністю (>97% у більшості випадків) відокремлює класи DJI Inspire, DJI Mavic та DJI Phantom навіть за різного рівня розмитості, ракурсу та освітлення. Це наочно демонструє спроможність мережі виділяти ключові просторово-текстурні ознаки дронів навіть у складних умовах, що особливо важливо для реальних систем протиповітряного моніторингу.

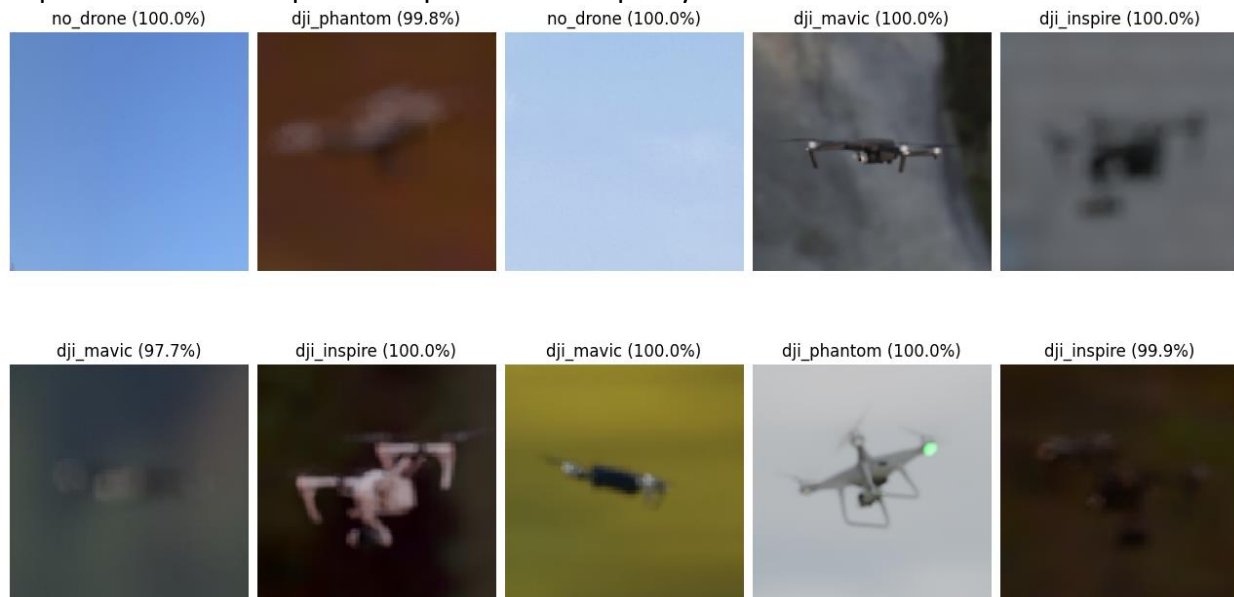


Рисунок 5 – Приклади прогнозів моделі для 10 випадкових зображень із відображенням класу та рівня впевненості

Джерело: побудовано програмним рішенням, розробленим автором

Отримані результати демонструють, що запропонована система здатна ефективно вирішувати задачу класифікації дронів навіть на обмеженому наборі вхідних даних та в умовах різних типів спотворень (розмитість, затемнення, низький контраст). Новизна підходу полягає в успішній реалізації гнучкої та легко масштабованої архітектури CNN, орієнтованої саме на виявлення і диференціацію повітряних об'єктів у складних реаліях реального середовища. Додатково, наявність негативного класу *no_drone* у структурі моделі підвищує її прикладну значущість, оскільки забезпечує здатність до фільтрації фонових сцен і зниження кількості помилкових спрацьовувань, що є ключовим у сценаріях реального часу (наприклад, у комплексах ППО або відеоспостереження).

Можна стверджувати, що розроблена модель не лише підтвердила свою функціональну ефективність у задачі розпізнавання дронів, але й є потенційною базою для побудови більш масштабованих систем моніторингу повітряного простору з використанням глибинного навчання.

Висновки

Проведене дослідження продемонструвало, що використання згорткових нейронних мереж (CNN) для автоматизованого розпізнавання повітряних цілей, зокрема безпілотних літальних апаратів, є перспективним напрямом, що має вагоме практичне значення для удосконалення систем моніторингу повітряного простору. На основі запропонованої архітектури було доведено можливість ефективної багатокласової класифікації об'єктів із різними геометричними та конструктивними характеристиками в умовах мінливої видимості та

фоновому шуму. Особливо цінною є властивість моделі виявляти відсутність об'єкта за наявності фонових сцен, що істотно знижує ймовірність хибнопозитивних спрацювань і підвищує надійність роботи системи у реальному середовищі.

Одержані результати засвідчили, що навіть при відносно компактній архітектурі й помірному обсязі навчальної вибірки можна досягти високих показників точності та стабільності прогнозування. Це створює умови для подальшої оптимізації моделі під реальні потреби сил протиповітряної оборони та цивільних структур моніторингу. Зокрема, перспективними є напрями адаптації архітектури для роботи на обмежених апаратних ресурсах — мобільних чи автономних комплексах спостереження, інтеграції у складі гібридних систем, які поєднують різномірні датчики: оптичні, акустичні та радіолокаційні.

Водночас результати даної розробки відкривають низку подальших дослідницьких завдань. По-перше, актуальним є розширення набору навчальних даних шляхом залучення реальних зображень дронів із різних джерел, що дозволить підвищити узагальнюючу здатність моделі до нових класів повітряних цілей. По-друге, доцільно розглянути інтеграцію технологій трансферного навчання та фізично обґрунтованих обмежень у структуру мережі, що забезпечить підвищення точності за умови обмеженої кількості розмічених даних. По-третє, значну перспективу становить розробка механізмів адаптивного донавчання безпосередньо під час експлуатації системи у польових умовах — з використанням методів безперервного навчання (continual learning).

Окремо слід підкреслити, що запропонований підхід має потенціал бути масштабованим і мультисенсорним. Це означає можливість розширення архітектури для роботи не лише з фото- чи відеоданими, але й зі складними сигналами акустичного чи радіолокаційного характеру. Такий напрямок відповідає сучасним тенденціям розвитку інтелектуальних систем спостереження, де ключовим є комплексний підхід до збору й обробки інформації з метою досягнення високої точності в умовах багатофакторної невизначеності.

У цілому проведена робота формує підґрунтя для подальших наукових і прикладних досліджень у сфері розпізнавання повітряних цілей із використанням глибинного навчання, що має стратегічне значення для підвищення обороноздатності, безпеки критичної інфраструктури та розвитку високотехнологічних автоматизованих систем у військовій і цивільній авіації.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Patil, G. U., Kwon, H.-S., Epureanu, B. I., & Popa, B.-I. (2025). Synthetically-trained neural networks for shape classification from measured acoustic scattering. *Journal of Sound and Vibration*, 618, 119229. <https://doi.org/10.1016/j.jsv.2025.119229>
2. Chen, Y., Huang, Y., Xu, C., & Zhao, X. (2024). Multi-fidelity surrogate-based shape optimization using deep neural networks and knowledge-based sampling. *Aerospace Science and Technology*, 153, 108932. <https://doi.org/10.1016/j.ast.2024.108932>
3. Lee, J., Choi, J., & Kim, J. (2025). Deep learning-based real-time structural damage detection using acoustic emission. *Engineering Structures*, 310, 117006. <https://doi.org/10.1016/j.engstruct.2025.117006>

4. Ahmed, S., Wang, X., Li, H., & Zhang, Y. (2024). A hybrid deep learning approach for fault diagnosis of rotating machinery. *Measurement*, 226, 113161. <https://doi.org/10.1016/j.measurement.2024.113161>
5. Wang, Q., Liu, Z., Chen, Z., & Xu, B. (2025). Physics-informed neural networks for solving inverse problems in structural dynamics. *Mechanical Systems and Signal Processing*, 205, 110807. <https://doi.org/10.1016/j.ymssp.2024.110807>
6. Kumar, R., Singh, R., Sharma, M., & Patel, S. (2024). An intelligent fault diagnosis method for roller bearings using ensemble deep learning models. *ISA Transactions*, 144, 554–564. <https://doi.org/10.1016/j.isatra.2024.04.015>
7. Li, J., Zhang, L., Wang, T., & Xu, K. (2024). Damage identification of beam structures using deep autoencoder networks. *Structural Control and Health Monitoring*, 31(3), e3039. <https://doi.org/10.1002/stc.3039>
8. Zhang, H., Gao, Y., Li, P., & Sun, W. (2025). Deep learning for fatigue life prediction of metallic materials. *International Journal of Fatigue*, 173, 107848. <https://doi.org/10.1016/j.ijfatigue.2024.107848>
9. Park, S., Kim, Y., Jung, H., & Lee, D. (2024). A convolutional neural network-based approach for impact force identification in composite structures. *Composite Structures*, 328, 116962. <https://doi.org/10.1016/j.compstruct.2023.116962>
10. Nguyen, T., Pham, H., Tran, D., & Bui, T. (2024). Deep learning-based structural health monitoring using acceleration response. *Sensors and Actuators A: Physical*, 361, 114529. <https://doi.org/10.1016/j.sna.2024.114529>
11. Zhao, H., Wang, Y., Chen, M., & Zhou, J. (2025). Transfer learning for damage detection in structures with limited labeled data. *Structural Health Monitoring*, 24(2), 123–136. <https://doi.org/10.1177/14759217231123609>
12. Liu, Y., Li, H., Zhang, J., & Chen, Y. (2025). Structural damage detection based on deep belief networks and wavelet packet decomposition. *Journal of Civil Structural Health Monitoring*, 15(1), 1–14. <https://doi.org/10.1007/s13349-024-00624-2>
13. Wang, J., Xu, Y., Yang, Z., & Hu, J. (2025). A deep learning framework for real-time damage detection of bridges under moving loads. *Computer-Aided Civil and Infrastructure Engineering*, 40(5), 482–499. <https://doi.org/10.1111/mice.12997>
14. Drone type classification. (n.d.). *Kaggle*. URL : <https://www.kaggle.com/datasets/balajikarthek/drone-type-classification>

References

1. Patil, G. U., Kwon, H.-S., Epureanu, B. I., & Popa, B.-I. (2025). Synthetically-trained neural networks for shape classification from measured acoustic scattering. *Journal of Sound and Vibration*, 618, 119229. <https://doi.org/10.1016/j.jsv.2025.119229>
2. Chen, Y., Huang, Y., Xu, C., & Zhao, X. (2024). Multi-fidelity surrogate-based shape optimization using deep neural networks and knowledge-based sampling. *Aerospace Science and Technology*, 153, 108932. <https://doi.org/10.1016/j.ast.2024.108932>
3. Lee, J., Choi, J., & Kim, J. (2025). Deep learning-based real-time structural damage detection using acoustic emission. *Engineering Structures*, 310, 117006. <https://doi.org/10.1016/j.engstruct.2025.117006>
4. Ahmed, S., Wang, X., Li, H., & Zhang, Y. (2024). A hybrid deep learning approach for fault diagnosis of rotating machinery. *Measurement*, 226, 113161. <https://doi.org/10.1016/j.measurement.2024.113161>
5. Wang, Q., Liu, Z., Chen, Z., & Xu, B. (2025). Physics-informed neural networks for solving inverse problems in structural dynamics. *Mechanical Systems and Signal Processing*, 205, 110807. <https://doi.org/10.1016/j.ymssp.2024.110807>

6. Kumar, R., Singh, R., Sharma, M., & Patel, S. (2024). An intelligent fault diagnosis method for roller bearings using ensemble deep learning models. *ISA Transactions*, 144, 554–564. <https://doi.org/10.1016/j.isatra.2024.04.015>
7. Li, J., Zhang, L., Wang, T., & Xu, K. (2024). Damage identification of beam structures using deep autoencoder networks. *Structural Control and Health Monitoring*, 31(3), e3039. <https://doi.org/10.1002/stc.3039>
8. Zhang, H., Gao, Y., Li, P., & Sun, W. (2025). Deep learning for fatigue life prediction of metallic materials. *International Journal of Fatigue*, 173, 107848. <https://doi.org/10.1016/j.ijfatigue.2024.107848>
9. Park, S., Kim, Y., Jung, H., & Lee, D. (2024). A convolutional neural network-based approach for impact force identification in composite structures. *Composite Structures*, 328, 116962. <https://doi.org/10.1016/j.compstruct.2023.116962>
10. Nguyen, T., Pham, H., Tran, D., & Bui, T. (2024). Deep learning-based structural health monitoring using acceleration response. *Sensors and Actuators A: Physical*, 361, 114529. <https://doi.org/10.1016/j.sna.2024.114529>
11. Zhao, H., Wang, Y., Chen, M., & Zhou, J. (2025). Transfer learning for damage detection in structures with limited labeled data. *Structural Health Monitoring*, 24(2), 123–136. <https://doi.org/10.1177/14759217231123609>
12. Liu, Y., Li, H., Zhang, J., & Chen, Y. (2025). Structural damage detection based on deep belief networks and wavelet packet decomposition. *Journal of Civil Structural Health Monitoring*, 15(1), 1–14. <https://doi.org/10.1007/s13349-024-00624-2>
13. Wang, J., Xu, Y., Yang, Z., & Hu, J. (2025). A deep learning framework for real-time damage detection of bridges under moving loads. *Computer-Aided Civil and Infrastructure Engineering*, 40(5), 482–499. <https://doi.org/10.1111/mice.12997>
14. Drone type classification. (n.d.). *Kaggle*. Available from : <https://www.kaggle.com/datasets/balajikartheek/drone-type-classification>

Організаційно-правові засади обліку військових витрат та втрат

Organizational and Legal Principles of Accounting for Military Expenditures and Losses

Артем Філіппов

Corresponding author: кандидат юридичних наук, доцент, професор кафедри військового права та правоохоронної діяльності, e-mail: avphill@ukr.net, ORCID: 0000-0002-9035-144X

Златіна Марчук

молодший науковий співробітник, e-mail: zkapanova71@gmail.com, ORCID: 0009-0003-5575-3093

Artem Filippov

Corresponding author: Candidate of Law, Associate Professor, Professor of the Department of Military Law and Law Enforcement, e-mail: avphill@ukr.net, ORCID: 0000-0002-9035-144X

Zlatina Marchuk

Junior researcher, e-mail: zkapanova71@gmail.com, ORCID: 0009-0003-5575-3093

Національний університет оборони України, м. Київ, Україна

National University of Defense of Ukraine, Kyiv, Ukraine

Received: July 30, 2025 | Revised: August 15, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.17>

Мета роботи. Розкрити організаційно-правові засади ведення обліку військових витрат і витрат у системі Міністерства оборони України в умовах збройної агресії російської федерації.

Метод дослідження. Порівняльний аналіз, синтез, індукція та дедукція, системний підхід, метод контент-аналізу, спеціально-юридичний метод.

Результати дослідження. Висвітлено організаційно-правові засади ведення обліку витрат і витрат у системі Міністерства оборони України, окреслено основні прогалини та проблемні аспекти чинної системи, зокрема в умовах воєнного стану.

Теоретична цінність дослідження. Аналіз чинної нормативно-правової бази засвідчив фрагментарність і недостатню інтеграцію системи обліку військових витрат та втрат із сучасними цифровими рішеннями та міжнародними практиками.

Практична цінність дослідження. Виявлено проблемні аспекти механізмів обліку військових витрат та втрат, які впливають на повноту і достовірність інформації про завдані збитки та формування доказової бази для подальших репарацій.

Тип статті. Теоретична.

Purpose. To elucidate the organizational and legal foundations for recording and accounting for military losses and expenditures within the system of the Ministry of Defence of Ukraine in the context of the Russian Federation's armed aggression.

Method. Comparative analysis; synthesis; induction and deduction; a systems approach; content analysis; and the doctrinal (special-legal) method.

Findings. The study outlines the organizational and legal framework for recording and accounting for losses and expenditures in the Ministry of Defence of Ukraine and identifies key gaps and problem areas in the current system, particularly under conditions of martial law.

Theoretical implications. Analysis of the current legal and regulatory framework indicates fragmentation and insufficient integration of the system for accounting for military expenditures and losses with modern digital solutions and international practices.

Practical implications. The study reveals problematic aspects of the mechanisms for accounting for military expenditures and losses that affect the completeness and reliability of information on damages incurred and the development of an evidentiary basis for subsequent reparations.

Paper type. Theoretical.

Ключові слова: витрати, втрати, збитки, облік, оцінка збитків, шкода.

Key words: expenditures, losses; damages, accounting, damage assessment, harm.

Вступ

В умовах сучасних збройних конфліктів питання обліку військових витрат і втрат набуває особливої актуальності. Ефективний облік є необхідною передумовою фінансової прозорості, раціонального використання ресурсів та стратегічного планування оборонної політики. Організаційні аспекти такого обліку нерозривно пов'язані з правовим регулюванням, що визначає відповідальні органи, процедури та методи ведення обліку. Не менш важливою є організаційна складова — міжвідомча взаємодія, впровадження сучасних інформаційних систем і використання міжнародного досвіду.

З огляду на міжнародну практику, особливої ваги набуває формування належної доказової бази для подальших міжнародних репарацій. Щоб це стало можливим, необхідно забезпечити повноту та достовірність обліку всіх видів втрат і витрат, спричинених збройною агресією російської федерації, а також створити належну доказову базу для їх підтвердження.

Теоретичні основи дослідження

Правові проблеми відшкодування шкоди, завданої агресією РФ, досліджувались як зарубіжними, так і вітчизняними науковцями. В українському дискурсі наявні праці, присвячені методиці оцінювання вартості бойових втрат угруповання військ (сил), аналізу системи показників ресурсного забезпечення сил оборони, нормативно-правовому забезпеченню процесів оцінки збитків у військовій сфері, дефініціям військових втрат та витрат, а також міжнародно-правовим аспектам компенсації України. Водночас комплексні правові проблеми відшкодування збитків і шкоди у розрізі військових втрат та витрат залишаються дослідженими фрагментарно, що зумовлює необхідність систематизації організаційно-правової бази обліку.

Постановка проблеми

Метою статті є аналіз правових актів, що регламентують облік військових втрат і витрат у Збройних Силах України та Міністерстві оборони України (МОУ), із фокусом на організаційній структурі суб'єктів, відповідальних за такий облік. На основі зібраних даних здійснено оцінку недоліків і проблемних аспектів чинної системи в умовах воєнного стану.

Результати

Організаційна архітектура обліку

Облік втрат і витрат у Збройних Силах України (ЗСУ) організовано як багаторівневу систему, центральну роль у якій відіграє МОУ як орган формування політики, нормотворчості та уніфікації методик. У структурі МОУ функціонують профільні департаменти (персонал, фінансовий облік, логістика, обіг майна, цифрові платформи — зокрема Єдина автоматизована система управління обліком особового складу ЗСУ (ЄАСУОС), АСУ “Оборона”). Генеральний штаб ЗСУ в межах делегованих повноважень координує збір, верифікацію та аналітику даних щодо втрат і витрат і забезпечує імплементацію стандартів у військах.

На оперативному рівні облік здійснюється в командуваннях видів ЗСУ (Сухопутні війська, Повітряні сили, ВМС) та територіальних оперативних командуваннях (“Схід”, “Захід”, “Північ”, “Південь”), що акумулюють звітність із підпорядкованих військових частин. Первинне документування здійснюється у військових частинах відповідними підрозділами з обліку особового складу, тилового забезпечення та логістики з оформленням актів, журналів і рапортів. Централізований аналіз у профільних структурах МОУ дозволяє здійснювати фінансове прогнозування, планування постачання, формувати резерви та готувати звітність.

Облік військового майна: нормативна основа та практики

Ключові акти, що регламентують бухгалтерський та матеріальний облік у ЗСУ, включають:

- Наказ МОУ № 905 від 19.12.2014 “Про затвердження Методичних рекомендацій з організації та ведення бухгалтерського обліку у Збройних Силах України”. Документ уніфікує підходи до бухгалтерського обліку, регламентує оформлення господарських операцій, ведення реєстрів, подання фінансової звітності та внутрішній контроль.
- Постанова КМУ № 1225 від 04.08.2000 (чинна редакція від 12.03.2024) “Про затвердження Положення про порядок обліку, зберігання, списання та використання військового майна у Збройних Силах України”. Положення встановлює детальний порядок обліку, зберігання, списання та використання військового майна і закріплює принцип всеосяжного обліку.
- Наказ МОУ № 440 від 17.08.2017 “Про затвердження Інструкції з обліку військового майна у Збройних Силах України”. Інструкція визначає порядок ведення реєстрів, заповнення форм, інвентаризацію та документування втрат.

- Наказ МОУ № 81 від 29.03.2021 “Про затвердження Порядку списання військового майна у Збройних Силах України та Державній спеціальній службі транспорту”, із урахуванням Наказу МОУ № 288 від 06.05.2024 (зміни щодо списання в умовах воєнного стану, спрощене підтвердження втрат у бойових умовах, можливість використання фото-/відеофіксації, свідчень та інспекторських посвідчень).

Облік військового майна передбачає ідентифікацію за заводськими/обліковими номерами, фіксацію якісних характеристик та вартості, що забезпечує зв'язок із бухгалтерським обліком і плануванням закупівель. Відстеження втрат за індивідуальними ідентифікаторами дає змогу проводити службові розслідування, запобігати незаконному обігу майна та планувати заміну конкретних одиниць.

Таблиця 1 – Керівні документи, які регламентують облік військового майна

Тип документу	Номер і дата	Назва	Короткий опис щодо обліку втрат та витрат
Наказ МОУ	№ 905 від 19.12.2014	Про затвердження Методичних рекомендацій з організації та ведення бухгалтерського обліку у ЗСУ	Єдині підходи до організації бухгалтерського обліку у військових частинах; регламентація документування, звітності та внутрішнього контролю.
Постанова КМУ	№ 1225 від 04.08.2000 (ред. 12.03.2024)	Про затвердження Положення про порядок обліку, зберігання, списання та використання військового майна у ЗСУ	Визначає порядок обліку/списання військового майна; закріплює принцип всеосяжного обліку й підстави для списання.
Наказ МОУ	№ 440 від 17.08.2017	Про затвердження Інструкції з обліку військового майна у ЗСУ	Деталізує облік майна, форми, реєстри, інвентаризацію, документування втрат.
Наказ МОУ	№ 81 від 29.03.2021	Про затвердження Порядку списання військового майна у ЗСУ та ДССТ	Встановлює процедуру списання майна як наслідку втрат; зв'язок із розслідуванням причин.
Наказ МОУ	№ 288 від 06.05.2024	Про затвердження Змін до Порядку списання військового майна у ЗСУ та ДССТ	Уточнює та спрощує процедури списання в умовах воєнного стану.
Постанова КМУ	№ 287 від 12.03.2024	Про внесення змін до Положення, затвердженого постановою № 1225	Оновлює положення щодо обліку військового майна, зокрема аспектів втрат/витрат.

Облік особового складу

Центральним актом є Наказ МОУ № 280 від 15.09.2022 “Про затвердження Інструкції з організації обліку особового складу в системі Міністерства оборони України”. Інструкція визначає перелік персональних документів (особові справи, послужні та обліково-послужні картки), стандарти електронного журналу обліку особового складу, порядок складання статистичних документів (донесення про склад і чисельність, відомості, довідки), а також процедури виключення зі списків у разі загибелі, полону, інтернування чи зникнення безвісти із відповідним інформуванням ТЦК та СП та архівуванням матеріалів.

Структурно пов'язаний акт — Постанова КМУ № 1487 від 30.12.2022 “Про затвердження Порядку організації та ведення військового обліку призовників, військовозобов'язаних і резервістів”. Хоча документ не регулює безпосередньо фіксацію втрат, він створює базові організаційні передумови воєнного обліку людських ресурсів.

Таблиця 2 – Керівні документи, які регламентують облік особового складу

Тип документу	Номер і дата	Назва	Короткий опис щодо обліку втрат та витрат
Постанова КМУ	№ 1487 від 30.12.2022	Про затвердження Порядку організації та ведення військового обліку призовників, військовозобов'язаних і резервістів	Визначає порядок військового обліку громадян — основу для підтримання актуальності даних про людські ресурси.
Наказ МОУ	№ 280 від 15.09.2022	Про затвердження Інструкції з організації обліку особового складу в системі МОУ	Регламентує персональний/штатно-посадовий облік, електронний журнал, повідомлення та виключення зі списків, статистичні звіти.

Первинний облік втрат і витрат та оцінка збитків (Методика № 277)

Первинний облік є критично важливим для подальшої **вартісної оцінки збитків**. Відповідно до Наказу МОУ № 277 від 14.09.2022 “Про затвердження Методики визначення військових втрат, завданих Україні внаслідок збройної агресії Російської Федерації”, оцінка здійснюється на основі первинних документів: рапортів командирів, актів знищення/пошкодження майна, довідок медичних підрозділів, бухгалтерських реєстрів, інвентаризаційних описів, журналів обліку боєприпасів тощо. Процедурно встановлюється зв'язок між фактологічним обліком (подія втрати) та вартісною оцінкою (визначення залишкової вартості/собівартості), що є необхідним для формування доказів у національних і міжнародних інституціях (у т. ч. для подальших механізмів міжнародних репарацій).

Інтеграція з міжнародними стандартами (НАТО/ЄС)

Інтеграція української системи з міжнародними стандартами зумовлена стратегічними пріоритетами, вимогами звітності перед міжнародними партнерами/донорами та перспективами вступу до НАТО. Гармонізація з STANAG (зокрема 2116 — Military Personnel Structure; 2034 — Logistics reporting; 2406 — логістичні норми) та впровадження LOGFAS, NATO Codification System (NSN), JLSG сприятимуть уніфікації кодів, звітних форм (у т. ч. BDCR — Battle Damage and Casualty Report), централізації даних і підвищенню оперативності управлінських рішень.

Таблиця 3 – Порівняльний аналіз систем обліку втрат і витрат: ЗСУ та країни-члени НАТО

Критерій	Україна (ЗСУ)	НАТО (країни-члени)	Необхідні зміни / правки в Україні
Нормативна основа	Національні акти МОУ/КМУ; часткова інтеграція	STANAG, уніфіковані процедури	Гармонізація з STANAG 2116, 2034, 2406; імплементація звітних форм BDCR
Облік особового складу	ЄАСУОС; обмежена інтеграція з цивільними реєстрами	Інтегровані бази, сумісні з е-урядом	Інтеграція ЄАСУОС із демографічним реєстром; уніфікація кодів категорій втрат
Облік майна/техніки	Накази № 440, № 81; бухгалтерський та оперативний облік	LOGFAS, NCS (NSN), централізовані бази	Обов'язкова кодифікація за NCS; повна автоматизація логістичних процесів
Списання втрат	Через акти/накази; часто тривалі процедури	Автоматизоване списання з негайною реєстрацією	Спрощення процедури “оперативного акта втрати” в бойових умовах
Фінансовий облік втрат	Наказ № 905; оцінка — за Методикою № 277	Єдині методики логістичних/фінансових втрат	Узгодження з логістичними нормами НАТО (зокрема STANAG 2406)
Звітування про	Внутрішні рапорти;	Єдина форма BDCR;	Розроблення національного

Критерій	Україна (ЗСУ)	НАТО (країни-члени)	Необхідні зміни / правки в Україні
втрати	ручне введення	автоматизація	аналога BDCR з автогенерацією
Цифрові системи	ЄАСУОС, АСУ “Оборона”, частково Excel	LOGFAS, NMCRL, JEMM	Хмарна інтегрована платформа, сумісна з JLSG
Контроль і аудит	Інспекції МОУ, ВСП, Рахункова палата	Незалежний аудит, міжнародні спостерігачі	Внутрішній незалежний аудит за моделлю NATO Audit Committee

Висновки

Система обліку військових витрат і втрат у ЗСУ має сформовану нормативну основу, чітку ієрархію відповідальності та інструменти документування. Водночас зберігається фрагментарність і недостатня інтегрованість із сучасними цифровими рішеннями та міжнародними стандартами, що обмежує ефективність у воєнний час. На наш погляд, пріоритетними є:

імплементація положень STANAG (2116, 2034, 2406) і формату BDCR у національне законодавство;

запровадження єдиного електронного журналу обліку втрат із автогенерацією звітів; реформування процедур списання у бойових умовах (спрощений “оперативний акт втрати”);

інтеграція ЄАСУОС та АСУ “Оборона” у хмарну платформу, сумісну з LOGFAS/JLSG;

впровадження незалежного внутрішнього аудиту за моделлю NATO Audit Committee.

Узгодженість обліку з міжнародними стандартами посилить довіру партнерів, підвищить якість звітності, оптимізує бюджетне планування та зміцнить позиції України в питаннях постконфліктного відшкодування збитків.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

- Семененко, О., Митченко, С., Добровольський, Ю., Коверга, В., Ярмольчик, М., & Тарасов, Р. (2022). Методика оцінювання вартості бойових втрат угруповання військ (сил) в операціях (бойових діях). *Social Development and Security*, 12(6), 11-18. <https://doi.org/10.33445/sds.2022.12.6.2>
- Сотник В. В., Косарецький Є. І., Могилевська В. О., Куцак С. В., Філіппов А. В. (2025). Аналіз системи показників ресурсного забезпечення сил оборони. *Бізнесінформ*, (3), 76–82.
- Марчук З. П., Коцюрuba Р. Б. (2025, 21 лютого). Нормативно-правове забезпечення процесів оцінки збитків у військовій сфері. *Правова система України: європейський вектор розвитку в умовах воєнного стану*: мат-ли XV МНПК. Київ: ДУ «Київський авіаційний інститут». Тернопіль: Вектор.
- Філіппов А. В. (2025, 21 лютого). Правова дефініція військових втрат та витрат: проблеми удосконалення. *Правова система України: європейський вектор розвитку в умовах воєнного стану*: мат-ли XV МНПК. Київ: ДУ «Київський авіаційний інститут». Тернопіль: Вектор.

5. Філіппов А. В., Юрко В. В. (2024, 20 грудня). Правові засади компенсації Україні військових витрат та втрат, збитків та шкоди, завданих агресією РФ. У: Андрійко О. Ф., Беззубов Д. О. (ред.). *Адміністративне і фінансове законодавство як інструмент правового забезпечення діяльності органів виконавчої влади в умовах воєнного стану*: мат-ли Всеукр. круглого столу. Київ: Видавництво Людмила, 2025.
6. Філіппов А. В. (2025). Міжнародно-правові засади компенсації Україні військових втрат та витрат. *Правова держава*.
7. Філіппов А. В., Косарецький Є. І. (2025). Термінологічні проблеми реалізації права України на відшкодування шкоди та збитків внаслідок збройної агресії РФ (за напрямом військових втрат). *Альманах права. Феномен реалізації права в контексті сучасного наукового дискурсу*, Вип. 16. Київ: ІДП ім. В. М. Корецького НАН України.
8. Про затвердження Інструкції з організації та ведення бухгалтерського обліку у Збройних Силах України: Наказ МОУ № 905 від 19.12.2014. (Офіц. публ.; доступні копії в мережі, зокрема: Scribd — *нормативний текст*).
9. Про затвердження Положення про порядок обліку, зберігання, списання та використання військового майна у Збройних Силах: Постанова КМУ № 1225 від 04.08.2000 (чинна ред. від 12.03.2024).
10. Про затвердження Інструкції з обліку військового майна у Збройних Силах України: Наказ МОУ № 440 від 17.08.2017.
11. Про затвердження Порядку списання військового майна у Збройних Силах України та Державній спеціальній службі транспорту: Наказ МОУ № 81 від 29.03.2021.
12. Про затвердження Змін до Порядку списання військового майна у Збройних Силах України та Державній спеціальній службі транспорту: Наказ МОУ № 288 від 06.05.2024.
13. Про затвердження Інструкції з організації обліку особового складу в системі Міністерства оборони України: Наказ МОУ № 280 від 15.09.2022.
14. Про затвердження Порядку організації та ведення військового обліку призовників, військовозобов'язаних і резервістів: Постанова КМУ № 1487 від 30.12.2022.
15. Про затвердження Методики визначення військових втрат, завданих Україні внаслідок збройної агресії Російської Федерації: Наказ МОУ № 277 від 14.09.2022.
16. Косарецький Є. І., Куцак С. В., Могилевська В. О., Сотник В. В. (2024). Дослідження механізмів оцінки збитків та шкоди, завданих складовим сил оборони внаслідок збройної агресії: нормативно-правові аспекти. *Зб. наук. праць Центру воєнно-стратегічних досліджень*, № 3(82).
17. Могилевська, В., Сотник, В., Коцюруба, Р., & Марчук, З. (2024). Аналіз методологічного забезпечення обліку та оцінки військових витрат та втрат. *Social Development and Security*, 14(6), 182-191. <https://doi.org/10.33445/sds.2024.14.6.18>
18. Косарецький Є. І. (2024). Обґрунтування показників визначення військових втрат, завданих внаслідок бойових дій. *Social Development and Security*, 14(6).
19. Коцюруба Р. Б. (2024, 17 жовтня). Особливості визначення збитків внаслідок пошкодження та знищення нерухомого майна. *Проблеми оборонного менеджменту: теорія і практика*: зб. мат-лів наук.-практ. конф. Київ.
20. Марчук З. П. (2024, 17 жовтня). Аналіз методики визначення втрат підприємств оборонно-промислового комплексу у зв'язку із збройною агресією. *Проблеми оборонного менеджменту: теорія і практика*: зб. мат-лів наук.-практ. конф. Київ.

References

1. Semenenko, O., Mytchenko, S., Dobrovolskyi, Y., Koverga, V., Yarmolchuk, M., & Tarasov, R. (2022). Methodology for estimating the cost of combat losses of a group of troops (forces)

- in operations (combat actions). *Social Development and Security*, 12(6), 11-18. <https://doi.org/10.33445/sds.2022.12.6.2> [in Ukrainian]
2. Sotnyk, V. V., Kosaretskyi, Ye. I., Mohylevska, V. O., Kutsak, S. V., & Filippov, A. V. (2025). Analiz systemy pokaznykiv resursnoho zabezpechennia syl oborony [Analysis of the indicator system for resource support of the defence forces]. *BiznesInform*, (3), 76–82. [in Ukrainian]
 3. Marchuk, Z. P., & Kotsiuruba, R. B. (2025, February 21). Normatyvno-pravove zabezpechennia protsesiv otsinky zbytkiv u viiskovii sferi [Regulatory framework for damage assessment processes in the military sphere]. In *Pravova systema Ukrainy: yevropeyskyi vektor rozvytku v umovakh voiennoho stanu: materialy XV mizhnarodnoi naukovo-praktychnoi konferentsii* (Kyiv, State University “Kyivskyi aviatsiinyi instytut”; Ternopil: Vektor). [in Ukrainian]
 4. Filippov, A. V. (2025, February 21). Pravova definitsiia viiskovykh vtrat ta vytrat: problemy udoskonalennia [Legal definition of military losses and expenditures: Issues of improvement]. In *Pravova systema Ukrainy: yevropeyskyi vektor rozvytku v umovakh voiennoho stanu: materialy XV mizhnarodnoi naukovo-praktychnoi konferentsii* (Kyiv, State University “Kyivskyi aviatsiinyi instytut”; Ternopil: Vektor). [in Ukrainian]
 5. Filippov, A. V., & Yurko, V. V. (2025). Pravovi zasady kompensatsii Ukraini viiskovykh vytrat ta vtrat, zbytkiv ta shkody, zavdanykh ahresiieiu RF [Legal grounds for compensating Ukraine’s military expenditures and losses caused by Russia’s aggression]. In O. F. Andriiko & D. O. Bezzubov (Eds.), *Administratyvne i finansove zakonodavstvo yak instrument pravovoho zabezpechennia diialnosti orhaniv vykonavchoi vlady v umovakh voiennoho stanu: materialy Vseukrainskoho kruhloho stolu* (Kyiv: Liudmyla). (Event date: December 20, 2024). [in Ukrainian]
 6. Filippov, A. V. (2025). Mizhnarodno-pravovi zasady kompensatsii Ukraini viiskovykh vtrat ta vytrat [International legal foundations for compensating Ukraine’s military losses and expenditures]. *Pravova derzhava*. [in Ukrainian]
 7. Filippov, A. V., & Kosaretskyi, Ye. I. (2025). Terminolohichni problemy realizatsii prava Ukrainy na vidshkoduvannia shkody ta zbytkiv vnaslidok zbroinoi ahresii RF (za napriamom viiskovykh vtrat) [Terminological issues in implementing Ukraine’s right to compensation for damage due to Russia’s aggression]. *Almanakh prava. Fenomen realizatsii prava v konteksti suchasnoho naukovoho dyskursu*, (16). Kyiv: Institute of State and Law named after V. M. Koretsky, NAS of Ukraine. [in Ukrainian]
 8. Ministry of Defence of Ukraine. (2014, December 19). Nakaz № 905: Pro zatverdzhennia Metodichnykh rekomendatsii z orhanizatsii ta vedennia bukhhalterskoho obliku u Zbroinykh Sylakh Ukrainy [Order No. 905: On approval of methodological recommendations for accounting in the Armed Forces of Ukraine]. [Government regulation; in Ukrainian]
 9. Cabinet of Ministers of Ukraine. (2000, August 4/2024, March 12, current version). Postanova № 1225: Pro zatverdzhennia Polozhennia pro poriadok obliku, zberihannia, spysannia ta vykorystannia viiskovoho maina u Zbroinykh Sylakh [Resolution No. 1225: On approval of the Regulation on accounting, storage, write-off and use of military property in the Armed Forces]. [Government regulation; in Ukrainian]
 10. Ministry of Defence of Ukraine. (2017, August 17). Nakaz № 440: Pro zatverdzhennia Instruksii z obliku viiskovoho maina u Zbroinykh Sylakh Ukrainy [Order No. 440: On approval of the Instruction on accounting for military property in the Armed Forces of Ukraine]. [Government regulation; in Ukrainian]
 11. Ministry of Defence of Ukraine. (2021, March 29). Nakaz № 81: Pro zatverdzhennia Poriadku spysannia viiskovoho maina u Zbroinykh Sylakh Ukrainy ta Derzhavnii spetsialnii sluzhbi transportu [Order No. 81: On approval of the Procedure for write-off of military property in

- the Armed Forces of Ukraine and the State Special Transport Service]. [Government regulation; in Ukrainian]
12. Ministry of Defence of Ukraine. (2024, May 6). Nakaz № 288: Pro zatverdzhennia Zmin do Poriadku spysannia viiskovoho maina u Zbroinykh Sylakh Ukrainy ta Derzhavnii spetsialnii sluzhbi transportu [Order No. 288: On amendments to the Procedure for write-off of military property]. [Government regulation; in Ukrainian]
 13. Ministry of Defence of Ukraine. (2022, September 15). Nakaz № 280: Pro zatverdzhennia Instruksii z orhanizatsii obliku osobovoho skladu v systemi Ministerstva oborony Ukrainy [Order No. 280: On approval of the Instruction on personnel accounting in the MoD system]. [Government regulation; in Ukrainian]
 14. Cabinet of Ministers of Ukraine. (2022, December 30). Postanova № 1487: Pro zatverdzhennia Poriadku orhanizatsii ta vedennia viiskovoho obliku pryzyvnykiv, viiskovozobov'iazanykh i rezervistiv [Resolution No. 1487: On approval of the Procedure for organising and maintaining military records of conscripts, liable reservists]. [Government regulation; in Ukrainian]
 15. Ministry of Defence of Ukraine. (2022, September 14). Nakaz № 277: Pro zatverdzhennia Metodyky vyznachennia viiskovykh vtrat, zavdanykh Ukraini vnaslidok zbroinoi ahresii Rosiiskoi Federatsii [Order No. 277: On approval of the Methodology for determining military losses caused to Ukraine]. [Government regulation; in Ukrainian]
 16. Kosaretskyi, Ye. I., Kutsak, S. V., Mohylevska, V. O., & Sotnyk, V. V. (2024). Doslidzhennia mekhanizmiv otsinky zbytkiv ta shkody, zavdanykh skladovym syl oborony vnaslidok zbroinoi ahresii: normatyvno-pravovi aspekty [Mechanisms for assessing losses and damage to defence components: Legal aspects]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen*, 3(82). [in Ukrainian]
 17. Mogylevska, V., Sotnyk, V., Kotsiuruba, R., & Marchuk, Z. (2024). Analysis of methodological providing for accounting and assessment of military costs and losses. *Social Development and Security*, 14(6), 182-191. <https://doi.org/10.33445/sds.2024.14.6.18> [in Ukrainian]
 18. Kosaretskyi, Ye. I. (2024). Obgruntuvannia pokaznykiv vyznachennia viiskovykh vtrat, zavdanykh vnaslidok boiovykh dii [Justification of indicators for determining military losses due to hostilities]. *Social Development and Security*, 14(6). [in Ukrainian]
 19. Kotsiuruba, R. B. (2024, October 17). Osoblyvosti vyznachennia zbytkiv vnaslidok poshkodzhennia ta znyshchennia nerukhomoho maina [Specifics of determining losses due to damage and destruction of real estate]. In *Problemy oboronnoho menedzhmentu: teoriia i praktyka: zbirnyk materialiv naukovo-praktychnoi konferentsii* (Kyiv). [in Ukrainian]
 20. Marchuk, Z. P. (2024, October 17). Analiz metodyky vyznachennia vtrat pidpriemstv oboronno-promyslovoho kompleksu u zv'iazku iz zbroinoiu ahresieiu [Analysis of the methodology for determining losses of defence-industrial enterprises]. In *Problemy oboronnoho menedzhmentu: teoriia i praktyka: zbirnyk materialiv naukovo-praktychnoi konferentsii* (Kyiv). [in Ukrainian]

Стан економічного розвитку росії в умовах повномасштабної агресії проти України

The State of Russia's Economic Development in the Context of Full-Scale Aggression Against Ukraine

Микола Ткач ^A

Corresponding author: доктор економічних наук, доцент, e-mail: nyck1985@ukr.net, ORCID: 0000-0002-8832-1268

Микола Хомік ^A

д. тех н., професор, e-mail: nkhomik@ukr.net, ORCID: 0000-0002-1201-7702

Іван Ткач ^A

д. екон. н., професор, e-mail: tim68@ukr.net, ORCID: 0000-0001-5547-6303

Тетяна Чернега ^B

здобувач, e-mail: chtetiana888@gmail.com, ORCID: 0009-0000-5534-6664

Дмитро Дриньов ^A

e-mail: drinevdim@gmail.com

Mykola Tkach ^A

Corresponding author: Dr of Economics, Associate Professor, e-mail: nyck1985@ukr.net, ORCID: 0000-0002-8832-1268

Mykola Khomik ^A

Dr of Technical Sciences, Professor, e-mail: nkhomik@ukr.net, ORCID: 0000-0002-1201-7702

Ivan Tkach ^A

Doctor of Economic Sciences, Professor, e-mail: tim68@ukr.net, ORCID: 0000-0001-5547-6303

Tetiana Cherneha ^B

Recipient, e-mail: chtetiana888@gmail.com, ORCID: 0009-0000-5534-6664

Dmytro Drynov ^A

e-mail: drinevdim@gmail.com

^A Національний університет оборони України, м. Київ, Україна

^B Міністерство оборони України, м. Київ, Україна

^A National University of Defense of Ukraine, Kyiv, Ukraine

^B Ministry of Defense of Ukraine, Kyiv, Ukraine

Received: August 03, 2025 | Revised: August 15, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.18>

Мета роботи. Системний аналіз трансформацій, що відбулися в економіці російської федерації (рф) у період з 2022 по 2025 роки внаслідок розв'язаної нею повномасштабної війни проти України.

Метод дослідження. У дослідженні використано системний та міждисциплінарний підходи, що поєднують елементи макроекономічного аналізу, політичної економії, воєнної економіки та санкційної політики.

Результати дослідження. Розробка конкретних, інноваційних рекомендацій для урядів, міжнародних організацій та інших зацікавлених сторін, які можуть бути впроваджені для максимізації зусиль щодо економічного тиску на російську федерацію.

Теоретична цінність дослідження. Дослідження допоможе поглибити розуміння впливу військових конфліктів на економіку країни, зокрема, на її макроекономічні показники, фінансовий сектор, зовнішньоекономічні зв'язки, соціальну сферу та інші аспекти.

Практична цінність дослідження. Результати дослідження можуть допомогти урядовим інституціям та міжнародним організаціям у розробці та адаптації економічних політик та стратегій, спрямованих на максимізацію економічного тиску на рф для зменшення її спроможностей по забезпеченню військових потреб.

Цінність дослідження. Полягає у забезпеченні конкретних інструментів та рекомендацій, які можуть бути застосовані різними зацікавленими сторонами для максимізації економічного тиску на економіку рф для зменшення її економічних спроможностей по забезпеченню військових потреб.

Обмеження дослідження. Обмеження дослідження полягає у використанні джерел, що знаходяться у відкритому доступі. Майбутні дослідження будуть спрямовані на вивченні позитивного та негативного досвіду щодо санкційної політики по відношенню до національної економіки рф.

Тип статті. теоретичний, практичний.

Purpose. The purpose of this study is a systematic analysis of the transformations that took place in the economy of the Russian Federation in the period from 2022 to 2025 as a result of the full-scale war against Ukraine.

Method. The study uses systemic and interdisciplinary approaches that combine elements of macroeconomic analysis, political economy, military economics and sanctions policy.

Findings. developing specific, innovative recommendations for governments, international organizations and other stakeholders that can be implemented to maximize efforts to put economic pressure on the russian federation.

Theoretical implications. The results of the study complement the existing theoretical research in the field of development of the military-industrial complex, and also take into account the practical experience of the russian-Ukrainian war.

Practical implications. The study will help to deepen the understanding of the impact of military conflicts on the country's economy, in particular, on its macroeconomic indicators, financial sector, foreign economic relations, social sphere and other aspects.

Originality/Value. The results of the study can help governmental institutions and international organizations in developing and adapting economic policies and strategies aimed at maximizing economic pressure on the russian federation to reduce its ability to meet military needs.

Research limitations/Future research. is to provide specific tools and recommendations that can be used by various stakeholders to maximize economic pressure on the russian economy to reduce its economic capacity to meet military needs.

Papertype. theoretical and practical.

Ключові слова: національна економіка, ВВП, нафта, інфляція, експорт, зовнішня торгівля.

Key words: national economy, GDP, oil, inflation, exports, foreign trade.

Вступ

Повномасштабне вторгнення російської федерації в Україну, що розпочалося 24 лютого 2022 року, стало не лише найбільшим збройним конфліктом у Європі з часів Другої світової війни, а й зумовило масштабні трансформації в економіці держави-агресора. В умовах безпрецедентного санкційного тиску, згорання зовнішньоекономічних зв'язків із Заходом та переведення економіки на "воєнні рейки" росія опинилася у стані глибокої структурної перебудови. Офіційна риторика про "адаптацію" та "імпортозаміщення" істотно контрастує з емпіричними індикаторами деградації окремих секторів, зростанням дефіциту бюджету, посиленням інфляційного тиску, зниженням інвестиційної привабливості та зростанням соціальної напруженості.

Дослідження стану економіки рф в умовах війни має не лише прикладне значення для оцінювання спроможностей противника, а й забезпечує глибше розуміння ефектів санкцій, ізоляції, мілітаризації та переформатування глобальної геоекономічної архітектури. Аналіз економіки рф також має важливе прогностичне значення для формування політик стримування, економічного тиску та підтримання міжнародної коаліції.

Теоретичні основи дослідження

Теоретичну основу дослідження становить міждисциплінарний синтез економічної теорії, політичної економії, підходів безпекових студій і воєнно-стратегічної аналітики. Такий підхід дає змогу комплексно оцінити стійкість, гнучкість і вразливості економіки російської федерації в умовах агресії та глобальної ізоляції. Аналітичний каркас спирається на такі теоретичні платформи:

- **Теорія воєнної економіки** — розглядає функціонування економіки держави в умовах збройного конфлікту, коли пріоритетом стає забезпечення військових потреб шляхом часткової або повної мобілізації ресурсів.
- **Геоекономічний підхід до оцінювання національної потуги** — акцентує увагу на ресурсній базі держави (енергоносії, корисні копалини, виробничий капітал), спроможності підтримувати та масштабувати військово-промисловий потенціал, а також на залежностях у міжнародній торгівлі та ланцюгах постачання.
- **Теорія економічного управління** — фіксує зміщення авторитарних економік (зокрема Росії) від ринкових механізмів до централізованого, державоцентричного регулювання.
- **Теорія військово-економічного циклу** — досліджує вплив військових витрат і конфліктів на економічні цикли (інфляція, безробіття, ВВП та інші макропоказники), пояснюючи коротко- й довгострокові наслідки воєнних дій.
- **Теорія військових витрат** — аналізує вплив оборонних видатків на економічний розвиток, розподіл ресурсів і фінансову політику; охоплює як прямі ефекти (військові закупівлі, дослідження та розробки), так і непрямі (зміни в податковій політиці, соціальних трансферах тощо).
- **Аналіз структурних змін** — з'ясовує, як масштабні шоки (зокрема війни) зумовлюють трансформації галузевої структури, регіонального розвитку, технологічних інновацій і ринку праці; цей підхід показує механізми адаптації економіки до нових викликів.
- **Теорія санкцій та економічних обмежень** — вивчає економічні, політичні та соціальні наслідки міжнародних санкцій як для країн-цілей, так і для ініціаторів; оцінює ефективність санкцій як інструменту міжнародної політики та їхній вплив на економічні відносини.

Постановка проблеми

Повномасштабне вторгнення російської федерації в Україну, розпочате 24 лютого 2022 року, стало не лише найбільшим збройним конфліктом у Європі від часів Другої світової війни, а й зумовило масштабні трансформації в економіці держави-агресора. В умовах безпрецедентного санкційного тиску, згортання зовнішньоекономічних зв'язків із Заходом та переведення економіки на “воєнні рейки” Росія опинилася у стані глибокої структурної перебудови. Офіційна риторика про “адаптацію” та “імпортозаміщення” істотно контрастує з емпіричними індикаторами деградації окремих секторів, зростанням дефіциту бюджету, посиленням інфляційного тиску, зниженням інвестиційної привабливості та наростанням соціальної напруженості.

Це формує складну аналітичну ситуацію: з одного боку — спостерігаються структурна деградація низки галузей, погіршення добробуту населення та дефіцит високотехнологічного імпорту; з іншого — офіційна статистика фіксує формальне зростання ВВП, передусім завдяки оборонному замовленню та експорту сировини. У зв'язку з цим постає завдання об'єктивної оцінки реального стану російської економіки, її спроможності до тривалого ведення війни та вразливостей, що постають унаслідок гіперцентралізації, санкційних обмежень і соціальних дисбалансів.

Ключова методологічна проблема полягає в тому, що за умов авторитарної економіки й обмеженого доступу до достовірних даних традиційні макроекономічні індикатори можуть спотворювати уявлення про реальні процеси. Крім того, міжнародні оцінки (МВФ, Світового банку, ОЕСР) часто спираються на офіційну російську статистику, що знижує їхню аналітичну точність. Додатковим викликом є комплексне врахування впливу військових видатків, “тінізації” економіки, схем обходу санкцій, міграції робочої сили та змін у структурі зайнятості. Отже, для об'єктивної оцінки стану економіки рф у період війни необхідно:

- критично аналізувати офіційні статистичні дані;
- урахувувати специфіку “воєнної економіки” в умовах авторитарного режиму;
- застосовувати альтернативні джерела (аналітичні звіти, open-source дані, розвіддані, супутникові знімки, моніторинг поставок);
- оцінювати не лише рівень, а й структуру економічної активності та її стійкість до екзогенних шоків.

Метою статті є системний аналіз трансформацій, що відбулися в економіці російської федерації у 2022–2025 роках унаслідок розв'язаної нею повномасштабної війни проти України.

Методологія дослідження

Для досягнення мети здійснено декомпозицію завдань і застосовано такі методи наукового пізнання:

- **емпіричний аналіз** — опрацювання офіційної статистики, звітів урядових і міжнародних організацій, фінансової звітності;
- **статистичний аналіз** — використання кореляційного та регресійного аналізу, а також методів аналізу часових рядів;
- **якісний аналіз** — інтерпретація текстових матеріалів (офіційні документи, пресрелізи, публікації ЗМІ) для виявлення тенденцій, тематичних кластерів і патернів;
- **метод кейс-стаді (case study)** — детальний розгляд релевантних випадків/подій, значущих для предмета дослідження;
- **експертний контент-аналіз** — аналіз матеріалів антивоєнних російських видань та моніторинг публічних заяв російських урядовців;
- **теоретичний аналіз** — систематизація наукових праць і теоретичних підходів із метою окреслення концептуальної бази та ідентифікації прогалин у знаннях;

- **системний аналіз** — виявлення взаємозв'язків між компонентами економічної системи та оцінювання впливу зовнішніх і внутрішніх чинників;
- **сценарний аналіз** — розроблення та оцінювання альтернативних сценаріїв розвитку подій з урахуванням поточних трендів і можливих змін у зовнішньому та внутрішньому середовищі.

Результати

Починаючи з 2022 року національна економіка російської федерації зазнала радикальної трансформації. Фундаментальні зміни в організації господарської діяльності були зумовлені збройною агресією проти України та невдалою реалізацією планів її швидкого захоплення. Уже в березні 2022 року воєнно-політичне керівництво рф усвідомило, що окупація України або принаймні значної частини її території є нереалістичною у короткостроковій перспективі, а реакція колективного Заходу виявилася більш згуртованою, ніж очікувалося. Це сформувало нову конфігурацію зовнішніх і внутрішніх чинників впливу на економіку рф і посилило стратегічну невизначеність для ухвалення рішень. Від 2022 року й дотепер економіка РФ функціонує в умовах дії взаємопов'язаних шоків та обмежень, що істотно змінюють її структуру, пріоритети та стійкість (табл. 1).

Таблиця 1 – Основні фактори впливу на економіку російської федерації у воєнний період

Сфера	Фактори
Геополітичні та безпекові фактори	1) Ведення тривалої війни проти України, що потребує мобілізації значних людських і матеріальних ресурсів. 2) Загроза ескалації та нестабільності в прикордонних регіонах, що стримує інвесторів. 3) Втрата доступу до стратегічних ринків країн G7 і ЄС.
Санкційний тиск і міжнародна ізоляція	1) Багаторівневі санкції (енергетичні, фінансові, технологічні, логістичні, індивідуальні), запроваджені США, ЄС, Японією, Великою Британією, Канадою. 2) Відключення значної частини банків від SWIFT та обмеження на операції з резервами Центробанку рф. 3) Заборона імпорту високотехнологічної продукції (мікроелектроніка, станки, авіадеталі). 4) Ембарго на морське транспортування російської нафти, "price cap" механізми.
Мілітаризація та деформація бюджету	1) Різке зростання оборонних витрат — у 2024–2025 рр. понад 6% ВВП. 2) Переорієнтація виробництва на потреби ВПК — збільшення держзамовлення, але зниження продуктивності в цивільному секторі. 3) Дефіцит бюджету і залучення внутрішніх позик — облігації внутрішнього займу, емісія, приховане фінансування.
Капітал, інвестиції і людські ресурси	1) Масовий вихід західних компаній і згорання інвестиційних проєктів. 2) Відтік висококваліфікованої робочої сили після мобілізаційних хвиль (2022 та 2023 роках). 3) Зменшення приватних інвестицій через невизначеність, контроль, ризики націоналізації.
Зовнішньоторговельна переорієнтація	1) Зміщення торгівлі в бік Китаю, Індії, ОАЕ, Туреччини, але з менш сприятливими умовами (знижки на нафту, payment delays). 2) Зростання ролі паралельного імпорту, тіньових схем постачання. 3) Збільшення залежності від Китаю як ключового постачальника

	технологій і обладнання.
Адміністративно-командні обмеження	1) Примусове регулювання валютних операцій, курсів, виведення дивідендів. 2) Встановлення квот, заборон на експорт/імпорт, розширення державного контролю. 3) Повернення до централізованого планування в критичних секторах (ВПК, логістика, транспорт).
Соціальні наслідки та внутрішня політика	1) Зростання інфляції та зниження реальних доходів, особливо серед незахищених верств населення. 2) Соціальна напруга, викликана мобілізацією, репресіями, втратою роботи. 3) Застосування жорсткого контролю за ЗМІ, цензура, переслідування бізнесу.
Макроекономічна нестабільність	1) Коливання курсу рубля, нестабільна грошово-кредитна політика. 2) Дефіцит ключових товарів і комплектуючих, імпортозалежність критичних секторів. 3) Проблеми з обслуговуванням держборгу, перехід до розрахунків у "дружніх валютах".

Для того щоб зрозуміти динаміку розвитку національної економіки рф та впливу на неї наведених вище факторів, потрібно здійснити аналіз макроекономічних показників рф на період з 2021 по 2025 роки.

У 2021 році росія зафіксувала високі темпи зростання (+5,9 %) після пандемічного спаду, що було зумовлено високими цінами на нафту, експортною активністю та низькою базою порівняння.

У 2022 році, після початку повномасштабного вторгнення в Україну, російська економіка скоротилася на 1,2 %. Хоча очікувалося глибше падіння (до –8 % за оцінками Єврокомісії), уряд РФ вдався до заходів стабілізації: валютного контролю, держпідтримки експортерів і нарощування оборонного замовлення.

У 2023 році реальний ВВП несподівано зріс на 3,6 %. Основним драйвером виступили масштабні державні закупівлі у військово-промисловому комплексі, а також сприятливі умови торгівлі з Китаєм та Індією. Однак це зростання було дисбалансованим — цивільні галузі економіки продовжували скорочення.

У 2024 році зростання економіки склало 4,1 %, знову переважно через мілітаризацію бюджету. Водночас уже в 2025 році зростання очікується на рівні +1,5 % — на тлі виснаження ресурсів, інвестиційної слабкості та перенавантаження фіскальної системи.

Таким чином, ВВП рф демонструє феномен "воєнного зростання", коли державні витрати (насамперед на оборону) тимчасово стимулюють економіку, але не створюють основи для довгострокового розвитку. Зростання відбувається на фоні технологічної деградації, скорочення споживчого попиту та втрати людського капіталу (рис. 1) [1-6].

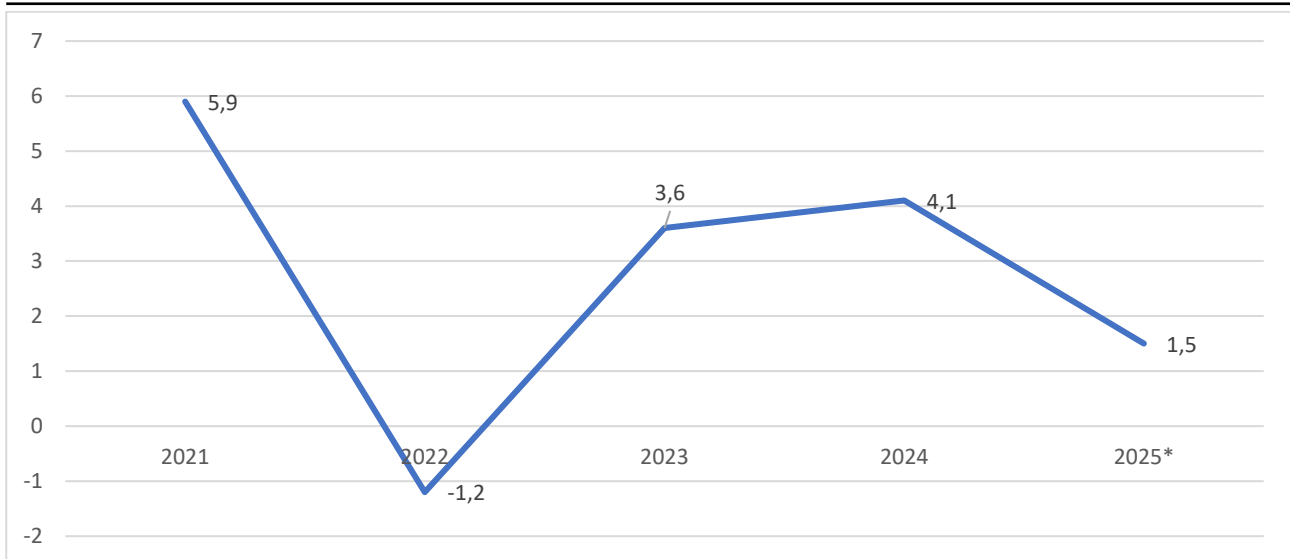


Рисунок 1 – Динаміка росту національної економіки рф 2021-2025 рр. (*прогноз).

За результатами макроекономічного моніторингу CEIC Data [7], у першій половині 2025 року в Росії спостерігається нерівномірний розвиток секторів, при цьому частина з них зазнає системного падіння (табл. 2).

Таблиця 2 – Галузі економіки рф, що скорочуються у 2025 році

Галузь економіки	Тенденції в галузі
1. Виробництво автомобілів та автокомпонентів	Обсяги випуску легкових автомобілів у січні–червні 2025 року знизились на понад 23 % у річному вимірі. Причинами стали санкції на імпорт компонентів, відсутність західних партнерів (Renault, VW, Nissan), обмежений доступ до мікроелектроніки. Вітчизняні заводи (наприклад, «АвтоВАЗ») працюють із зниженим завантаженням. Завезення готових автомобілів з Китаю.
2. Хімічна промисловість	CEIC вказує на -7,4 % скорочення обсягів виробництва в хімічному секторі. До таких наслідків призвела втрата європейських ринків, технологічна деградація, дефіцит каталітичних і синтетичних компонентів.
3. Виробництво побутової техніки та електроніки	Впали обсяги на понад 15 % на квітень–травень 2025 року. Відсутність іноземних брендів і компонентів (наприклад, чипів і процесорів), складнощі з логістикою паралельного імпорту.
4. Сфера послуг (особливо фінансові послуги та IT)	Зниження обсягу наданих послуг на 6–8 %, зокрема в банківській справі, страхуванні та корпоративному IT. Причиною стала втеча капіталу, вихід іноземних банків, часткове згортання бізнесу великих технологічних компаній (SAP, Oracle, IBM).
5. Будівельна галузь (окремі сегменти)	Незважаючи на активність у військовому та дорожньому будівництві, житлове будівництво демонструє падіння до -5 %, зменшення іпотечного кредитування та зростання вартості матеріалів. Що говорить про системі збоїв в економіці рф адже саме будівельна галузь є основним драйвером її економіки.

Економіка рф у 2025 році демонструє зростання переважно в секторах, пов'язаних з обороною, видобутком і транспортуванням енергоресурсів. Натомість цивільні високотехнологічні галузі, виробництво споживчих товарів і сектор послуг деградують під впливом санкцій, дефіциту імпорту, відтоку фахівців та зниження купівельної спроможності населення.

Одним із ключових макроекономічних індикаторів “економічного здоров’я” країни є річна інфляція. Високі інфляційні показники свідчать про проблеми в економіці та недоліки фінансово-грошової політики. Починаючи з 2022 року в рф фіксуються підвищені темпи зростання цін. У 2022 році інфляція сягнула 13,8 % на тлі шоків, спричинених початком війни, та зростання цін на продовольство й енергоносії. У 2023 році її рівень знизився до 5,9 % завдяки жорсткій процентній політиці Центрального банку рф, валютному контролю та стабілізації імпортованих цін [8].

На початку 2024 року зафіксовано новий інфляційний сплеск (9,5 %), зумовлений розширенням бюджетних витрат на війну та девальвацією рубля; у відповідь Центральний банк утримував ключову ставку на рівні 21 %. У 2025 році річний показник за червень становить 9,4 %, що дещо менше, ніж у травні (9,9 %), однак істотно перевищує цільовий орієнтир регулятора (4 %) (рис. 2) [9].

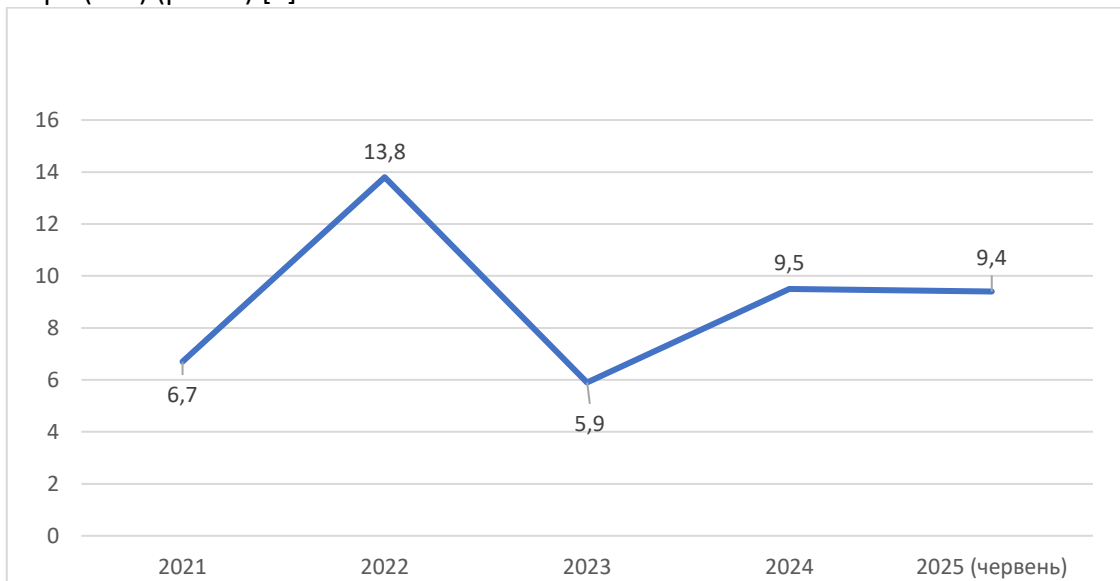


Рисунок 2 – Динаміка індексу споживчих цін рф у відсотках

Слід зазначити, що річний показник інфляції на рівні близько 10 % не є критичним для економіки й зазвичай не потребує суттєвого підвищення облікової ставки — наприклад, до 21 % річних, як у випадку рф. Підвищена увага Центрального банку рф до інфляційних коливань і висока ключова ставка можуть свідчити, що фактичні темпи інфляції дещо вищі, ніж ті, які наводить федеральна служба статистики.

Бюджет рф є надзвичайно чутливим до курсу USD/RUB. Державні доходи від експорту вуглеводнів, сформовані у доларах США, конвертуються в рублі. За умов девальвації рубля рублеві надходження зростають, створюючи ілюзію “стабільності”; за зміцнення рубля, навпаки, виникає дефіцит. У бюджеті рф на 2025 рік закладено курс 94 RUB/USD, тоді як фактичний курс у липні становив близько 78 RUB/USD. Це означає зменшення доходів у рублевому еквіваленті приблизно на 16–20 %, що призводить до скорочення субсидій, нарощування запозичень і відкладання неперіоритетних витратів (інфраструктура, регіони, ЖКГ) [10].

Девальвація рубля у 2022–2023 роках посилила імпортовану інфляцію (понад 40 % комплектувальних виробів є імпортними). У 2025 році зміцнення рубля теоретично знижує інфляційний тиск, однак цей ефект нівелюється бюджетними вливаннями, монетарною емісією та високими воєнними видатками; імпорт залишається обмеженим.

Для експортерів вигідніший слабкий рубль, оскільки доларові доходи конвертуються у більший обсяг рублів. Сильніший рубль у 2025 році (наприклад, 78 RUB/USD проти 94, закладених у бюджеті) знижує рентабельність експорту, спонукаючи компанії вимагати субсидій, скорочувати інвестиції та активніше оптимізувати податкове планування.

Важливим індикатором є й обсяг дефіциту державного бюджету РФ. Якщо у 2021 році спостерігався профіцит на рівні 0,4 % ВВП, то з 2022 року розпочався стрімкий перехід до дефіцитності. Уже у 2022–2023 роках зафіксовано значний дефіцит бюджету (2,3 % та 1,9 % ВВП відповідно), зумовлений зменшенням доходів від енергоносіїв і різким зростанням видатків на оборонно-промисловий комплекс. У 2024 році дефіцит становив 3,5 трлн руб., або 1,7 % ВВП [11]. За перші п'ять місяців 2025 року дефіцит досяг 1,5 % ВВП (3,4 трлн руб.) внаслідок випереджального зростання видатків (+20,7 %) порівняно зі зростанням доходів (+3,1 %) [12–14]. У першому півріччі 2025 року дефіцит зріс до 1,7 % ВВП (3,69 трлн руб.), попри плани утримати його на рівні 0,5 % ВВП, що посилює фінансовий тиск і змусило уряд активніше використовувати резервні фонди (рис. 3).

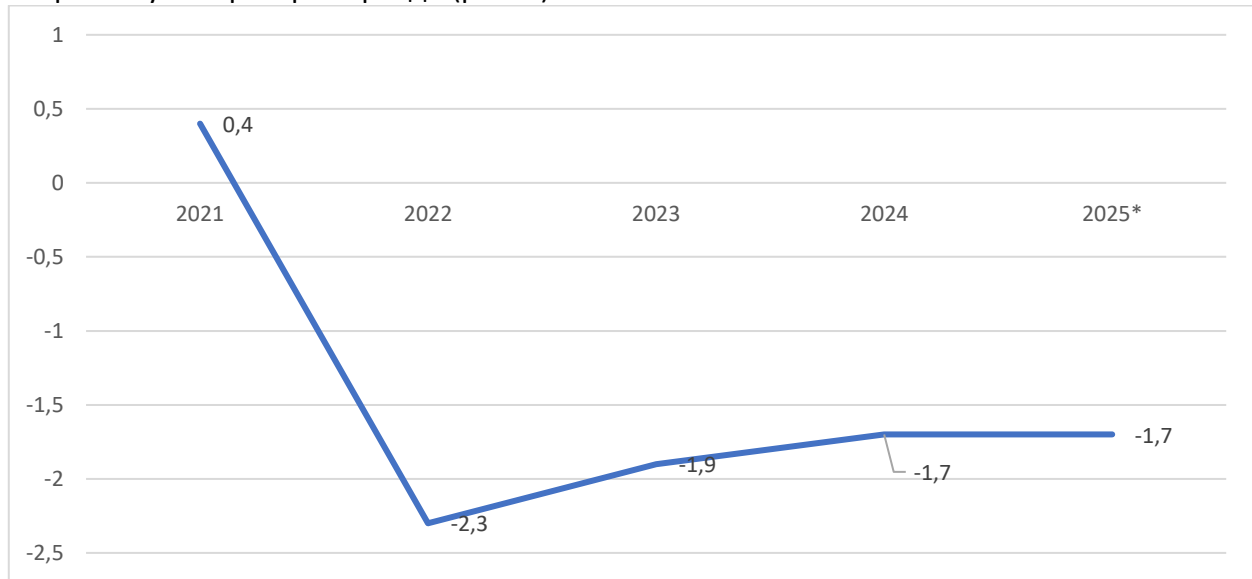


Рисунок 3 – Динаміка дефіциту державного бюджету РФ 2021-2025 рр.
(*2025 рік за два квартали)

Дефіцит державного бюджету чітко детермінується військовими видатками, що зумовило перехід від профіциту до хронічного дефіциту. У 2025 році його розширення прискорилося на тлі падіння нафтових доходів (на 11 % нижче плану) та сталого рівня оборонних видатків (6,3 % ВВП). Темпи зростання видатків випереджають темпи зростання доходів (≈ 20 % проти ≈ 3 %), що змушує покривати дефіцит за рахунок використання резервів та внутрішніх запозичень. Це формує суттєві ризики для фіскальної стабільності, посилює інфляційний тиск, сприяє наростанню державного боргу та загрожує скороченням соціальних програм [15–17].

Динаміка зайнятості та середньої заробітної плати в РФ також набуває екстремальних значень, що зумовлено агресією проти України. У 2021 році офіційний рівень безробіття становив 4,9 %; у 2022–2023 роках — 3,6 % та 3 % відповідно, що є історичними мінімумами. У 2024 році безробіття зменшилося до 2,5 %, а у 2025 році подібна тенденція збереглася: за підсумками першого півріччя показник становив 2,2 % (рис. 4) [18–19].

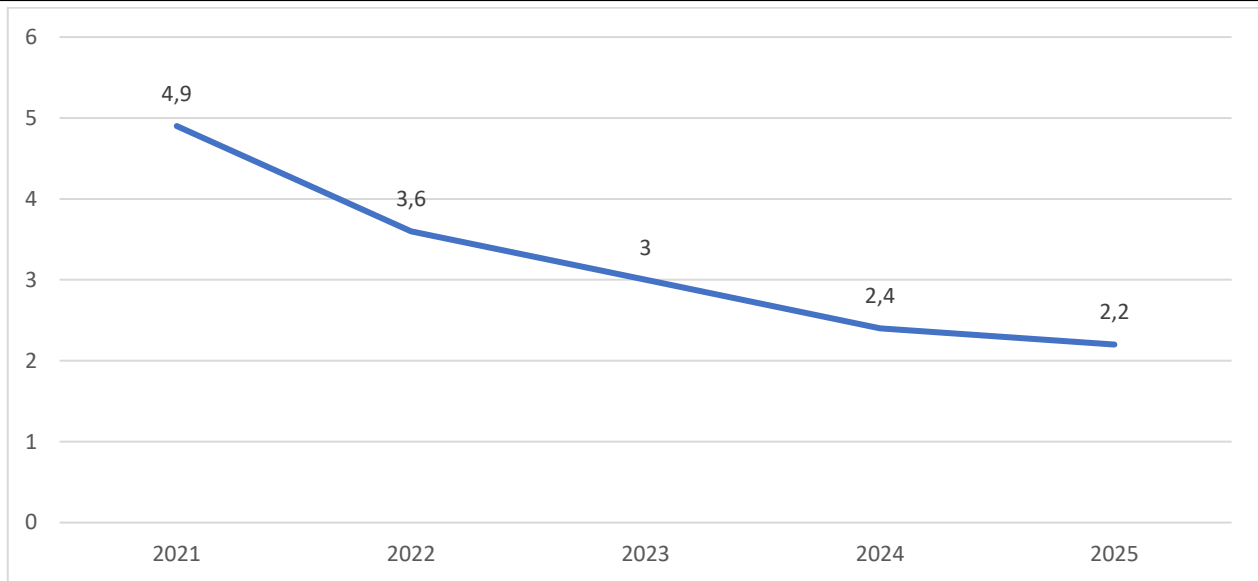


Рисунок 4 – Динаміка зайнятості в рф з 2021 року до червня 2025 року

Високі показники зайнятості спричинили зростання заробітних плат: зокрема, середня заробітна плата у 2020–2021 роках становила 50–55 тис. руб. на місяць; у 2024 році — 86,6 тис. руб.; станом на березень 2025 року — 97,6 тис. руб. на місяць (рис. 5) [20–21].

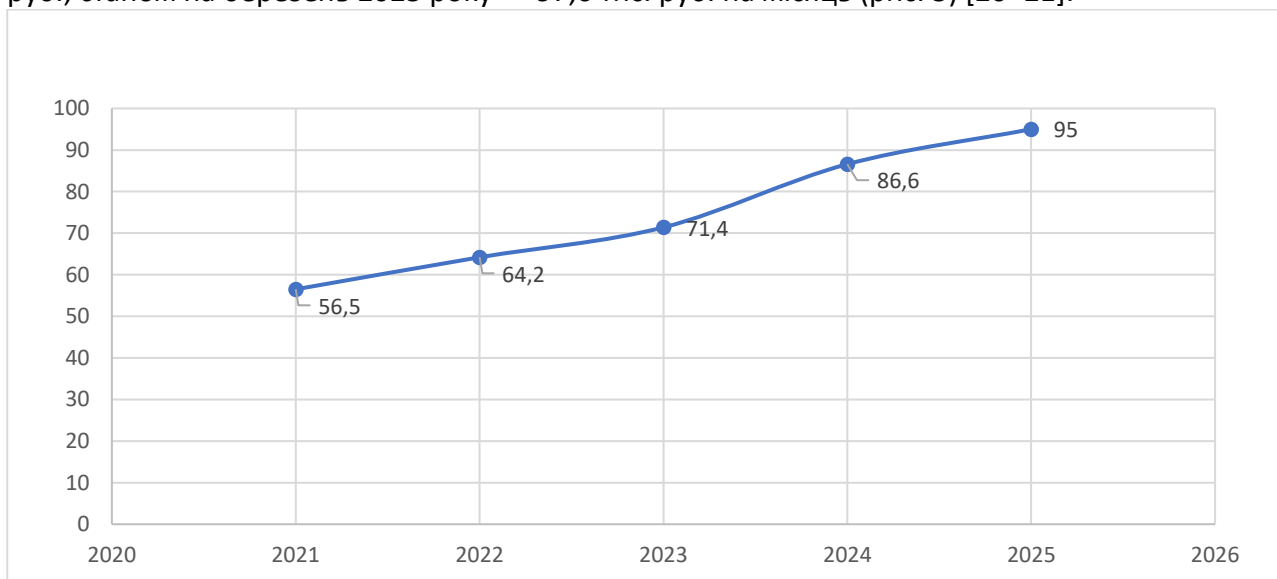


Рисунок 5 – Динаміка зростання середньої заробітної плати в рф з 2021 року до березня 2025 року

Мобілізація, еміграція та перетікання робочої сили до оборонно-промислового комплексу (ОПК) спричинили хронічний дефіцит кадрів у цивільних галузях — будівництві, торгівлі, аграрному секторі, освіті та охороні здоров'я. Підприємства не можуть укомплектувати штати навіть за підвищених зарплат. Конкуренція за працівників стимулює адміністративне зростання оплати праці, яке не супроводжується підвищенням продуктивності, що посилює інфляційний тиск і знижує рентабельність бізнесу.

Висока зайнятість у воєнному секторі деформує ринок праці: спостерігається надмірна концентрація зайнятих в ОПК і державному секторі за одночасного дефіциту кадрів у приватному. Це зумовлює структурні дисбаланси. Держава фактично “утримує” мільйони працівників у

малоефективних виробництвах (особливо в сегменті держзамовлень), що створює ризики прихованого безробіття або формальної зайнятості. Висококваліфіковані фахівці переходять до армії та ОПК або емігрують, послаблюючи технологічний і науковий потенціал.

Експорт товарів рф до інших країн у 2021–2025 роках загалом залишався відносно стабільним. Після пандемічного спаду російський експорт зріс до 548,8 млрд дол. США у 2021 році. У 2022 році, попри початок вторгнення та санкції, експорт і сировинні ціни збільшилися, досягнувши 635,1 млрд дол. США. Через скорочення доходів від газу та втрату ринків ЄС у 2023 році експортні надходження зменшилися на 26,5 % — до 466,8 млрд дол. США. У 2024 році експорт становив близько 417,2 млрд дол. США, а за перше півріччя 2025 року місячні експортні надходження оцінюються приблизно у 40 млрд дол. США; поточні тенденції свідчать, що річний показник може становити 450–470 млрд дол. США [22–23].

У 2024 році експорт нафти та нафтопродуктів приніс рф близько 192 млрд дол. США; металів і матеріалів — 60 млрд дол. США; продукції сільського господарства — 42 млрд дол. США; машин і обладнання — близько 23 млрд дол. США (падіння приблизно на 43 % порівняно з попереднім роком). Високотехнологічні галузі рф фактично витісняються з глобальних ринків; країна втрачає технологічний паритет у машинобудуванні, приладобудуванні та ІТ-індустрії. Спостерігається зростання залежності від Китаю, який виступає ключовим партнером у форматі “постачальник технологій — покупець сировини”. Наявні тенденції є ознаками системної деградації: економіка рф стає дедалі більш ресурсною й дедалі менш інноваційною, із переважно агросировинною моделлю експорту [24].

З 2021 року фіксується зростання експорту аграрної продукції. У 2021 році він становив близько 30 млрд дол. США, у 2022 році зріс до 40 млрд дол. США внаслідок зміни структури експорту, у 2023–2024 роках — 43,5 та 42,6 млрд дол. США відповідно [25–28]. За оцінками українських аналітиків, із тимчасово окупованих регіонів (Крим, Херсонщина, Запоріжжя, Луганщина, Донеччина) у 2023 році РФ вивезла приблизно 6,4 млн тонн пшениці на суму близько 800 млн дол. США. Загалом від початку війни додатково було вивезено 10–15 млн тонн зерна (пшениця, кукурудза, соняшник) — до 7 млрд дол. США доходу [29–30]. Отримані від незаконного експорту зернові доходи становлять вагомую частку фінансового підживлення російської економіки та війни.

Ключові тенденції розвитку економіки рф:

1. Структурна трансформація:

мілітаризація економіки; оборонні видатки перевищили 6 % ВВП у 2024–2025 роках; деградація цивільних галузей (передусім машинобудування, ІТ, хімії, будівництва); зміна структури експорту — домінування сировини (нафта, зерно) й агропродукції замість машин і технологій.

2. Макроекономічна напруга:

ВВП: спад у 2022 році (–1,2 %), «штучне» зростання у 2023–2024 роках за рахунок оборонних закупівель (+3,6 % і +4,1 %), у 2025 році — прогнозовано +1,5 %;

інфляція: від піку 13,8 % у 2022 році до 9,4 % у червні 2025 року;

дефіцит бюджету: 1,7 % ВВП у 2024 році; 1,5 % ВВП за 5 місяців 2025 року — близько граничних значень;

валютний курс: у бюджеті на 2025 рік закладено 94 RUB/USD, фактичний — близько 78 RUB/USD, що скорочує рублеві доходи від експорту;

ключова ставка ЦБ РФ (21 %) — індикатор дефіциту довіри до офіційних інфляційних даних.

3. Зайнятість і заробітна плата:

безробіття у 2025 році рекордно низьке (2,2 %), що зумовлено еміграцією, мобілізацією та перетіканням кадрів, а не розвитком ринку праці;

зарплати зростають: від 55 тис. руб. (2021) до 97,6 тис. руб. (березень 2025);

гострий дефіцит кадрів у цивільному секторі, зокрема в освіті, медицині, аграрній сфері.

4. Зовнішня торгівля:

експорт стабілізувався на рівні 450–470 млрд дол. США, зростає частка аграрної продукції;

високотехнологічний експорт (машини, електроніка) скоротився на 43 % (до ≈23 млрд дол. США);

аграрний експорт у 2024 році — 42,6 млрд дол. США; суттєва частка припадає на продукцію з окупованих територій України (понад 6 млн тонн зерна).

5. Нарощування дефіциту бюджету:

у 2025 році на кожні +1 % доходів припадає +6–7 % видатків; оборонні видатки перевищують 30 % зведеного бюджету;

закладений курс 94 RUB/USD проти фактичного ≈78 RUB/USD зменшує рублеві експортні доходи на 15–20 %;

дефіцит фінансується внутрішніми позиками (ОВДП/облігації), використанням ФНБ і квазімонетарними каналами через держбанки.

Війна та міжнародний економічний тиск уже чинять негативний вплив на економіку РФ, хоча наразі він недостатній для припинення агресивної політики. Це зумовлює потребу подальшого посилення економічного тиску за такими напрямками:

- запровадження вторинних санкцій проти “обхідних” юрисдикцій; адресні санкції щодо компаній у Китаї, Індії, ОАЕ, Туреччині, які постачають РФ критичні компоненти (електроніка, двигуни, прилади);
- конфіскація активів ЦБ РФ і використання заморожених ≈300 млрд дол. США на підтримку України;
- розширення механізму *price cap* на нафту, контроль за “тіньовим флотом”, цифрове маркування танкерів, унеможливлення обходу лімітів;
- санкції проти компаній, залучених до аграрного та іншого експорту з окупованих територій; публікація «чорних списків» покупців сировини й товарів із Криму, Херсонщини, Луганщини тощо;
- розрив технологічних ланцюгів: заборона експорту ЧПУ-верстатів, лазерних технологій, чипів ≥5 нм, у т. ч. через треті країни;
- тарифна стратегія ЄС/США: запровадження ставок 100 % (за окремими позиціями — до 500 %) на товари з країн, що купують сировину або товари походженням із РФ, а також підвищення мит на залишковий російський імпорт (алюміній, хімія, добрива).

Висновки

Проведене дослідження засвідчує, що економіка російської федерації перебуває у стані глибокої структурної трансформації, зумовленої повномасштабною війною проти України, міжнародними санкціями та внутрішньою політикою мілітаризації. Аналіз ключових макроекономічних індикаторів, галузевих тенденцій, бюджетної динаміки та зовнішньоторговельної структури дає підстави для таких узагальнень:

1. Джерела зростання. Економічне зростання у 2023–2024 роках мало переважно штучний характер і забезпечувалося насамперед розширенням державних оборонних видатків, а не збільшенням виробництва чи інвестицій у високотехнологічні сектори.

2. Структурні зрушення. Посилюється сировинна залежність (нафта, газ, зернові); аграрний сектор розширюється, зокрема за рахунок експлуатації тимчасово окупованих територій України, тоді як машинобудування, електроніка, ІТ та цивільне промислове виробництво демонструють стійке скорочення.

3. Фіскальні ризики. Хронічний дефіцит бюджету став індикатором економічного

виснаження: видатки зростають істотно швидше за доходи, насамперед через фінансування війни, що формує системні ризики фінансової нестабільності у 2025–2027 роках.

4. Ринок праці та демографія. Дефіцит робочої сили поглиблює структурні деформації. Рекордно низький рівень безробіття зумовлений еміграцією, мобілізацією та перетіканням кадрів до оборонно-промислового комплексу, а не зростанням продуктивної зайнятості.

5. Зовнішні резерви та торгівля. Міжнародні резерви РФ поступово скорочуються; залежність від “тіньового” експорту, обходу санкцій та торгівлі з авторитарними режимами (Іран, КНДР, Китай) підвищує довгострокові ризики ізоляції та технологічного відставання.

6. Політика стабілізації. Економічна політика РФ орієнтована на підтримання короткострокової стабільності ціною погіршення довгострокових перспектив розвитку. Без структурних реформ, мирного врегулювання та відновлення доступу до глобальних ринків економіка рухатиметься до стагнації й розбалансування.

7. Ефект санкцій. Результативність міжнародних санкцій і експортного контролю проявляється не лише у прямому звуженні доходної бази, а й у поступовому виснаженні фінансово-економічної спроможності РФ вести затяжну війну.

Таким чином, економіка РФ входить у фазу уповільнення: збереження видимості макроекономічної стабільності досягається ціною глибоких внутрішніх деформацій, зниження інвестиційної привабливості та зростання соціальної напруженості. Подальше посилення тиску на фінансову, логістичну та технологічну інфраструктуру РФ є необхідною умовою зниження її спроможності фінансувати війну проти України.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Trading Economics. Russia GDP Annual Growth Rate. URL: <https://tradingeconomics.com/russia/gdp> (Дата звернення: 16.07.2025).
2. International Monetary Fund. World Economic Outlook Database, April 2024. URL: <https://www.imf.org/en/Publications/WEO/weo-database/2024/April> (Дата звернення: 16.07.2025).
3. Reuters. Putin's economic resilience rests on war addiction / by Pierre Briançon // Reuters Breakingviews. – 2024. – Oct. 15. URL: <https://www.reuters.com/breakingviews/putins-economic-resilience-rests-war-addiction-2024-10-15/> (Дата звернення: 16.07.2025).
4. FocusEconomics. Russia: GDP growth slows in early 2024. URL: <https://www.focus-economics.com/countries/russia> (Дата звернення: 16.07.2025).
5. Bruegel. The Russian war economy: macroeconomic performance / by Maria Demertzis, Nicolas Poitiers. – 2024. URL: <https://www.bruegel.org/analysis/russian-war-economy-macroeconomic-performance> (Дата звернення: 16.07.2025).
6. The Guardian. What have three years of Putin's war done to both nations' economies? – 2025. – Feb. 22. URL: <https://www.theguardian.com/world/2025/feb/22/what-have-three-years-of-putins-war-done-to-both-nations-economies> (Дата звернення: 19.07.2025).
7. CEIC Data. Russia – Economic Indicators by Sector. URL: <https://www.ceicdata.com/en/country/russia> (Дата звернення: 20.07.2025).
8. Trading Economics. Russia GDP Annual Growth Rate. URL: <https://tradingeconomics.com/russia/gdp> (Дата звернення: 22.07.2025).
9. Trading Economics. Russia Inflation Rate – annual CPI. URL:

- <https://tradingeconomics.com/russia/inflation-cpi> (Дата звернення: 25.07.2025).
10. Russian oil price in roubles has stayed below the 2025 budget target. URL: <https://www.reuters.com/business/energy/russian-oil-price-roubles-has-stayed-below-2025-budget-target-2025-07-16/> (Дата звернення: 20.07.2025).
11. Економічна правда. Росія закінчила 2024 рік з рекордним дефіцитом бюджету – росЗМІ. URL: <https://www.epravda.com.ua/finances/dira-v-byudzheti-rf-vstanovila-rekordniy-rozmir-802270/> (Дата звернення: 29.07.2025).
12. Reuters. *Russia's Q1 budget deficit narrows to 1% of GDP* / Apr 8, 2025. URL: <https://www.reuters.com/markets/europe/russias-q1-budget-deficit-narrows-1-gdp-2025-04-08/> (Дата звернення: 30.07.2025).
13. Reuters. *Russian January–April budget deficit widens to 1.5% of GDP* / May 7, 2025. URL: <https://www.reuters.com/markets/europe/russian-january-april-budget-deficit-widens-15-gdp-2025-05-07/> (Дата звернення: 23.07.2025).
14. Reuters. *Russia budget deficit reaches 2025 target level of 1.7% GDP in first half of year* / Jul 7, 2025. URL: <https://www.reuters.com/markets/europe/russia-budget-deficit-reaches-2025-target-level-17-gdp-first-half-year-2025-07-07/> (Дата звернення: 15.07.2025).
15. Osiński, T. *Russia's Budget 2025: War Above All* / Tadeusz Osiński // OSW Commentary. – 2024. – No. 566. – 22 November. URL: <https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-11-22/russias-budget-2025-war-above-all> (Дата звернення: 17.07.2025).
16. CEIC Data. *Russia: Consolidated Fiscal Balance (% of Nominal GDP)*. URL: <https://www.ceicdata.com/en/indicator/russia/consolidated-fiscal-balance--of-nominal-gdp> (Дата звернення: 02.08.2025).
17. FocusEconomics. *Russia: Fiscal Balance (% of GDP)*. URL: <https://www.focus-economics.com/country-indicator/russia/fiscal-balance/> (Дата звернення: 10.08.2025).
18. GlobalData. *The Unemployment Rate of Russia, 2021 г., 2024* URL: https://www.globaldata.com/data-insights/macroeconomic/the-unemployment-rate-of-russia-220152/?utm_source=chatgpt.com (Дата звернення: 09.08.2025).
19. FocusEconomics. *Russia Unemployment Outlook & Estimate, 2024.* – <https://www.focus-economics.com/country-indicator/russia/unemployment/> (Дата звернення: 12.08.2025).
20. Trading Economics. *Russia Unemployment Rate, May 2025.* URL: <https://tradingeconomics.com/russia/wages> (Дата звернення: 14.08.2025).
21. Financial Times. *Russia's surprising consumer spending boom* / FT News, 10.07.2024 . URL: <https://www.ft.com/content/3e2b2e63-082e-4058-ba92-dea580d4f40c> (Дата звернення: 15.08.2025).
22. *Russia Exports 1960–2025.* URL: <https://www.macrotrends.net/global-metrics/countries/rus/russia/exports> (Дата звернення: 03.08.2025).
23. Trading Economics. *Russia Exports.* URL: <https://tradingeconomics.com/russia/exports> (Дата звернення: 12.08.2025).
24. Re:Russia. *Export Without Innovation: The Changing Structure of Russia's Trade Balance* / Re:Russia Analytics, Policy & Ideas for Modernization. – 2024. – 16 February. URL: <https://re-russia.net/en/analytics/0244/> (Дата звернення: 15.08.2025).
25. Tridge. *The Share of Grain in the Export of Agricultural Products in Russia.* URL: <https://www.tridge.com/news/the-share-of-grain-in-the-export-of-agricult-bqykh> (Дата звернення: 10.08.2025).
26. Emerald Insight. *Russia's Grain Exports from Black Sea Ports in 2025* / Oxford Analytica Daily Brief Service. URL: <https://www.emerald.com/insight/content/doi/10.1108/oxan-db291434/full/html> (Дата звернення: 11.08.2025).

27. The Washington Post. Russia Uses Black Sea to Export Food Amid Ukraine War. – 25.03.2025. URL: <https://www.washingtonpost.com/world/2025/03/25/russia-ukraine-black-sea-exports/> (Дата звернення: 05.08.2025).
28. TAdviser. Export of Food and Agricultural Raw Materials from Russia. URL: <https://tadviser.com/index.php/Article:Export of food and agricultural raw materials from Russia> (Дата звернення: 06.08.2025).
29. Radio Free Europe / Radio Liberty. Ukraine Accuses Russia Of Stealing Grain From Occupied Territories And Exporting It As Its Own. URL: <https://www.rferl.org/a/ukraine-russia-war-occupation-grain-shipments/33004062.html> (Дата звернення: 08.08.2025).
30. Rail Insider. З початку повномасштабної війни РФ вивезла 15 млн т зерна з окупованих територій. URL: <https://www.railinsider.com.ua/z-pochatku-povnomasshtabnoyi-vijny-rf-vyvezla-15-mln-t-zerna-z-okupovanyh-terytorij/> (Дата звернення: 01.08.2025).

References

1. Trading Economics. Russia GDP Annual Growth Rate. Available from : <https://tradingeconomics.com/russia/gdp> (Дата звернення: 16.07.2025).
2. International Monetary Fund. World Economic Outlook Database, April 2024. Available from : <https://www.imf.org/en/Publications/WEO/weo-database/2024/April> (Дата звернення: 16.07.2025).
3. Reuters. Putin's economic resilience rests on war addiction / by Pierre Briançon // Reuters Breakingviews. – 2024. – Oct. 15. Available from : <https://www.reuters.com/breakingviews/putins-economic-resilience-rests-war-addiction-2024-10-15/> (Дата звернення: 16.07.2025).
4. FocusEconomics. Russia: GDP growth slows in early 2024. Available from : <https://www.focus-economics.com/countries/russia> (Дата звернення: 16.07.2025).
5. Bruegel. The Russian war economy: macroeconomic performance / by Maria Demertzis, Niclas Poitiers. – 2024. Available from : <https://www.bruegel.org/analysis/russian-war-economy-macroeconomic-performance> (Дата звернення: 16.07.2025).
6. The Guardian. What have three years of Putin's war done to both nations' economies? – 2025. – Feb. 22. Available from : <https://www.theguardian.com/world/2025/feb/22/what-have-three-years-of-putins-war-done-to-both-nations-economies> (Дата звернення: 19.07.2025).
7. CEIC Data. Russia – Economic Indicators by Sector. Available from : <https://www.ceicdata.com/en/country/russia> (Дата звернення: 20.07.2025).
8. Trading Economics. Russia GDP Annual Growth Rate. Available from : <https://tradingeconomics.com/russia/gdp> (Дата звернення: 22.07.2025).
9. Trading Economics. Russia Inflation Rate – annual CPI. Available from : <https://tradingeconomics.com/russia/inflation-cpi> (Дата звернення: 25.07.2025).
10. Reuters. Russian oil price in roubles has stayed below the 2025 budget target. Available from : <https://www.reuters.com/business/energy/russian-oil-price-roubles-has-stayed-below-2025-budget-target-2025-07-16/> (Дата звернення: 20.07.2025).
11. Ekonomichna pravda. Rosiya zakinchyla 2024 rik z rekordnym defitsytom byudzhetu – rosZMI. Available from : <https://www.epravda.com.ua/finances/dira-v-byudzheti-rf-vstanovila-rekordniy-rozmir-802270/> (Дата звернення: 29.07.2025).
12. Reuters. Russia's Q1 budget deficit narrows to 1% of GDP / Apr 8, 2025. Available from : <https://www.reuters.com/markets/europe/russias-q1-budget-deficit-narrows-1-gdp-2025-04-08/> (Дата звернення: 30.07.2025).
13. Reuters. Russian January–April budget deficit widens to 1.5% of GDP / May 7, 2025. Available from : <https://www.reuters.com/markets/europe/russian-january-april-budget-deficit-widens-15-gdp-2025-05-07/> (Дата звернення: 23.07.2025).

14. Reuters. *Russia budget deficit reaches 2025 target level of 1.7% GDP in first half of year* / Jul 7, 2025. Available from : <https://www.reuters.com/markets/europe/russia-budget-deficit-reaches-2025-target-level-17-gdp-first-half-year-2025-07-07/> (Дата звернення: 15.07.2025).
15. Osiński, T. *Russia's Budget 2025: War Above All* / Tadeusz Osiński // OSW Commentary. – 2024. – No. 566. – 22 November. Available from : <https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-11-22/russias-budget-2025-war-above-all> (Дата звернення: 17.07.2025).
16. CEIC Data. *Russia: Consolidated Fiscal Balance (% of Nominal GDP)*. Available from : <https://www.ceicdata.com/en/indicator/russia/consolidated-fiscal-balance--of-nominal-gdp> (Дата звернення: 02.08.2025).
17. FocusEconomics. *Russia: Fiscal Balance (% of GDP)*. Available from : <https://www.focus-economics.com/country-indicator/russia/fiscal-balance/> (Дата звернення: 10.08.2025).
18. GlobalData. *The Unemployment Rate of Russia, 2021 г., 2024*. Available from : https://www.globaldata.com/data-insights/macroeconomic/the-unemployment-rate-of-russia-220152/?utm_source=chatgpt.com (Дата звернення: 09.08.2025).
19. FocusEconomics. *Russia Unemployment Outlook & Estimate, 2024*. Available from : <https://www.focus-economics.com/country-indicator/russia/unemployment/> (Дата звернення: 12.08.2025).
20. Trading Economics. *Russia Unemployment Rate, May 2025*. Available from : <https://tradingeconomics.com/russia/wages> (Дата звернення: 14.08.2025).
21. Financial Times. *Russia's surprising consumer spending boom* / FT News, 10.07.2024. Available from : <https://www.ft.com/content/3e2b2e63-082e-4058-ba92-dea580d4f40c> (Дата звернення: 15.08.2025).
22. *Russia Exports 1960–2025*. Available from : <https://www.macrotrends.net/global-metrics/countries/rus/russia/exports> (Дата звернення: 03.08.2025).
23. Trading Economics. *Russia Exports*. Available from : <https://tradingeconomics.com/russia/exports> (Дата звернення: 12.08.2025).
24. Re:Russia. *Export Without Innovation: The Changing Structure of Russia's Trade Balance* / Re:Russia Analytics, Policy & Ideas for Modernization. – 2024. – 16 February. Available from : <https://re-russia.net/en/analytics/0244/> (Дата звернення: 15.08.2025).
25. Tridge. *The Share of Grain in the Export of Agricultural Products in Russia*. Available from : <https://www.tridge.com/news/the-share-of-grain-in-the-export-of-agricult-bqykh> (Дата звернення: 10.08.2025).
26. Emerald Insight. *Russia's Grain Exports from Black Sea Ports in 2025* / Oxford Analytica Daily Brief Service. Available from : <https://www.emerald.com/insight/content/doi/10.1108/oxan-db291434/full/html> (Дата звернення: 11.08.2025).
27. The Washington Post. *Russia Uses Black Sea to Export Food Amid Ukraine War*. – 25.03.2025. Available from : <https://www.washingtonpost.com/world/2025/03/25/russia-ukraine-black-sea-exports/> (Дата звернення: 05.08.2025).
28. TAdviser. *Export of Food and Agricultural Raw Materials from Russia*. Available from : <https://tadviser.com/index.php/Article:Export of food and agricultural raw materials from Russia> (Дата звернення: 06.08.2025).
29. Radio Free Europe / Radio Liberty. *Ukraine Accuses Russia Of Stealing Grain From Occupied Territories And Exporting It As Its Own*. Available from : <https://www.rferl.org/a/ukraine-russia-war-occupation-grain-shipments/33004062.html> (Дата звернення: 08.08.2025).
30. Rail Insider. *З початку повномасштабної війни РФ вивезла 15 млн т зерна з окупованих територій*. Available from : <https://www.railinsider.com.ua/z-pochatku-povnomasshtabnoyi-vijny-rf-vyvezla-15-mln-t-zerna-z-okupovanyh-terytorij/> (Дата звернення: 01.08.2025).

Expenditures of the Ministry of Defence of Ukraine: Analysis from the Perspective of Transformational Economic Prospects

Видатки Міністерства оборони України: аналіз з точки зору трансформаційних економічних перспектив

Maria Zozulinska

Corresponding author: Cadet in Finance, Banking, Insurance and Stock Market, e-mail: mariazozulinskaa2703@gmail.com, ORCID: 0009-0002-8529-9138

Oleksandr Artiushenko

PhD, Senior Lecturer Department of Financial Support of Military Troops, e-mail: mr.apemi@gmail.com, ORCID: 0000-0002-3638-4961

Марія Зозулінська^A

Corresponding author: Курсант, e-mail: mariazozulinskaa2703@gmail.com, ORCID: 0009-0002-8529-9138

Олександр Артюшенко

доктор філософії, старший викладач кафедри фінансового забезпечення військ, e-mail: mr.apemi@gmail.com, ORCID: 0000-0002-3638-4961

Military Institute of Taras Shevchenko National University of Kyiv, Ukraine

^AВійськовий інститут Київського національного університету імені Тараса Шевченка, Київ, Україна

Received: August 02, 2025 | **Revised:** August 19, 2025 | **Accepted:** August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.19>

Purpose. Investigate the link between military expenditures and economic growth in Ukraine's prewar and wartime economy using econometric tools.

Method. Quantitative time-series econometrics (stationarity tests, Granger causality, VAR, Ridge/OLS).

Findings. No significant statistical or causal relationship between GDP and military spending; coefficients are weak/insignificant. Models are unstable with low predictive power, indicating the defense budget is largely decoupled from short-term macro indicators.

Theoretical implications. Challenges the assumption that wartime defense outlays spur growth; calls for revising models to allow independence and nonlinearities under emergency fiscal conditions.

Value. Applies advanced time-series methods to prewar/war data, offering evidence for budget sustainability, fiscal planning, and institutional reform; finds no predictive links.

Future research. Extend the time span, add cross-country comparisons, and test machine-learning-based forecasting.

Paper type: theoretical-empirical.

Мета дослідження. Дослідити зв'язок між військовими видатками та економічним зростанням України у передвоєнний та воєнний періоди із застосуванням економетричних інструментів.

Метод дослідження. Кількісний економетричний підхід: тестування стаціонарності, причинність Грейнджера, VAR, регресії (Ridge/OLS).

Результати дослідження. Статистично значущої причинно-наслідкової залежності між ВВП і військовими видатками не виявлено; коефіцієнти слабкі або незначущі. Моделі нестабільні з низькою прогностичною спроможністю, що свідчить про відносну незалежність оборонного бюджету від короткострокових макроіндикаторів.

Теоретичне значення. Результати ставлять під сумнів тезу про стимулювальний ефект оборонних витрат на ВВП у війні та вказують на потребу перегляду моделей прямих зв'язків державних видатків і зростання з урахуванням надзвичайних фінансових умов і можливих нелінійностей.

Цінність дослідження. Поєднання VAR, тестів стаціонарності та регресії Ріджа на реальних даних до- й воєнного часу демонструє відсутність статистичної значущості й прогностичних зв'язків, надаючи підстави для рішень щодо стійкості бюджету, фінансового планування та інституційних реформ.

Тип статті: теоретико-емпірична.

Key words: defense budgeting, military expenditures, economic growth, Granger causality, time-series analysis.

Ключові слова: оборонний бюджет, військові видатки, економічне зростання, причинність Грейнджера, аналіз часових рядів.

Introduction

Ensuring effective management of budget expenditures in the defence sector has become especially important under martial law introduced in response to full-scale armed aggression. Financing national security is not only a matter of safeguarding state sovereignty but also an indicator of state institutions' ability to adapt to new challenges, use limited resources rationally, and ensure transparency in defence-sector decision-making. The Ministry of Defence of Ukraine's budget expenditures have undergone significant transformation: the share of current spending has increased, and approaches to procurement, planning, and control have changed. Against this backdrop, there is a growing need for in-depth analysis of the composition, structure, and dynamics of the defence budget, the identification of weaknesses in financial management, and the formulation of strategic priorities focused on strengthening defence capabilities and effective coordination with international assistance.

During the period of armed aggression against Ukraine, interest in financing processes in the defence sector—particularly the Ministry of Defence’s budget expenditures—has grown markedly. This is driven both by the unprecedented rise in the share of defence spending within the state budget and by the need to ensure its efficiency, transparency, and adaptability to the rapidly changing conditions of war.

Certain aspects of defence financing are regulated by the Budget Code of Ukraine, the Law of Ukraine “On the Defence of Ukraine”, and programme documents, including the National Security Strategy of Ukraine and the Programme of Activities of the Cabinet of Ministers of Ukraine.

The scientific discourse on defence budgeting in Ukraine centres on several key areas. Ukraine has implemented capability-based defence planning, threat-oriented and aligned with NATO standards, as outlined in the *Doctrine of Defence Planning in the Armed Forces of Ukraine* (2020), which defines the roles, functions, and tasks of military management bodies in defence planning. Karp (2018) examines structural changes in defence expenditures in Ukraine’s state budget, analysing key parameters and trends, including indicators of defence spending and their calculation in NATO countries. Researchers pay particular attention to limited parliamentary oversight, high data opacity, and weak integration of medium-term budget planning, while emphasising the importance of programme-based budgeting and a procurement system grounded in integrity and audit.

Regarding econometric modelling in wartime, recent studies highlight the specific challenges facing Ukraine’s defence budget, especially transparency, efficiency, and macroeconomic implications. Nate, Stavytskyi, and Kharlamova (2023) introduce a quantitative index to assess openness in defence-sector financial management, revealing significant accountability gaps despite strong public demand for oversight; they argue for digital monitoring systems and standardised disclosure. Petlenko et al. (2025) add comparative context by examining Scandinavian models, underscoring the benefits of real-time budgeting and institutionally inclusive reforms supported by appropriate digital platforms. Similarly, Lyutiy, Petlenko, and Drozd (2022) contend that transparency in budgeting is foundational to a democratic system, especially under martial law, and stress that alignment with EU integration efforts can enhance long-term stability.

Beyond the domestic context, global econometric evidence offers a broader view of the relationship between militarisation and economic growth. Saeed (2025), using panel data for 133 countries and instrumental-variable methods, identifies a negative correlation between military expenditure and economic growth, particularly in low- and middle-income economies; the framework suggests defence outlays can dampen growth when not strategically justified (although Ukraine’s situation is distinct given the existential importance of defence investment). Complementing this, Awaworyi Churchill and Yew (2018) conduct a meta-analysis of 48 studies (272 estimates) and conclude that military spending typically slows growth—more so in developing countries—while revealing nonlinearities and methodological differences that call for context-sensitive modelling.

Taken together, this literature indicates that while the defence budget is a critical safeguard in times of geopolitical tension, its economic implications are complex and often opaque, necessitating sophisticated quantitative tools for proper assessment. These studies underscore the need for econometric research on Ukraine’s military expenditure to identify structural patterns and to inform transparent, evidence-based policy reform.

Theoretical Foundations of Research

The study found that the conditions of martial law required the immediate adaptation of the budget process. Parliament repeatedly amended budget legislation to ease existing restrictions. In particular, the Law of Ukraine No. 2134-IX, “On Amendments to Certain Laws of Ukraine Regarding

Budget Legislation,” temporarily suspended several provisions of the Budget Code (e.g., part 3 of Article 24 on the maximum size of the reserve fund and part 3 of Article 27 on the timing of budget decisions) (On amendments to Section VI..., 2025). This ensured greater flexibility in forming reserves and allowed for prompt reallocation of funds. To balance revenues, the military tax rate was increased (from 1.5% to 5% for most taxpayers) under the Law of Ukraine No. 4015-IX, “On Amendments to Tax Legislation Regarding the Military Tax Rate” (On amendments to the Tax Code..., 2025).

The Ministry of Defence of Ukraine’s budget expenditures underwent significant structural changes during martial law. In particular, the share of operational support—salaries, logistics, and weapons procurement—increased markedly, indicating a prioritisation of short-term needs over long-term investment. Expenditures on the Ministry of Defence in 2024 amounted to UAH 1,149.0 billion, of which UAH 882.8 billion was spent on the Armed Forces and UAH 265.3 billion on weapons and equipment. Compared with 2023 (UAH 1,440 billion), these expenditures fell slightly but remain at record levels.

According to Article 87 of the Budget Code of Ukraine, defence is financed from the State Budget through targeted (programme) classifications. Under Article 13 of the Law of Ukraine No. 4059-IX, “On the State Budget of Ukraine for 2025,” expenditures under the economic classification code 2101150 of the Ministry of Defence of Ukraine are a key element of strategic financing and are directed to the development, procurement, modernisation, and repair of weapons and military equipment (On the State Budget..., 2025).

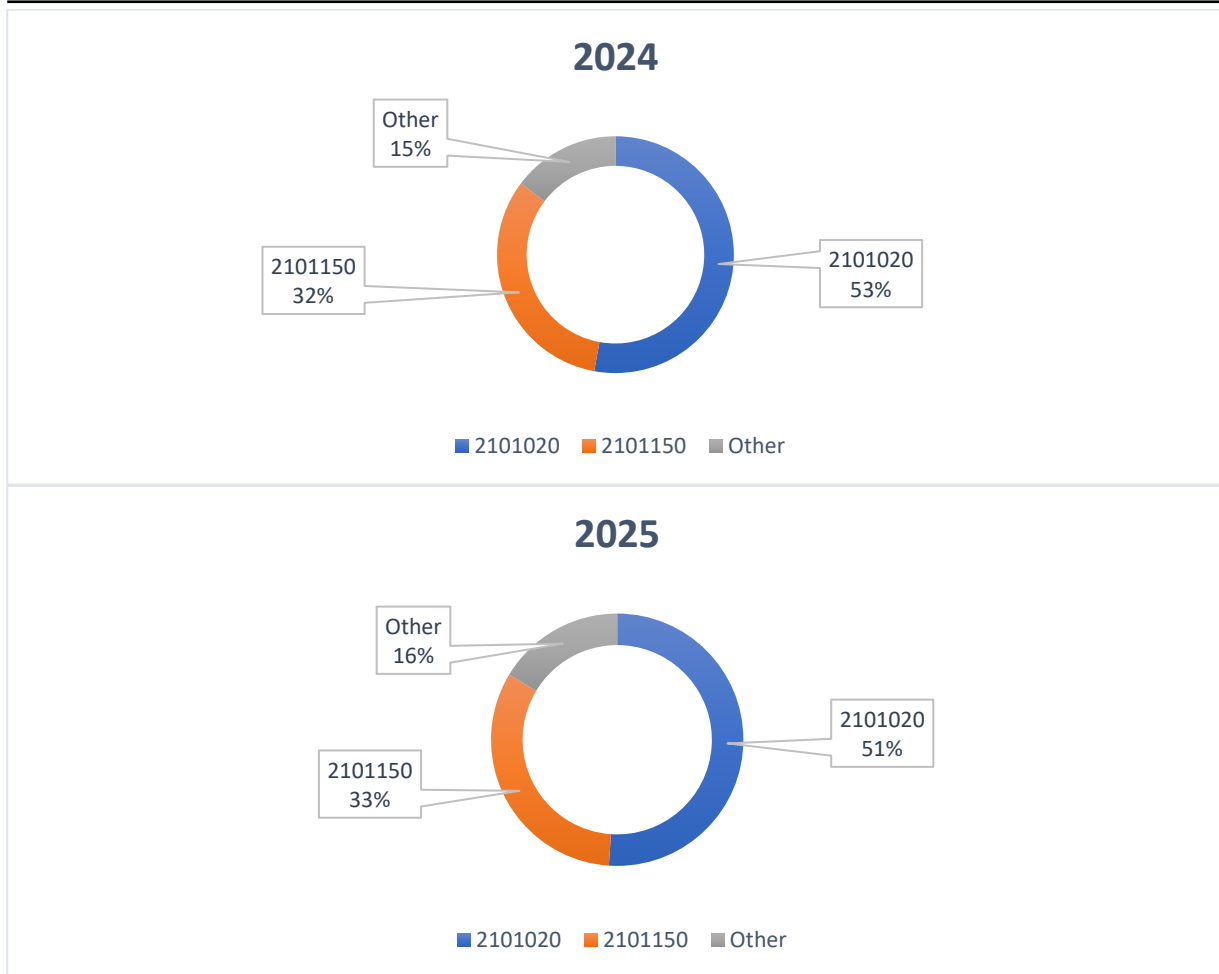
In 2024, spending on the security and defence sector exceeded UAH 2.1 trillion, while UAH 2.22 trillion (26.3% of GDP) is planned in the 2025 State Budget of Ukraine, indicating an unprecedented concentration of resources on defence. However, a key challenge remains insufficient funding for the development of the defence industry. Low budget flexibility and fragmented strategic planning hinder adaptation to the dynamic conditions of war.

At the same time, several positive trends are evident: increased international donor assistance; cooperation with the IMF, the EU, the United States, and other partners; and the gradual introduction of medium-term budget planning. Under international financial assistance agreements, State Budget revenues can help expand funding for strategic defence programmes.

Econometric analysis indicates a direct positive association between improved institutional capacity in public administration, increased volumes of international financial support to the State Budget of Ukraine, and higher levels of strategic defence expenditure under code 2101150 (“Development, procurement, modernisation and repair of weapons and military equipment”).

Accordingly, the hypothesis is supported: improvements in institutional capacity, positive economic growth, and increases in international financial support to the State Budget of Ukraine have a direct positive effect on the volume of strategic defence expenditure, particularly under the Ministry of Defence’s economic classification code 2101150 (“Development, procurement, modernisation and repair of weapons and military equipment”).

On the basis of current legislation and the regulatory framework, it is reasonable to assume that growth in international support, reform of the defence sector, and greater transparency in public administration will contribute to higher strategic defence spending, in line with national interests and the requirements of Ukrainian law.



Picture 1 – Structural comparison of Ukraine’s defense expenditures in 2025-2025 (UAH billion)

Source: systemized by author based on “On the State Budget... (2025)”

The comparative breakdown of the Ministry of Defence of Ukraine’s budget expenditures for 2024 and 2025, as shown in the diagram, indicates a gradual rebalancing between operational needs and strategic programmes. In 2025, allocations under economic classification code 2101150 increase, signalling greater emphasis on technical modernisation and the long-term development of defence capabilities—evidence of the government’s commitment to strategic rearmament amid ongoing military aggression. At the same time, funding for operational support under code 2101020 remains dominant, underscoring the continuing priority of meeting the Armed Forces’ immediate requirements.

Problem Statement

The Ministry of Defence of Ukraine’s budget faces critical wartime challenges of transparency, efficiency, and strategic alignment with growth objectives. Despite substantial allocations under martial law, there is limited empirical evidence on whether these outlays affect economic growth or are economically justified in the short or long term.

We address this by positing two hypotheses: (H1) defence expenditure affects economic growth in Ukraine; (H2) defence expenditure operates independently under wartime fiscal constraints.

Using econometric analysis and time-series modelling, we examine whether defence expenditure interacts with economic growth—a question crucial for policy-making, fiscal planning, and post-conflict recovery.

Research Methodology

This study employs a quantitative, time-series econometric approach using data on Ukraine's GDP and defence expenditure for 1993–2023. Data were compiled from national statistical databases, international financial reports, and official Ukrainian budget documents. To achieve stationarity, GDP is modelled in second differences and defence expenditure in log-differences.

We apply the following econometric methods: the Augmented Dickey–Fuller (ADF) test to assess stationarity and determine required transformations; Granger causality tests to examine directional predictability between economic growth and defence expenditure; vector autoregression (VAR) to analyse the dynamics of a multivariate system and model interactions; and Ridge and ordinary least squares (OLS) regressions to evaluate predictive power and address potential multicollinearity among explanatory variables.

For diagnostics and validation, we check eigenvalue stability (all roots inside the unit circle), compute variance inflation factors (VIFs) to confirm low multicollinearity, and use impulse response functions (IRFs) to visualise shock effects and temporal responses.

This integrated methodological framework enables a rigorous assessment of causal linkages, evaluation of forecast reliability, and the derivation of robust conclusions in the context of Ukraine's defence economy.

Results and Discussion

Before conducting statistical tests, we examine the underlying trends

Table 1 — GDP and Military Expenditures

Year	GDP (current US\$)	Military Expenditure (current US\$)
1993	65,648,559,903	152,233,867
1994	52,549,553,403	919,044,682
1995	48,213,856,469	1,046,793,431
1996	44,558,831,005	1,464,905,136
1997	50,151,531,592	2,068,583,952

Created by the author based on **source:** *World Bank ... (2025)*

The graph above provides a compelling visual representation of Ukraine's GDP and military expenditures over three decades (1993–2023). Several key observations stand out:

GDP growth and fluctuations: steady growth until 2013, followed by a sharp drop in 2014 — possibly related to geopolitical events. Recovery in 2016 and a strong peak in 2021 is likely to be driven by economic stabilization.

Military expenditures trends: relatively stable until 2014, when expenditures spiked, reflecting increased investment in defense. Another sharp increase in 2022, possibly influenced by Russo-Ukrainian conflicts. This suggests that economic growth and military expenditures may be interdependent — an ideal situation for causality analysis.



Picture 2 – GDP & Military Expenditures visualizing over time

Source: World Bank ... (2025)

Let's check if GDP and Military Expenditures are stationary using the Augmented Dickey-Fuller test. This test helps determine whether the time series data has a unit root, which would mean it needs transformation (e.g., differencing) before econometric modelling.

Table 2 — The Augmented Dickey-Fuller test results

Variable	ADF Statistic	p-value	Stationarity Conclusion
GDP	-1.0576	0.7317	Non-Stationary (Fail to reject (H_0))
Military Expenditures	2.5364	0.9991	Non-Stationary (Fail to reject (H_0))

Created by the author

From a Table above it is obvious that:

since the p-values > 0.05 , we fail to reject the null hypothesis, meaning both GDP and Military Expenditures are non-stationary in their current form;

to achieve stationarity, we need to consider applying log differencing or higher-order differencing.

Differencing removes trends and makes the series stationary. From a structured summary table below we propose to observe the descriptive statistics for GDP and Military Expenditures after differencing.

Table 3 — Descriptive statistics

Metric	GDP_Diff	Military_Expenditures_Diff
Count	30	30
Mean	3.77×10^9	2.15×10^9
Standard Deviation (Std)	2.62×10^{10}	7.43×10^9
Min	-6.65×10^{10}	-1.35×10^9
25th Percentile	-4.17×10^9	-1.88×10^7
Median (50th Percentile)	7.42×10^9	2.54×10^8
75th Percentile	1.94×10^{10}	6.87×10^8
Max	4.31×10^{10}	3.43×10^{10}

Created by the author

From the table above it's obvious that:
 wide range of values—both variables exhibit large fluctuations over time;
 high standard deviation—GDP and Military Expenditures show significant volatility in their growth rates;
 negative minimum values—indicating periods of contraction in both GDP and military expenditures.

In the Table below we present ADF Test Results for Differenced Variables.

Table 4 — ADF Test Results for Differenced Variables

Variable	ADF Statistic	p-value	Stationarity Conclusion
GDP (Differenced)	-5.0311	1.93×10^{-5}	Stationary (Reject (H_0))
Military Expenditures (Differenced)	1.5146	0.9976	Non-Stationary (Fail to reject (H_0))

Created by the author

It's worth noting that GDP (Differenced) is now stationary, meaning past GDP values can be used for meaningful time-series modelling. Military Expenditures (Differenced) remain non-stationary, implying that further transformations may be needed.

Thus, if both GDP and Military Expenditures are stationary, we proceed to Granger causality testing. If one or both are still non-stationary, we need to apply second-order differencing.

Bellow we present structured summary table of the descriptive statistics for second-differenced GDP and Military Expenditures.

Table 5 — ADF Test Results for Differenced Variables

Metric	GDP_Diff2	Military_Expenditures_Diff2
Count	29	29
Mean	1.03×10^9	7.86×10^8
Standard Deviation (Std)	3.69×10^{10}	6.77×10^9
Min	-1.06×10^{11}	-1.07×10^{10}
25th Percentile	-2.29×10^9	-3.95×10^8
Median (50th Percentile)	4.19×10^9	1.36×10^8
75th Percentile	1.11×10^{10}	4.10×10^8
Max	8.62×10^{10}	3.42×10^{10}

Created by the author

We can conclude that a second differencing reduced long-term trends but retained significant short-term variability. Large standard deviations—suggesting continued volatility, even after second differencing. Negative minimum values—indicating that both GDP and Military Expenditures experienced contractions.

In the Table below we present ADF Test Results for Second-Order Differencing.

Table 6 — ADF Test Results for Second-Order Differencing

Variable	ADF Statistic	p-value	Stationarity Conclusion
GDP (Second-Order Differenced)	-4.7726	6.13×10^{-5}	Stationary (Reject (H_0))
Military Expenditures (Second-Order Differenced)	-2.2247	0.1974	Non-Stationary (Fail to reject (H_0))

Created by the author

Our results show that GDP is now stationary (since $p\text{-value} < 0.05$), but Military Expenditures are still non-stationary ($p\text{-value} = 0.197$). This means we need further transformation on Military Expenditures before proceeding with econometric modelling. Therefore, since second-order differencing wasn't enough, let's apply third-order differencing to Military Expenditures.

Table 7 — Third-order differencing to Military Expenditures

Metric	Military_Expenditures_Diff3
Count	28
Mean	-3.60×10^8
Standard Deviation (Std)	1.10×10^{10}
Min	-4.49×10^{10}
25th Percentile	-7.50×10^8
Median (50th Percentile)	-2.39×10^7
75th Percentile	5.91×10^8
Max	3.47×10^{10}

Created by the author

We can observe that mean is close to zero. It indicates that third-order differencing reduced long-term trends. High standard deviation suggests military expenditures remain volatile even after transformation. Negative values in minimum and median indicate periods of contraction in military expenditures.

Meanwhile we must conclude that differencing is not working, so we must try log transformation to stabilize variance and remove unit roots. In the Table below we present log-differenced Military Expenditures.

Table 8 — Third-order differencing to Military Expenditures

Metric	Military_Expenditures_LogDiff
Count	26
Mean	0.1325
Standard Deviation (Std)	0.3988
Min	-0.4001
25th Percentile	-0.0202
Median (50th Percentile)	0.0828
75th Percentile	0.2107
Max	1.7868

Created by the author

Log-differenced military expenditures data is now clean, with only one missing value removed. By the way, the summary statistics show:

Mean: 0.132, indicating slight overall growth.

Standard deviation: 0.398, suggesting moderate fluctuations.

Min & Max: -0.40 to 1.78, capturing major shifts.

Now, let's re-run the ADF test to confirm stationarity.

Table 9 — Descriptive statistics

Metric	Military_Expenditures_LogDiff
Count	26
Mean	0.1325
Standard Deviation (Std)	0.3988
Min	-0.4001
25th Percentile	-0.0202
Median (50th Percentile)	0.0828
75th Percentile	0.2107
Max	1.7868

Created by the author

Mean ~ 0.13 , indicating a moderate average annual change in military expenditures. Standard deviation ~ 0.40 , showing some variability, but not extreme fluctuations. Negative minimum value (-0.40) confirms certain years saw declines in military expenditures.

Table 10 — ADF test results

Variable	ADF Statistic	p-value	Stationarity Conclusion
Military Expenditures (Log Differenced)	-3.9996	0.0014	Stationary (Reject (H_0))

Created by the author

From a Table above we can observe that military expenditures data is now stationary, since the p-value is below 0.05. Both GDP and military expenditures are now stationary, meaning we can proceed to Granger causality testing.

Next, we must test whether GDP influences military expenditures—or vice versa. The Granger causality test will determine if past values of one variable help predict the other.

Table 11 — The Granger causality test results

Lags	F-Test (F, p-value)	Chi ² Test (Chi ² , p-value)	Likelihood Ratio (Chi ² , p-value)
1	1.1180, 0.3018	1.2704, 0.2597	1.2392, 0.2656
2	0.4564, 0.6403	1.1530, 0.5619	1.1262, 0.5694
3	0.6428, 0.5986	2.7721, 0.4281	2.6174, 0.4545
4	0.4001, 0.8051	2.7087, 0.6077	2.5545, 0.6349
5	0.4321, 0.8165	4.5368, 0.4750	4.1076, 0.5340

Created by the author

Granger causality test results indicate that GDP does not Granger-cause Military Expenditures, at least within the specified lags. Across all lag choices (1 to 5 lags), the p-values remain above 0.05, meaning we fail to reject the null hypothesis. This suggests that past GDP values do not significantly predict future military expenditures in Ukraine.

Reverse Granger causality test results show that military expenditures do not Granger-cause GDP across all lags tested. P-values remain above 0.05 across lags 1 to 5, meaning we fail to reject the null hypothesis. This suggests that past military expenditures do not significantly predict future GDP in Ukraine. Together with our initial Granger test (GDP $\rightarrow$ Military Expenditures), this means there is no clear unidirectional causality between these two variables.

Table 11 — The reverse Granger causality test results

Lags	F-Test (F, p-value)	Chi ² Test (Chi ² , p-value)	Likelihood Ratio (Chi ² , p-value)
1	0.0036, 0.9529	0.0041, 0.9492	0.0041, 0.9492
2	1.2551, 0.3076	3.1709, 0.2049	2.9782, 0.2256
3	0.6606, 0.5882	2.8488, 0.4155	2.6857, 0.4427
4	0.4009, 0.8046	2.7136, 0.6068	2.5588, 0.6341
5	0.3069, 0.8978	3.2225, 0.6657	2.9980, 0.7003

Created by the author

Since causality tests alone didn't show a direct predictive relationship, let's analyze the dynamic interactions between GDP and Military Expenditures using Vector Autoregression (VAR).

Table 12 — Vector Autoregression results

Model	Method	No. of Equations	Nobs	BIC	HQIC	Log Likelihood	FPE	AIC	Det (Omega_mle)
VAR	OLS	2	26	47.0806	47.0117	-682.574	2.54×10^{20}	46.9838	2.355×10^{20}

Created by the author

Next, we present regression results for Military_Expenditures_LogDiff and GDP_Diff2 variables.

Table 13 — Regression results for Military_Expenditures_LogDiff

Coefficient	Std. Error	t-Statistic	p-Value
Const	0.1325	0.0782	1.694

Created by the author

Table 14 — Regression results for GDP_Diff2

Coefficient	Std. Error	t-Statistic	p-Value
Const	4.30×10^8	7.64×10^9	0.056

Created by the author

Table 15 — Correlation Matrix of Residuals

Variable	Military_Expenditures_LogDiff	GDP_Diff2
Military_Expenditures_LogDiff	1.0000	-0.1546
GDP_Diff2	-0.1546	1.0000

Created by the author

VAR model results provide valuable insight into the relationship between military expenditures and GDP in Ukraine. Coefficient Estimates:

Military Expenditures Equation: Constant = 0.132, indicating slight upward movement, but p-value (0.090) suggests it's not statistically significant.

GDP Equation: Constant = ≈ 429.78 million, but with a very high standard error—the p-value (0.955) indicates no statistical significance.

Model Performance Indicators:

AIC (46.98) and BIC (47.08) show how well the model fits; lower values indicate better model selection.

Det (Ω_{mle}) $\approx 2.35 \times 10^{20}$ reflects the estimated variance of residuals—high values suggest volatility.

Weak negative correlation (-0.154) between GDP and military expenditures, meaning they do not strongly move together.

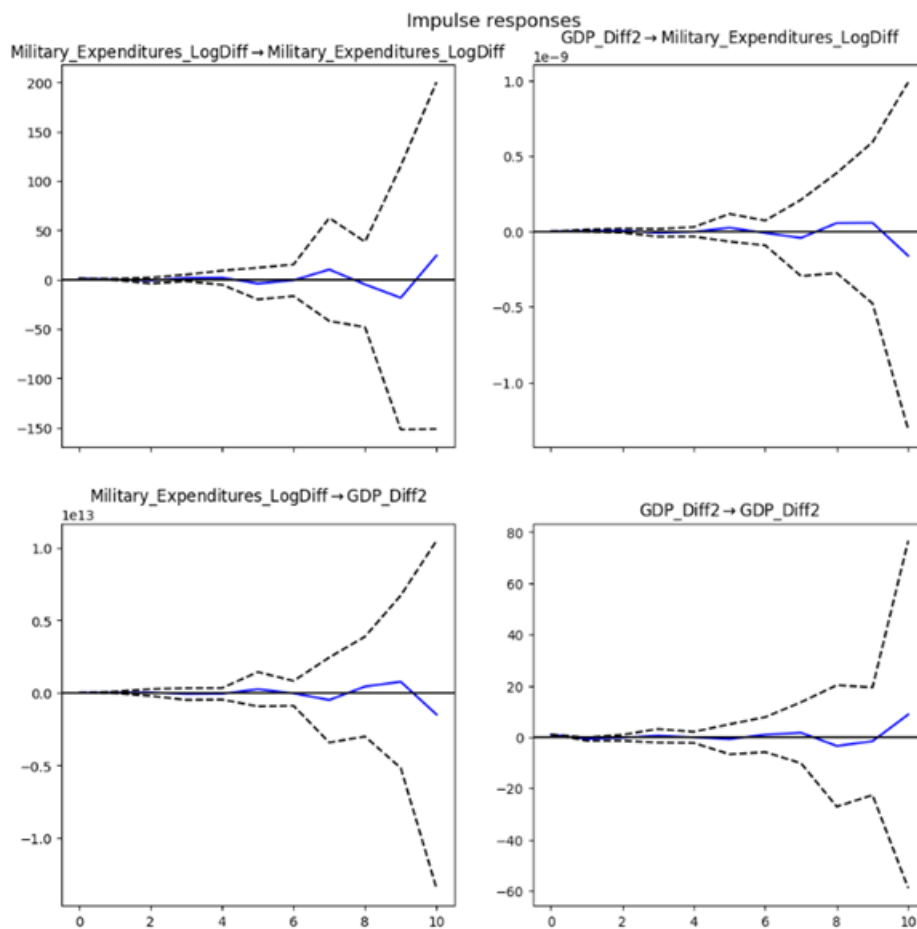
Next, we'll use the VAR model to simulate how a shock in one variable affects the other.

Also, from the tables above we can conclude:

Military Expenditures' coefficient has marginal significance ($p = 0.090$), but not strong evidence.

GDP constant is statistically insignificant ($p = 0.955$), confirming weak relationship between GDP and military expenditures.

Negative residual correlation (-0.1546) suggests weak inverse association between GDP and Military Expenditures.



Picture 3 – Impulse Response Function plot

Source: created by the author

Our Impulse Response Function (hereinafter—IRF) plots provide valuable insights into how military expenditures and GDP interact over time when experiencing shocks. So, we must break them down:

Military Expenditures → Military Expenditures (Top-left plot). The response gradually declines over time, suggesting that military expenditure shocks have a short-term effect before stabilizing.

GDP → Military Expenditures (Top-right plot). The response is close to zero, indicating that GDP shocks do not significantly influence future military expenditures.

Military Expenditures → GDP (Bottom-left plot). The response fluctuates slightly, but overall remains weak, meaning military expenditure shocks do not strongly impact GDP growth.

GDP → GDP (Bottom-right plot). The response remains stable, implying that GDP shocks have a persistent effect on future GDP values

Therefore, the IRF results confirm weak interaction between military expenditures and GDP, which aligns with the Granger causality test findings. To further refine insights, we can test different lag structures (e.g., extending to 10+ lags); introduce additional economic variables (such as inflation or government spending); explore structural breaks or geopolitical influences. However, it is important to note that such research possibilities should be left out of the scope of the current study due to their considerable scope.

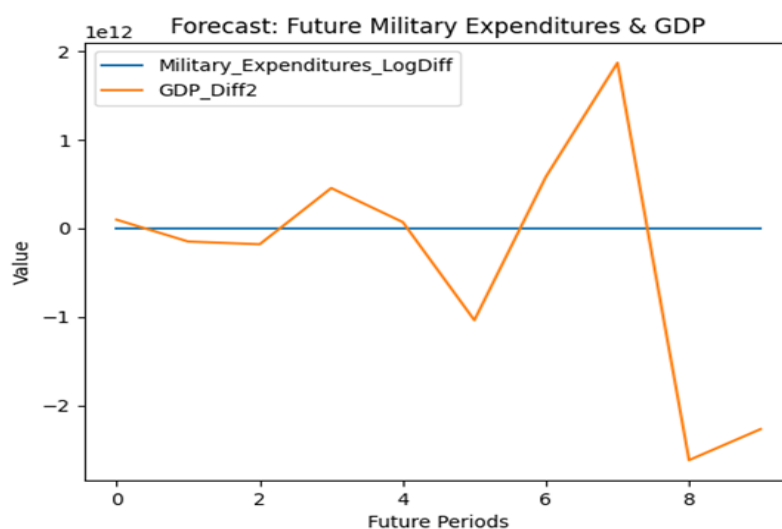
Since VAR model captures dynamic relationships between GDP and military expenditures, we can predict future values using VAR forecasting. In the Table below we present military expenditures (Log-Differenced) and GDP (Second-Order Differenced).

Table 16 — Values predicted

Index	Military_Expenditures_LogDiff
0	-2.2616
1	2.4058
2	4.9367
3	-7.3655
4	-4.3117
5	20.5546
6	-3.7274
7	-41.4708
8	38.6514
9	65.1673

Created by the author

To make the projections clearer, we plot the forecasted values.



Picture 4 – Military Expenditures and GDP forecast

Source: created by the author

Our forecasted values show considerable fluctuations in both military expenditures and GDP over the next 10 periods. Need to highlight specific features of military expenditures forecast: alternating between positive and negative values, suggesting short-term volatility.

some extreme swings (e.g., -41.47 at period 7, then +38.65 at period 8), hinting at possible sensitivity to economic shifts.

GDP forecast:

Massive fluctuations in predicted GDP values, ranging from positive trillions to negative trillions.

Such high variability suggests underlying structural instability in the economic relationships captured by the model

Next step is to check the model stability. We can provide this action by running a roots test to ensure the VAR system is dynamically stable. This data is shown in a Table below.

Table 17 — Model stability checking

Index	Eigenvalue
1	-15.6749 + 0.j
2	3.1093 + 0.j
3	-1.4505 + 0.j
4	-0.9416 + 0.8702j
5	-0.9416 - 0.8702j
6	1.2075 + 0.j
7	0.4971 + 1.0938j
8	0.4971 - 1.0938j
9	-0.1603 + 0.6542j
10	-0.1603 - 0.6542j

Source: created by the author

Roots test results indicate potential instability in our VAR model. Possible solution is to apply ridge regression for VAR to dampen extreme parameter fluctuations.

Ridge Regression Coefficients: [-1.58243915e-12]

Ridge regression coefficients are extremely small (-1.58×10^{-12}), suggesting that the model barely adjusts the relationship between GDP and military expenditures. Near-zero coefficients mean weak predictive power. Ridge regression penalizes large coefficients, but here, the relationship is already weak, meaning military expenditures do not strongly predict GDP (or vice versa).

Updated Ridge Coefficients: [-1.58243915e-12]

Ridge regression coefficients are still near zero, even after adjusting the regularization strength ($\alpha=0.01$). This suggests that military expenditures have little predictive influence on GDP in the current dataset.

Table 18 — Model stability checking

Feature	VIF
Military_Expenditures_LogDiff	1.0208
GDP_Diff2	1.0208

Source: created by the author

Possible reason for near-zero coefficient is that there could be the multicollinearity in predictors. So, there must be a possibility to take an additional test using Variance Inflation Factor (hereinafter—VIF).

Variance Inflation Factor (VIF) results suggest low multicollinearity between military expenditures and GDP, since both VIF values are close to 1.02. However, since multicollinearity isn't an issue, the near-zero Ridge regression coefficients are likely due to a weak statistical relationship between GDP and military expenditures.

It's worth noting that our goal is to confirm model stability before forecasting. Given instability in the VAR roots test, we should either run standard OLS regression to compare coefficient strengths.

OLS Regression Coefficients: [-0.06044556]

Least-squares regression coefficient (-0.0604) indicates a weak negative relationship between GDP and military expenditures in our dataset. This is consistent with your previous findings — there does not appear to be a strong direct economic relationship between these two variables.

To summarize, we need to interpret the results. Overall, a small decrease in military expenditures is correlated with a small increase in GDP, but the impact is minimal.

At the same time, such empirical results can obviously indicate that indeed an increase in military expenditures could lead to a decrease in economic growth for Ukraine. Meanwhile, we are aware of our responsibility to the country and its people, which is the importance of maintaining a high level of national security and defence, which cannot be achieved without an appropriate (high) level of military expenditures, given the fact of Russian armed aggression for more than a decade.

We also see, —analysing the historical aspect of military expenditures and their impact on economic growth, that this impact could have been negative (given the prospect of thirty-two years of Ukraine's independence). Nevertheless, it's reasonable propose to look for possible solutions to this problematic situation, and, as we noted in the first half of this paper, financial support from partners will remain an important source of economic stability for Ukraine for at least the next ten to twenty years, which may well be in line with Ukraine's long-term development perspective.

The process of Europeanisation may play a key role here, given the initial volumes of investment in the Ukrainian economy at the stage of accession to the EU.

The last call to install an appropriate test result before providing a ratio in our forecast is by model fitting—using R^2 score. The question is, how well OLS explains variance in military expenditures?

OLS R^2 Score: 0.023895089616717047

OLS R^2 score is extremely low, meaning the model explains only ~2.4% of the variance in military expenditures based on GDP differences. This confirms that GDP does not significantly predict military expenditures in our dataset.

What could be the next steps to improve modelling and its results?

- while GDP alone does not have a strong influence on military expenditures (or another variables/vice-versa), adding factors such as inflation, government spending or foreign aid can improve forecasting;
- if the relationship is non-linear (this fact can be obviously accepted for our case), approaches such as polynomial regression or decision trees can reveal hidden patterns;
- if military expenditures are politically driven, traditional econometric models may not fully capture the decision-making process.

Thus, we inclined to make such calculations in future research.

Conclusion

For the Granger tests, GDP and defence expenditure were transformed to achieve stationarity using log-differencing and, where required, higher-order differencing. Granger causality tests indicated no significant causal relationship between the two variables: neither GDP Granger-causes defence expenditure nor vice versa.

A VAR model was estimated, but the coefficients were not statistically significant (p -values > 0.05), consistent with weak interaction. Residual correlations suggested a modest negative association (≈ -0.154), implying minimal influence between GDP and defence spending. Impulse responses showed that shocks to defence expenditure dissipate quickly, with no persistent effects on GDP, while GDP shocks had little impact on subsequent defence expenditure—further evidence against direct causality.

VAR forecasts exhibited pronounced volatility, suggesting model instability. A stability (roots) test confirmed this, with a large explosive root ($|\lambda|_{\max} \approx 15.67$). Ridge regression produced near-zero coefficients, and OLS yielded a small negative coefficient (-0.0604) with $R^2 \approx 0.024$, indicating that GDP explains little of the variation in defence expenditure.

Implications for further work. Consider longer lag structures to capture delayed effects; incorporate additional macroeconomic controls (e.g., total government spending, inflation, geopolitical risk); and explore non-linear modelling approaches to uncover potential hidden dynamics.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

- Awaworyi Churchill, S., & Yew, S. L. (2018). The effect of military expenditure on growth: An empirical synthesis. *Empirical Economics*, 55(3), 1357–1387. <https://doi.org/10.1007/s00181-017-1300-z>
- Doctrine of defense planning in the armed forces of Ukraine. (2020). Main department of defense planning of the general staff of the armed forces of Ukraine. Available from : https://sprotyvg7.com.ua/wp-content/uploads/2024/08/2_%D0%A1%D0%9F-5-006701.01-%D0%94%D0%9E%D0%9A-%D0%97-%D0%9E%D0%91%D0%9E%D0%A0-%D0%9F%D0%9B-%D0%A3-%D0%97%D0%A1%D0%A3.pdf
- Karp, E. V. (2018). *Structural changes in Ukraine's state budget expenditures on defence*. Economy and Society, (14). Available from : https://economyandsociety.in.ua/journals/14_ukr/115.pdf
- Lyutiy, I., Petlenko, Y., & Drozd, N. (2022, December 1). *The importance of openness and transparency in the budget process in the defence and security sector of Ukraine*. Financial and Credit Activity: Problems of Theory and Practice, 6(47), 99–110. <https://doi.org/10.55643/fcaptp.6.47.2022.3900>
- Nate, S., Stavitsky, A., & Kharlamova, G. (2023). *Index of the openness and transparency of budgeting and financial management of the defence and security sector: Case of Ukraine*. Sustainability, 15(7), 5617. <https://doi.org/10.3390/su15075617>
- On amendments to Section VI “Final and Transitional Provisions” of the Budget Code of Ukraine and other legislative acts of Ukraine, Law of Ukraine No. 2134-IX (15 March 2022). Retrieved July 21, 2025, Available from : <https://zakon.rada.gov.ua/go/2134-20>

- On amendments to the Tax Code of Ukraine and other laws of Ukraine regarding ensuring balanced budget revenues during the period of martial law, Law of Ukraine No. 4015-IX (10 October 2024). Retrieved July 21, 2025, Available from : <https://zakon.rada.gov.ua/go/4015-20>
- On the State Budget of Ukraine for 2025, Law of Ukraine No. 4059-IX (19 November 2024; current version as of August 1, 2025). Retrieved July 21, 2025, Available from : <https://zakon.rada.gov.ua/go/4059-20>
- Petlenko, Y., Kharlamova, G., Giedraitis, V. R., Stavitsky, A., & Ulvidienė, E. (2025). *Exploring Scandinavian approaches to defense budget transparency in Ukraine: A theoretical review of opportunities and challenges*. *Public and Municipal Finance*, 14(1), 65–84. [https://doi.org/10.21511/pmf.14\(1\).2025.06](https://doi.org/10.21511/pmf.14(1).2025.06)
- Saeed, L. (2025). *The impact of military expenditures on economic growth: A new instrumental variables approach*. *Defence and Peace Economics*, 36(1), 86–101. <https://doi.org/10.1080/10242694.2023.2259651>
- World Bank. (n.d.). *World Bank Open Data*. Retrieved July 19, 2025, Available from : <https://data.worldbank.org/>.

Список використаних джерел

- Awaworyi Churchill, S., Yew, S. L. The effect of military expenditure on growth: An empirical synthesis // *Empirical Economics*. – 2018. – Vol. 55, No. 3. – P. 1357–1387. – DOI: <https://doi.org/10.1007/s00181-017-1300-z>. ideas.repec.org/research/monash.edu
- Генеральний штаб Збройних Сил України. Головне управління оборонного планування. Доктрина з оборонного планування у Збройних Силах України. – 2020. – URL: https://sprotyv7.com.ua/wp-content/uploads/2024/08/2_%D0%A1%D0%9F-5-006701.01-%D0%94%D0%9E%D0%9A-%D0%97-%D0%9E%D0%91%D0%9E%D0%A0-%D0%9F%D0%9B-%D0%A3-%D0%97%D0%A1%D0%A3.pdf (дата звернення: 02.09.2025). Sprotyv G7
- Karp, E. V. Structural changes in Ukraine's state budget expenditures on defence // *Economy and Society*. – 2018. – Issue 14. – URL: https://economyandsociety.in.ua/journals/14_ukr/115.pdf (дата звернення: 02.09.2025). Економіка та суспільство
- Lyutiy, I., Petlenko, Y., Drozd, N. The importance of openness and transparency in the budget process in the defence and security sector of Ukraine // *Financial and Credit Activity: Problems of Theory and Practice*. – 2022. – Vol. 6, No. 47. – P. 99–110. – <https://doi.org/10.55643/fcaptp.6.47.2022.3900>. [fkd.net.ua/CBS Research Portal](https://fkd.net.ua/CBS_Research_Portal)
- Nate, S., Stavitsky, A., Kharlamova, G. Index of the openness and transparency of budgeting and financial management of the defence and security sector: Case of Ukraine // *Sustainability*. – 2023. – 15(7), Article 5617. – <https://doi.org/10.3390/su15075617>. MDPI
- Про внесення змін до розділу VI «Прикінцеві та перехідні положення» Бюджетного кодексу України та інших законодавчих актів України : Закон України від 15.03.2022 № 2134-IX. – URL: <https://zakon.rada.gov.ua/go/2134-20> (дата звернення: 02.09.2025). Законодавство України
- Про внесення змін до Податкового кодексу України та інших законів України щодо забезпечення збалансованості бюджетних надходжень у період дії воєнного стану : Закон України від 10.10.2024 № 4015-IX. – URL: <https://zakon.rada.gov.ua/go/4015-20> (дата звернення: 02.09.2025). Законодавство України tax.gov.ua
- Про Державний бюджет України на 2025 рік : Закон України від 19.11.2024 № 4059-IX (чинна ред. станом на 01.08.2025). – URL: <https://zakon.rada.gov.ua/go/4059-20> (дата звернення: 02.09.2025). Законодавство України

- Petlenko, Y., Kharlamova, G., Giedraitis, V. R., Stavytskyi, A., Ulvidienė, E. Exploring Scandinavian approaches to defense budget transparency in Ukraine: A theoretical review of opportunities and challenges // *Public and Municipal Finance*. – 2025. – Vol. 14, No. 1. – P. 65–84. – [https://doi.org/10.21511/pmf.14\(1\).2025.06](https://doi.org/10.21511/pmf.14(1).2025.06). [businessperspectives.orgCBS Research Portal](https://businessperspectives.org/CBS-Research-Portal)
- Saeed, L. The impact of military expenditures on economic growth: A new instrumental variables approach // *Defence and Peace Economics*. – 2025. – 36(1). – P. 86–101. – <https://doi.org/10.1080/10242694.2023.2259651>. [ideas.repec.orgUlster University](https://ideas.repec.org/Ulster-University)
- World Bank. World Bank Open Data. – URL: <https://data.worldbank.org/> (дата звернення: 02.09.2025).

Розвиток державної політики в публічних та оборонних закупівлях України: виклики та шляхи розвитку

The Evolution of State Policy in Public and Defense Procurement in Ukraine: Challenges and Development Pathways

Олена Голота

Olena Holota

к. екон. н., доцент, доцент, професор кафедри оборонного менеджменту, e-mail: o.holota@mil.ua, ORCID: 0000-0003-4323-4344

Ph. D., Associate Professor, Professor of the Defense Management Department, e-mail: o.holota@mil.ua, ORCID: 0000-0003-4323-4344

Національний університет оборони України, м. Київ, Україна

National University of Defense of Ukraine, Kyiv, Ukraine

Received: August 02, 2025 | Revised: August 19, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.20>

Мета роботи. Проаналізувати етапи розвитку державної політики у сфері публічних і оборонних закупівель України (2014–2024), виявити ключові виклики трансформації та оцінити відповідність міжнародним стандартам.

Методи дослідження. Теоретичний та інституційний аналіз, порівняльно-правовий підхід.

Результати дослідження. Систематизовано етапи реформ; зафіксовано зростання прозорості (Prozorro, гармонізація з директивами ЄС) і ризики воєнного стану через спрощені процедури. Оцінено ефективність нових інституцій — ДП «Агенція оборонних закупівель» і ДП «Державний оператор тилу» — у контексті професіоналізації закупівель. Зроблено висновок про потребу посилення інституційної спроможності, контролю та підзвітності й повернення до конкурентних процедур після війни.

Теоретична цінність дослідження. Показано закупівлі як результат взаємодії законодавчих процесів, міжнародних зобов'язань і інституційних змін. Запропоновано концепт циклічності реформ, де під впливом війни змінюються пріоритети між прозорістю, швидкістю та безпекою.

Практична цінність дослідження. Визначено критичні точки трансформації в умовах воєнного стану та напрями вдосконалення для політики відновлення, адаптації до міжнародних вимог і підготовки управлінських рішень в оборонних закупівлях.

Цінність дослідження. Уперше комплексно проаналізовано трансформацію політики публічних і оборонних закупівель України в умовах війни з урахуванням міжнародних стандартів; подано рекомендації для подальшого реформування в період поствоєнного відновлення.

Тип статті. Теоретико-аналітична.

Purpose. Analyse stages of Ukraine’s public and defense procurement policy (2014–2024), identify key transformation challenges, and assess compliance with international standards.

Method. Theoretical analysis, comparative-legal method, institutional analysis.

Findings. Systematises the 2014–2024 policy transformation; records transparency gains (Prozorro, EU harmonisation) and wartime risks from simplified procedures. Evaluates new institutions—State Enterprise “Defense Procurement Agency” and State Enterprise “State Logistics Operator”—against international professionalisation benchmarks. Concludes on the need to strengthen institutional capacity, tighten control and accountability, and return to competitive procedures after martial law.

Theoretical implications. Frames procurement policy as an interplay of national legislation, international commitments, and institutional change; conceptualises reforms as cyclical, with war shifting priorities among transparency, speed, and security. Contributes to scholarship in public administration, defense policy, and European integration.

Practical implications. Identifies critical inflection points and improvement areas; informs post-war recovery policy, alignment with international standards, and managerial decisions in defense procurement.

Value. Offers the first comprehensive wartime analysis of public and defense procurement transformation aligned with international standards, providing actionable recommendations for reform during post-war recovery.

Paper type. Theoretical and analytical

Ключові слова: державні (публічні) закупівлі, оборонні закупівлі, державна політика, воєнний стан, ефективність закупівель.

Key words: public procurement, defense procurement, state policy, martial law, procurement efficiency.

Вступ

В умовах посилення загроз національній безпеці України (зокрема повномасштабного вторгнення РФ) особливо підвищується значення такої складової державного управління, як управління системою державних (публічних) закупівель, це стосується як і в цілому усієї системи публічних закупівель, так і її окремої складової оборонних закупівель. Система державних (публічних) закупівель має безпосередній вплив на економічну ефективність, якість надання державних послуг та рівень довіри громадян до державних інституцій.

Сфера публічних закупівель охоплює значну частку державних витрат, і тому є пріоритетною ділянкою для забезпечення раціонального використання коштів, запобігання їх нецільовому використанню та корупційним проявам. Ефективна та прозора система

закупівель сприяє розвитку конкуренції, залученню інвестицій та підвищенню загального добробуту суспільства.

Реформа закупівельної системи упродовж останніх років проходить під впливом євроатлантичних інтеграційних зобов'язань та викликів пов'язаних з введенням воєнного стану. Задля пошуку напрямків подальшого розвитку державної політики у сфері публічних закупівель проведемо аналіз еволюції зазначеної державної політики, зокрема законодавчих змін в публічних та оборонних закупівлях, впливу міжнародних стандартів (ЄС, США, НАТО), а також інституційних та нормативних викликів, що стоять перед Україною в цій галузі.

Теоретичні основи дослідження

Проблематика публічних та оборонних закупівель в Україні є предметом значної уваги з боку науковців, експертів та громадськості. Реформа системи публічних закупівель, зокрема запровадження електронної системи Prozorro, стала об'єктом численних досліджень, що аналізують її вплив на підвищення прозорості, конкуренції та економії бюджетних коштів [1, 2, 3]. Значний внесок у дослідження ефективності Prozorro та моніторинг корупційних ризиків зробили такі організації, як Transparency International Ukraine [4], Центр економічної стратегії [5], Центр вдосконалення закупівель Київської школи економіки [6, 7], Інститут економічних досліджень та політичних консультацій [8, 9], а також державні контролюючі органи, зокрема Національне агентство з питань запобігання корупції (НАЗК) [10, 11] та Рахункова палата [12].

Окремий напрям досліджень стосується специфіки оборонних закупівель, їх реформування відповідно до стандартів НАТО та викликів, пов'язаних із забезпеченням обороноздатності в умовах війни [13, 14, 15]. Вплив воєнного стану на систему публічних закупівель загалом та на окремі її аспекти також активно аналізується у наукових публікаціях та аналітичних звітах [16, 17, 18, 19].

Незважаючи на значну кількість публікацій, існує потреба у комплексному аналізі взаємозв'язку державної політики у сферах публічних та оборонних закупівель, особливо в динаміці останніх років, що охоплюють як період активних реформ, так і повномасштабну війну. Часто ці сфери розглядаються відокремлено, тоді як вони є тісно переплетеними, особливо в умовах війни, коли значна частина публічних закупівель прямо чи опосередковано спрямована на потреби оборони. Недостатньо дослідженим залишається питання довгострокового впливу змін, запроваджених під час воєнного стану, на стійкість та ефективність системи закупівель, а також на процеси майбутньої відбудови України.

Постановка проблеми

Мета статті – комплексно проаналізувати еволюцію державної політики України у сфері публічних та оборонних закупівель, зокрема: дослідити ключові законодавчі зміни та впровадження електронної системи закупівель Prozorro; оцінити вплив міжнародних стандартів (ЄС, НАТО, США, GPA COT) на розвиток національного законодавства; розкрити особливості регулювання публічних та оборонних закупівель в умовах воєнного стану; порівняти українську практику із міжнародними підходами у сфері закупівель; виявити інституційні та нормативні виклики; надати рекомендації щодо удосконалення системи закупівель з урахуванням євроатлантичної інтеграції, національної безпеки та доброчесного управління бюджетними ресурсами.

Результати

Аналізуючи зміни, які відбулись у сфері регулювання закупівельної діяльності в державному секторі, варто зазначити, що до 2014 року система державних закупівель в Україні характеризувалася системними вадами, що глибоко вкорінилися та створювали сприятливе підґрунтя для масштабних зловживань в цій сфері. Ключовою нормативно-правовою зміною

стало ухвалення Закону України “Про публічні закупівлі” № 922-VIII від 25.12.2015, який передбачав введення єдиної електронної системи закупівель [20]. Зокрема, вищевказаним законом було встановлено обов’язкове використання електронної системи Prozorro для закупівель товарів та послуг вартістю від 200 тис. грн та робіт – від 1,5 млн грн (для окремих галузей підвищені пороги) [21]. Ухвалення цього закону завершило формування базового правового поля державних (публічних) закупівель, ліквідувавши дублювання норм старого Закону “Про здійснення державних закупівель”. Новий закон окрім того, що зобов’язав використовувати згадану електронну систему закупівель ще і визначив її ключові компоненти: веб-портал Уповноваженого органу та авторизовані електронні майданчики, між якими забезпечується автоматичний обмін інформацією та документами [20]. Детально регламентував процедури планування закупівель, оголошення тендерів, подання пропозицій, проведення аукціонів, визначення переможців та оприлюднення всієї релевантної інформації [20]. Важливим нововведенням стало скорочення переліку підстав для застосування неконкурентних процедур закупівлі та наближення українського законодавства до європейських практик [22].

В Україні в закупівельну діяльність послідовно впроваджувались електронні аукціони: з 1 квітня 2016 року використання електронної системи публічних закупівель Prozorro стало обов’язковим для центральних органів влади та монополістів, а з 1 серпня 2016 року – для всіх публічних замовників [23]. Слід зазначити, що такий підхід дозволив підвищити конкуренцію та прозорість процедур, про що свідчать численні звіти про зниження цін та уникнення корупційних ризиків.

Наступним важливим кроком у реформуванні державної закупівельної системи стало приєднання України до Угоди СОТ про державні закупівлі (Agreement on Government Procurement – GPA). Так, 18 травня 2016 року Міністерство економіки повідомило, що процедура приєднання до GPA завершена [24]. Цим кроком українським компаніям відкрився доступ до ринку держзакупівель 45 країн-учасниць (ЄС, США, Японії тощо) [24], а іноземним – рівний доступ до тендерів в Україні. Угода проілюструвала прихильність до принципу рівного доступу й прозорості в закупівлях. Окрім WTO-GPA, Україна в Угоді про асоціацію з ЄС зобов’язалася поступово гармонізувати вітчизняне законодавство з європейськими директивами про закупівлі, що означає імплементацію таких принципів, як відкритість торгів, недискримінація учасників, обґрунтованість закупівель тощо.

За результатами реформування система публічних закупівель в Україні наблизилася до практик ЄС. Так, Директива ЄС 2014/24/ЄУ підкреслює прозорість, недискримінацію та конкурентність публічних закупівель. Вона вимагає заздалегідь визначати тендерні умови та критерії, фіксувати всі етапи процедури і публікувати інформацію в електронному форматі [25]. Український закон № 922 враховує ці підходи: усі процедури мають бути публічними, рішення оприлюднюються, а підґрунтям їх проведення є заздалегідь затверджений річний план. У результаті реформи 2016–2020 років змінилися й органи управління: уповноваженим органом у сфері закупівель стало Міністерство економіки на чолі з Департаментом державних закупівель, а громадський контроль посилюється завдяки регулярним звітам і відкритому моніторингу.

Окрім вищезгадуваної директиви, існують інші, що також вплинули на українську практику: Директива 2014/25/ЄУ, яка координує процедури закупівель у секторах води, енергії, транспорту та поштових послуг; “директиви про засоби правового захисту” (Remedies Directives), що встановлюють спільні стандарти для всіх держав-членів у разі виявлення дискримінаційних практик у публічних закупівлях; а також Директива 2014/55/ЄУ, що з 2018 року зробила обов’язковим отримання та обробку електронних рахунків (e-invoicing) у публічних закупівлях [26]. Послідовне приведення законодавства у відповідність до директив ЄС (2014/24/ЄУ для публічних, 2009/81/ЄС для оборонних) є не просто юридичною

формальністю, а стратегічним вибором, спрямованим на інтеграцію економічної та безпекової систем України у ширшу європейську рамку, що свідчить про довгострокову відданість євроінтеграції. Директиви ЄС щодо засобів правового захисту та вимоги до електронного виставлення рахунків підкреслюють комплексний характер євроінтеграції, що виходить за рамки лише основних принципів закупівель. Це передбачає необхідність створення надійних механізмів оскарження та подальшу цифровізацію фінансових процесів в Україні.

Все ж таки варто наголосити, що повномасштабне вторгнення рф в Україну зумовило необхідність негайної адаптації системи публічних закупівель до екстремальних умов та подальших суттєвих змін. Так, ключовим нормативно-правовим актом, що врегулював ці питання, стала Постанова Кабінету Міністрів України від 28 лютого 2022 року №169 (далі – Постанова №169), яка на період воєнного стану суттєво спростила процедури закупівель: замовники дістали право не застосовувати конкурентні процедури та відтерміновувати оприлюднення інформації в електронній системі Prozorro. У подальшому Постанова №169 перебувала у стані швидкої регуляторної еволюції: до моменту виведення з під її дії цивільних (публічних) закупівель було прийнято десять її редакцій. Ці зміни поступово звужували початкові спрощення – від практично необмеженого відкладання публікації даних через 20 днів після завершення дії воєнного стану до встановлення обов'язку розкривати відомості та проводити більшість закупівель через Prozorro у визначені строки. Накопичені редакційні розбіжності та потреба у стабільному правовому механізмі зумовили ухвалення нового комплексного акту – постанови Кабінету Міністрів України №1178 від 12 жовтня 2022 року “Про затвердження особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України “Про публічні закупівлі”, на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування” (далі – Постанова №1178) [27], яка систематизувала особливості публічних закупівель у період воєнного стану, а Постанова №169 продовжила діяти лише для оборонних закупівель, хоча не дуже довго, лише до 11 листопада 2022 року.

Необхідно зазначити, що Постанова №1178 суттєво змінила правила гри по відношенню до тих позицій які були викладені у Законі України “Про публічні закупівлі”, зокрема, знизивши порогові значення для обов'язкового проведення конкурентних процедур, запровадивши процедуру “відкриті торги з особливостями”, розширивши можливості використання електронного каталогу Prozorro Market, скоротивши строки проведення процедур та надавши більше гнучкості щодо укладання прямих договорів та внесення змін до істотних умов вже укладених договорів. Наприклад, відкриті торги з особливостями можуть відбутися навіть за наявності одного учасника, а строки для подання пропозицій та укладання договорів були значно скорочені [27]. Одним із дискусійних моментів стало тимчасове скасування з 3 січня 2023 року триаундових електронних аукціонів, що, за оцінками експертів, призвело до зниження рівня економії, особливо у великовартісних тендерах. Хоча з 19 травня 2023 року аукціони були повернуті, замовники отримали право проводити відкриті торги без них, яким, втім, скористалися лише у 0,6% випадків до кінця 2023 року [28]. Так, замовник може скористатися опцією “без аукціону” (п. 37 “Особливостей...”), якщо він: ухвалив обґрунтоване рішення, вказав це у оголошенні та оприлюднив протокол розкриття одразу після дедлайну пропозицій.

Варто відмітити, що Постанова №1178 неодноразово змінювалася Кабінетом Міністрів протягом 2022–2025 років, а якщо точніше, то до неї було внесено 30 змін. Це пов'язано з тим, що перший варіант “Особливостей...” виявив низку прогалин та потребував вдосконалення у міру розвитку ситуації з веденням бойових дій та досвіду замовників. Зокрема, експерти відзначали, що після запровадження Постанови №1178 виявилися певні недоліки, тому уряд кілька разів вносив зміни та продовжує їх удосконалювати дотепер [29]. Наголосимо, що згідно поправки від 1 вересня 2023 року, у відповідності до вимог Постанови №1178 публічні

закупівлі з того моменту та протягом 90 днів після припинення або скасування воєнного стану здійснюються відповідно до Закону України “Про публічні закупівлі” з урахуванням “Особливостей...” та з дотриманням принципів здійснення публічних закупівель викладених у зазначеному законі.

Наведемо основні причини численних поправок:

передусім, це адаптація до нових умов війни. У ході війни з’являлися нові виклики (наприклад, масовані атаки на енергетику восени 2022), що вимагали термінового спрощення закупівель певних категорій. В результаті до “Особливостей...” додавали спеціальні норми – приміром, процедури для закупівлі пального, генераторів, послуг енергосервісу тощо. Кожна така потреба реалізовувалася окремою зміною до постанови;

виправлення початкових обмежень. Первинна редакція Постанови №1178 була досить жорсткою (скасовані переговорні процедури, євроторги тощо). Згодом уряд повернув деякі інструменти, щоб підвищити гнучкість. Наприклад, повернення відкритих торгів з публікацією англійською мовою було здійснено у відповідь на вимоги міжнародних донорів фінансувати закупівлі за прозорими конкурентними процедурами. Так само поступово дозволили переговорну процедуру у виключних випадках (наприклад, для оборонних потреб або якщо відкриті торги не відбулися двічі);

уточнення процедур і критеріїв. Багато змін стосувалися технічних уточнень: підвищення мінімальних строків подання пропозицій на торгах (щоб збільшити конкуренцію), уточнення переліку підстав для відхилення учасників та для внесення змін до договорів, регламентація використання електронних каталогів, деталізація кваліфікаційних вимог для різних предметів закупівлі тощо. Ці зміни покращували і конкретизували правила, базуючись на практиці застосування постанови;

законодавчі та політичні чинники. Постанова №1178 тісно пов’язана із Законом “Про публічні закупівлі”, зокрема з перехідними положеннями воєнного стану. Коли змінювали сам закон або приймали нові урядові рішення (наприклад, про санкції проти РФ/РБ чи про бюджетні обмеження), це вимагало коригування “Особливостей...”. Тому Кабінет Міністрів України оперативно вносив правки, щоб Постанову №1178 узгодити з актуальними нормами та рішеннями.

Таким чином, численні зміни до Постанови № 1178 пояснюються динамічними обставинами воєнного часу та необхідністю постійно вдосконалювати правила закупівель. Такий процес оновлення є фактичним свідченням гнучкого підходу держави, яка балансувала між швидкістю закупівель, їхньою ефективністю та прозорістю в умовах війни.

В свою чергу, сфера оборонних закупівель тривалий час була окремою зоною та регулювалася Законом України “Про державне оборонне замовлення”, а закупівлі у цій сфері відповідно регулювались базуючись на принципах радянської планової економіки. Першим підґрунтям для глибокої реформи стало введення в дію Закону України “Про оборонні закупівлі” № 808-IX від 17.07.2020 року. Вказаний закон визначив загальні правові засади планування та проведення закупівель товарів, робіт і послуг оборонного призначення, а також механізми громадського та демократичного контролю над ними. Він докорінно змінив законодавство про оборонні закупівлі з радянських на європейські стандарти, оскільки передбачав гармонізацію принципів та засад з Директивою ЄС 2009/81/ЄС про оборонні закупівлі відповідно до Угоди про асоціацію, та замінив Державне оборонне замовлення (ДОЗ) трирічним планом закупівель. Було виділено два важливих органи у сфері планування та здійснення оборонних закупівель, а саме: головний орган у сфері планування оборонних закупівель (Міністерство з питань стратегічних галузей промисловості України) та головний орган у сфері здійснення оборонних закупівель (Міністерство оборони України). Основне спрямування нового закону було на забезпечення відкритості процедур, підвищення прозорості планування та запобігання корупції в оборонному секторі. Зокрема, в преамбулі

закону зазначено, що метою є забезпечення потреб оборони через ефективні й прозорі закупівлі з дотриманням захисту національних інтересів і створення конкурентного середовища [30]. Слід наголосити на тому, що закон дозволяє здійснювати оборонні придбання у співпраці з міжнародними організаціями: через Агенцію НАТО з підтримки і постачання (NSPA) та за програмою уряду США Foreign Military Sales (FMS), що інтегрує Україну у глобальні ланцюги постачання оборонної продукції.

Додатково механізми планування і контролю визначені Постановою Кабінету Міністрів України №363 від 03.03.2021 “Про порядок планування, формування, розміщення, контролю та звітування про оборонні закупівлі”, що регламентує деталізацію очікуваної вартості контрактів і строки проведення процедур [31]. Варто зазначити, що вимогами вищезазначеної Постанови №363 встановлено, що визначення очікуваної вартості для оборонних закупівель в основному базується на маркетингових дослідженнях, передусім це стосується закупівель, які здійснюються через конкурентні процедури. Для будь-яких торгів (відкритих, обмежених, спрощених) замовник самостійно формує очікувану вартість на підставі аналізу ринку. В свою чергу, для закупівель, які здійснюються без застосування конкурентних процедур (особливо це стосується закупівель у єдиного постачальника), виконавець подає калькуляцію ціни з розгорнутими розрахунками, які представництво замовника перевіряє й формує висновок, який замовник затверджує як орієнтовну вартість; якщо ж закупівлі проводять через закриті переговори, тоді можуть поєднуватися обидва підходи [31].

Наступним важливим кроком у реформуванні оборонних закупівель стає затвердження “Особливостей здійснення оборонних закупівель під час воєнного стану” (Постанова КМУ № 1275 від 11.11.2022), які прийшли на заміну “Деяким питанням здійснення оборонних закупівель товарів, робіт і послуг в умовах воєнного стану” (Постанова КМУ № 169 від 28.02.2022). Зауважимо, що згідно вимог Постанови №169 на час воєнного стану оборонні й публічні закупівлі можна укладати без застосування будь-яких процедур, визначених законами “Про публічні закупівлі” та “Про оборонні закупівлі”. Тоді як, вимоги Постанови №1275 поступово виводять оборонні закупівлі у конкурентну площину майже до рівня до введення в дію воєнного стану. Разом з іншими пов’язаними нормативно-правовими актами, вимоги Постанови №1275 адаптують закупівельні правила до умов війни. Усі ці заходи покликані забезпечити своєчасне озброєння армії та запровадити цивільний контроль у зонах, де він раніше був обмеженим. Водночас практика показує, що ефективність впровадження цих механізмів залежить від реалізації на рівні міністерств і відомств сектору безпеки і оборони та рівня підготовки закупівельних фахівців.

З моменту прийняття Закону України “Про оборонні закупівлі”, сам закон та пов’язані з ним нормативно-правові акти, зокрема Постанова Кабінету Міністрів України №1275 від 11 листопада 2022 року, зазнали численних змін, особливо в умовах воєнного стану. Наприклад, Постанова №1275 зазнала дванадцяти змін до лютого 2025 року [32]. Постійна, швидка послідовність змін до регулювання оборонних закупівель, що підтверджується, наприклад, згаданими дванадцятьма змінами до Постанови №1275 до лютого 2025 року, висвітлює напругу між потребою в законодавчій стабільності та імперативом гнучкої адаптації в динамічному середовищі воєнного часу. Хоча це демонструє законодавчу чуйність, така плинність також може створювати адміністративні труднощі та невизначеність для закупівельних організацій та постачальників, потенційно впливаючи на ефективність та довгострокове планування. Ця постійна законодавча плинність становить значний інституційний виклик. Хоча вона необхідна для оперативності під час війни, вона підкреслює потребу в оптимізованих законодавчих процесах та чітких каналах комунікації для мінімізації збоїв. Слід зазначити, що у відповідності до останніх змін станом на 25.02.2025 року Постановою Кабінетом Міністрів України від 11.11.2022 року №1275 разом з вищезгаданими “Особливостями...” затверджено “Порядок визначення предмета закупівлі продуктів

харчування для ЗСУ” (доданий 09.05.2023); “Порядок закупівлі вітчизняних БПЛА та засобів РЕБ” (доданий 20.12.2024).

Хоча, Постанова №1275 скасувала “авральний” режим прямого укладення контрактів, запроваджений Постановою №169, і поетапно відновила контрольовану конкуренцію в оборонних закупівлях. Нині вона надає державним замовникам три рівні операційної гнучкості: використання стандартних відкритих або спрощених процедур у системі Prozorro, коли обставини це дозволяють; укладення прямих договорів виключно у разі чітко визначених форс-мажорних обставин або після безрезультатного проведення торгів; застосування спеціальних порядків для критично важливих сфер (постачання продуктів харчування, безпілотні авіаційні комплекси, засоби радіоелектронної боротьби) та для окремих уповноважених служб. Послідовні зміни до постанови розширювали або конкретизували ці механізми, водночас посилюючи вимоги до прозорості й безпекові запобіжники. Водночас після завершення воєнного стану виникне нагальна потреба в консолідації та стабілізації відповідної нормативної бази для забезпечення передбачуваності й розвитку сталої довгострокової оборонно-промислової системи, у якій буде збалансовано оперативну гнучкість і регуляторну визначеність.

Додаткової уваги потребує створення окремих закупівельних агенцій, які задовольняють потреби Збройних Сил та Міністерства оборони України, а саме державних підприємств у сфері управління Міністерства оборони України “Державний оператор тилу” (далі – ДП “ДОТ”) та “Агенція оборонних закупівель” (далі – ДП “АОЗ”). Закупівельні організації здійснюють закупівлі централізованим порядком та є службами державного замовника у сфері оборони за двома окремими напрямками, а саме: ДП “ДОТ” за тиловим напрямом та ДП “АОЗ” за напрямом закупівлі озброєння, військової та спеціальної техніки (ракет і боєприпасів, іншого військово-технічного майна і послуг тощо). Потребу у закупівлях формують Збройні Сили України (певні структури Генерального Штабу ЗСУ та командування ЗСУ) передають її до Департаменту політики закупівель МОУ (тепер Департаменту закупівель МОУ), який формує Перелік та обсяг закупівель за кожним напрямом та затверджує їх у Заступника Міністра оборони відповідального згідно розподілу обов’язків за цей напрям після погодження у Генеральному штабі ЗСУ. Затверджені Переліки є підставою для здійснення закупівель кожною окремою закупівельною службою за своїм напрямом.

Поява цих двох закупівельних агенцій дає можливість вести мову про те, що реформа оборонних закупівель в Україні супроводжується значними інституційними змінами, спрямованими на централізацію, професіоналізацію та підвищення ефективності закупівельних процесів. Створення ДП “ДОТ” та ДП “АОЗ” та передача їм функцій із закупівлі відповідно товарів, робіт та послуг за тиловим напрямом та напрямом ОВТ є спробою централізувати та професіоналізувати ці надскладні та чутливі процеси, відокремивши функцію формування політики закупівель, яка залишається за Міністерством оборони України, від безпосереднього укладання контрактів. Цей підхід відповідає рекомендаціям міжнародних партнерів, зокрема НАТО, щодо підвищення ефективності та підзвітності оборонних закупівель.

Варто зазначити, що діяльність ДП “ДОТ” та ДП “АОЗ” регламентується статутами підприємств, законом України “Про публічні закупівлі”, законом України “Про оборонні закупівлі”, Постановою КМУ №1275 та низкою інших нормативно-правових актів. Розглянемо коротко діяльність окремо кожної зі закупівельних організацій.

Так, ДП “ДОТ” було створено для забезпечення тилових потреб Збройних Сил України (ЗСУ), таких як харчування, речове майно та пально-мастильні матеріали. Місія вказаного підприємства – забезпечувати потреби ЗСУ, дозволяючи їм зосередитися на виконанні бойових завдань, з амбітною метою стати драйвером розвитку системи забезпечення за стандартами НАТО.

У своїй діяльності закупівельна агенція активно використовує електронну систему закупівель Prozorro для проведення тендерів. За 2024 рік, за даними моніторингу StateWatch, ДП “ДОТ” уклало контракти (після корекцій) на суму 90,5 млрд грн. [33] Агенція також впроваджує цифрові інструменти, такі як ІТ-платформа DOT-Chain для харчових процедур, що має на меті цифровізацію процесів постачання та контролю якості.

Активне впровадження цифрових інструментів, а також антикорупційних заходів (таких, як: перевірка посадових осіб Агенції на доброчесність, належна перевірка постачальників, управління конфліктом інтересів, автоматизація процесів, з метою мінімізації людського фактору) свідчить про намір побудувати більш прозору та підзвітну систему тилових закупівель, які історично були сферою підвищених корупційних ризиків. Однак, як свідчать результати моніторингу StateWatch за 2024 рік [33], ДП “ДОТ” стикається з низкою викликів. А саме це: проблеми з недосконалими технічними специфікаціями, що обмежують конкуренцію (наприклад, у закупівлях військового взуття, де домінувала одна компанія), неуспішні закупівлі бронежилетів через орієнтацію на цінову пропозицію одного виробника, неоптимальне розподілення великих обсягів товару на лоти, що сприяє концентрації закупівель, а також укладання прямих договорів за потенційно завищеними цінами (наприклад, закупівля пластикових фляг) [33]. Ці факти вказують на те, що сама по собі цифровізація та декларування антикорупційних намірів не вирішують усіх проблем. Необхідні системні зміни в підходах до планування закупівель, формування технічних завдань та лотів, а також посилення реального, а не формального контролю якості. Без комплексного підходу існує ризик, що ДП “ДОТ”, попри позитивні починання, може повторити помилки попередніх структур, відповідальних за тилове забезпечення.

В свою чергу, ДП “АОЗ” здійснює закупівлі за трьома основними напрямками: боєприпаси (артилерійські, танкові, реактивні снаряди, мінометні постріли тощо), БПЛА (камікадзе, розвідувальні, боєприпаси до них, засоби РЕБ) та військова техніка (танки, БМП, БТР, САУ, інженерна техніка тощо) [34].

Місія цієї Агенції, яка задекларована на її офіційній сторінці, полягає у “задоволенні потреби в озброєнні та техніці, щоб ЗСУ могли сфокусуватись на головній місії” [34], що є негайною, тактичною метою. Водночас, також на офіційній сторінці Міністерства Оборони України в розділі Закупівельна діяльність/ Агенція оборонних закупівель (АОЗ), наголошується на “формуванні ефективної системи закупівель озброєння, яка відповідає стандартам НАТО”, “співпраці зі світовими виробниками для укладання прямих контрактів” та “залученні українських виробників” [35]. Останні пункти вказують на довгострокову, стратегічну мету побудови стійкої, диверсифікованої та внутрішньо спроможної оборонно-промислової бази. Зосередження на безпілотних літальних апаратах (БПЛА) додатково ілюструє це, оскільки це галузь, що швидко розвивається, де вітчизняні інновації можуть дати значні стратегічні переваги. Цей подвійний фокус демонструє складне розуміння оборонних потреб у воєнний час. Йдеться не лише про придбання існуючого озброєння, а й про формування майбутнього оборонного ландшафту шляхом сприяння технологічним інноваціям та промислового потенціалу в Україні, зменшення довгострокової залежності та інтеграції у світові оборонні ринки на вигідних умовах.

Тому варто зауважити, що одним із помітних досягнень є значні фінансові зобов'язання перед українськими виробниками БПЛА. Станом на 16 квітня 2025 року Міністерство оборони, значною мірою завдяки зусиллям ДП “АОЗ”, спрямувало понад 104 мільярди гривень вітчизняним виробникам дронів у 2024-2025 роках. Агенція успішно уклала контракти з 76 українськими виробниками БПЛА, охоплюючи різні типи дронів, включаючи розвідувальні, ударні та дрони-камікадзе [36]. Ця ініціатива є основою ширшої стратегії України щодо технологічного переозброєння Збройних Сил та розвитку національного оборонного виробництва.

Варто відмітити, що ініціатива із БПЛА виходить за рамки простого придбання існуючого озброєння до активного формування та розвитку майбутніх військових спроможностей та промислового потенціалу України. Це пряма відповідь на вразливості, виявлені залежністю від зовнішніх ланцюгів постачання, та нагальну потребу у швидких, адаптивних інноваціях у сучасній війні. А відповідно, ініціатива підкреслює складне розуміння того, що оборонні витрати можуть служити подвійній меті: негайній військовій ефективності та довгостроковому національному економічному розвитку. Підтримуючи місцевих виробників, Україна не лише забезпечує свої негайні оборонні потреби, але й будує стійку, інноваційну оборонно-промислову базу, яка може сприяти післявоєнному відновленню та зменшити стратегічні залежності. Цей підхід позиціонує Україну як потенційного лідера в певних оборонних технологіях.

Нещодавні законодавчі зміни, такі як Постанова Кабінету Міністрів України №603 від 23 травня 2025 року, розширили фінансові можливості Агенції. Це дозволяє їй безпосередньо фінансувати ключові супутні послуги, такі як митні платежі, транспортно-експедиційні, логістичні, брокерські та агентські послуги, а також витрати, пов'язані з рахунками в іноземних банках [37].¹³ Ці розширені повноваження є важливими для оптимізації складних міжнародних закупівель та зменшення логістичних вузьких місць.

Однак, попри певні досягнення, діяльність ДП “АОЗ” супроводжується викликами. Зокрема, згадувалися публічні скандали та питання довіри до агенції, пов'язані, наприклад, зі зміною керівництва [38]. Ефективність АОЗ залежить не лише від її формального мандату та обсягів фінансування, але й від рівня прозорості внутрішніх процесів (наскільки це можливо для закупівель ОБТ), якості менеджменту, інституційної стійкості та здатності вибудовувати довірчі відносини з вітчизняними та міжнародними постачальниками. Вирішення цих питань є критичним для успішної роботи Агенції, особливо в контексті залучення міжнародної допомоги та уникнення корупційних ризиків.

Паралельно зі створенням потужних централізованих закупівельних агенцій ДП “АОЗ” та ДП “ДОТ”, в Україні відбувається процес розширення певної децентралізації оборонних закупівель. Наказом Міністерства оборони України № 111 від 1 березня 2023 року військові частини (установи, заклади) в системі МОУ були уповноважені на здійснення оборонних закупівель та укладення державних контрактів (договорів) на період дії правового режиму воєнного стану [39]. Для підтримки цього процесу Департамент політики закупівель Міністерства оборони України розробив методичні рекомендації щодо здійснення децентралізованих закупівель у військових частинах [40]. Військові частини можуть закуповувати широкий спектр товарів та послуг, як для забезпечення бойових (автомобілі, спецтехніка тощо) так і небойових потреб, наприклад, канцелярське приладдя, дрібний ремонт, окремі види обладнання.

Такий підхід відображає спробу знайти оптимальну модель, яка б поєднувала переваги централізації (економія на масштабі, професіоналізація для складних та великих закупівель, єдині стандарти) та децентралізації (оперативність, гнучкість, краще врахування специфічних потреб на місцях). Централізовані агенції, такі як ДП “АОЗ” та ДП “ДОТ”, фокусуються на стратегічних та великомасштабних закупівлях (ОБТ, ПММ, централізоване постачання харчування та речового майна), тоді як військові частини отримують можливість самостійно та швидко задовольняти свої менш масштабні, але нагальні потреби. Хоча централізація може підвищити ефективність та контроль для великомасштабних, стратегічних закупівель, подібно до функцій Агенції НАТО з підтримки та закупівель (NATO Support and Procurement Agency, NSPA) або Агенції НАТО з питань зв'язку та інформації (NATO Communications and Information Agency, NCIA), вона створює нові виклики, пов'язані з координацією, потенційним дублюванням та підтримкою нагляду за децентралізованими компонентами.

Тобто, така гібридна модель створює низку викликів. По-перше, це питання координації між центральними агенціями та військовими частинами, щоб уникнути дублювання закупівель або придбання несумісних товарів. По-друге, виникає проблема контролю за децентралізованими закупівлями, оскільки на рівні окремих частин може бути менше зовнішнього нагляду, що підвищує корупційні ризики. По-третє, існує питання достатності професійної підготовки у сфері закупівель у персоналу військових частин. Запуск спеціалізованих навчальних курсів, як-от ті що провадять у Національному університеті оборони України, також є онлайн курс у застосунку “Армія+” [41], свідчить про визнання цієї проблеми та спроби її вирішити. Успіх децентралізованих закупівель залежатиме від чіткого розмежування повноважень, ефективної системи навчання закупівельників на місцях та впровадження дієвих механізмів контролю, що запобігатимуть фрагментації системи та зловживанням.

NSPA є централізованою закупівельною системою НАТО, відповідальною за логістику, підтримку та придбання товарів і послуг оборонного призначення. Рамки закупівель НАТО є децентралізованими, з кількома агенціями, що обробляють закупівлі відповідно до своїх мандатів, такими як NSPA, Агенція НАТО з питань зв'язку та інформації (NCIA) та Інвестиційний комітет НАТО (NATO Investment Committee, NIC) [42]. Важливо розуміти, що закупівлі НАТО здійснюються різними суб'єктами (включно з усіма вище переліченими агенціями НАТО) за дорученням НАТО. Немає центральної організації, яка б відповідала за закупівлі. Існує багато джерел фінансування НАТО для різних типів проєктів, але більшість проєктів капітальних інвестицій, які реалізує НАТО, фінансуються Програмою безпеки та інвестицій НАТО (NSIP) [43]. Тобто, наприклад, кораблі, літаки, танки або системи озброєнь країни-члени закуповують самостійно. В свою чергу і Україна зберігає суверенну відповідальність за більшість своїх оборонних закупівель, тоді як співпраця з НАТО стосується специфічних, спільно фінансованих потреб та стандартизації. Зазначене вказує, що хоча Україна прагне до інтеграції, вона все ще несе основний тягар національної оборони та її фінансування. Міжнародна допомога та співпраця є доповненням, а не повною заміною національних зусиль.

Принцип “витрати лягають там, де вони виникають” (costs lie where they fall) означає, що кожна країна залишається відповідальною за національні закупівлі озброєння та військової техніки для своїх військ. Спільне фінансування НАТО (Military Common Funding), що включає Військовий бюджет (операційні та експлуатаційні витрати) та Програму безпекових інвестицій НАТО (NSIP) для капітальних інвестицій, використовується для закупівлі “мінімально необхідних військових потреб” (Minimum Military Requirement – MMR). [43]

Окрім прямих механізмів співпраці, важливу роль відіграє форум UDCG NADs (Ukraine Defense Contact Group National Armaments Directors). Заснований у вересні 2022 року, цей форум зосереджений на прискоренні поставок озброєнь в Україну шляхом синхронізації міжнародних зусиль із закупівель, виробництва та підтримки. Він сприяв розширенню виробничих потужностей критично важливих боєприпасів у світі [44]. Цей форум додатково підкреслює спільний, синхронізований підхід до розширення оборонно-промислової бази.

Підводячи підсумки проведеного аналізу розглянемо зведені дані щодо нормативно-правових змін у закупівельній сфері України та їх відповідність міжнародним стандартам (дивись таблиця 1).

Таблиця.1. Ключові нормативно-правові зміни у публічних та оборонних закупівлях України (2015-2025) та їх вплив на відповідність міжнародним стандартам*

Рік/ період	Назва нормативно- правового акту/ подія	Ключові зміни/ нововведення	Вплив на публічні закупівлі	Вплив на оборонні закупівлі	Відповідність міжнародним стандартам (ЄС, НАТО, COT GPA, США)
2015	Закон України “Про публічні закупівлі” № 922-VIII від 25.12.2015	запровадження єдиної електронної системи Prozorro, обов’язкове використання для порогових закупівель, детальна регламентація процедур, скорочення неконкурентних процедур	фундаментальна реформа, підвищення прозорості, конкуренції, економії	непрямий вплив через загальні принципи прозорості	часткова відповідність принципам Директиви ЄС 2014/24/ЄС; потрібні додаткові зміни для повної гармонізації (реалізовано 2019 року); підготовка до GPA
травень 2016	приєднання України до Угоди COT про державні закупівлі (GPA)	відкриття ринків державних закупівель для українських та іноземних компаній; заборона офсетів	посилення конкуренції, залучення іноземних постачальників	застосовується за винятком для “істотних інтересів безпеки” (зброя, боєприпаси)	висока відповідність GPA, винятки для оборонних закупівель (безпека); необхідність подальших оборонних реформ
2016 – 2020	гармонізація з Директивами ЄС (Угода про асоціацію) Внесення низки змін у Закон України “Про публічні закупівлі” та пов’язані з ним, підзаконні акти, підписання Закону України “Про концесію	імплементация принципів прозорості, недискримінації, конкурентності, електронних процедур, механізмів оскарження	системна інтеграція в європейський правовий та економічний простір	гармонізація з Директивою ЄС 2009/81/ЄС для оборонних закупівель	системна інтеграція стандартів ЄС для цивільних закупівель; затримка інтеграції оборонного сектора до 2020 року
липень 2020	Закон України “Про оборонні закупівлі” № 808-IX від 17.07.2020	заміна ДОЗ трирічним планом, гармонізація з Директивою ЄС 2009/81/ЄС,	непрямий вплив на загальну культуру прозорості	докорінна реформа, підвищення прозорості, конкуренції, запобігання	формальна відповідність Директиві ЄС 2009/81 та НАТО/США; затримки у

Рік/ період	Назва нормативно- правового акту/ подія	Ключові зміни/ нововведення	Вплив на публічні закупівлі	Вплив на оборонні закупівлі	Відповідність міжнародним стандартам (ЄС, НАТО, COT GPA, США)
		визначення ключових органів, дозвіл на співпрацю з NSPA та FMS		корупції в оборонному секторі	практичний реалізації
лютий – листопа д 2022	Постанова КМУ №169 від 28.02.2022	суттєве спрощення процедур на період воєнного стану, дозвіл на неконкурентні процедури та відтермінування оприлюднення інформації	максимальн е спрощення для оперативно сті	максимальне спрощення для оперативност і	тимчасове відхилення від міжнародних стандартів прозорості та конкуренції, виправдане форс- мажорними обставинами (виняток GPA для безпеки)
жовтень 2022 – червень 2025	Постанова КМУ №1178 від 12.10.2022 ("Особливості здійснення публічних закупівель...")	систематизація особливостей публічних закупівель під час воєнного стану, зниження порогів для конкурентних процедур, "відкриті торги з особливостями", розширення Prozorro Market (30 змін, які були викликані необхідністю адаптації до швидких змін в умовах введення бойових дій та вимог міжнародних партнерів)	поступове повернення до конкурент- них процедур, але з гнучкістю	не застосовуєтьс я (замінена для оборонних закупівель, за винятком певних відсилок у ПКМУ №1275)	часткове повернення до стандартів ЄС/GPA, адапованих до воєнного стану; потребує уточнення щодо нестабільності правил
листопа д 2022 – червень 2025	Постанова КМУ №1275 від 11.11.2022 ("Особливості здійснення оборонних закупівель...")	заміна Постанови №169 для оборонних закупівель, поступове відновлення контрольованої конкуренції, три рівні операційної гнучкості;	не застосовує- ться (замінила №169 для оборонних).	поступове повернення до конкуренції, але з гнучкістю та спеціальними порядками для	часткове повернення до конкуренції, з обмеженням прозорості; потребує посилення анти- корупційних заходів

Рік/ період	Назва нормативно- правового акту/ подія	Ключові зміни/ нововведення	Вплив на публічні закупівлі	Вплив на оборонні закупівлі	Відповідність міжнародним стандартам (ЄС, НАТО, COT GPA, США)
		12 змін, які також були викликані необхідністю адаптації аналогічно Постанові №1178		критичних сфер	
червень 2022 – грудень 2023	створення ДП “Агенція оборонних закупівель” (АОЗ) та ДП “Державний оператор тилу” (ДОТ)	централізація та професіоналізація закупівель за напрямами (ОВТ та тилове забезпечення)	непрямий вплив на загальну ефективність системи	підвищення ефективності та підзвітності оборонних закупівель	відповідає рекомендаціям НАТО щодо професіоналізації, але злиття агенцій потребує подальших оцінок; важливість наглядових рад
березень 2023	наказ МОУ №111 від 01.03.2023 (розширення кола установ (організацій тощо), які застосовують вимоги ПКМУ №1275 у закупівельній діяльності)	уповноваження військових частин на здійснення оборонних закупівель	непрямий вплив на загальну гнучкість	забезпечення оперативності і та гнучкості на місцях для менш масштабних потреб	децентралізація; ризики через недостатній контроль та підзвітність на місцях

*Джерело: сформовано автором на основі [20, 27, 30, 32, 39, 45, 46, 47].

Тобто, що ми бачимо з цієї таблиці: по-перше, що починаючи з 2015 року Україна поступово намагається наблизити закупівельне законодавство у публічному секторі до міжнародних вимог, це і директиви ЄС і Модельний закон ЮНСІТРАЛ як один міжнародних орієнтирів у сфері закупівель. Так, прийнятий закон у 2015 році у цілому відповідав його духу (відкриті торги як основний метод, чіткі правила оскарження, публічність інформації);

після цього відбувається логічне просування по курсу на інтеграцію в світову економіку, закріпленого Угодою про асоціацію з ЄС, шляхом до єднання до Угоди СОТ, також врегулювання законодавчої бази у сфері концесій, як однією із складових питань, пов'язаних із врегулюванням сфери публічних закупівель відповідно до директив ЄС щодо закупівель. У жовтні 2019 році був підписаний Закон України “Про концесію”, який був створений з метою наближення законодавства до основних принципів здійснення концесій та державно-приватного партнерства до вимог міжнародних стандартів. На цьому етапі відбувається імплементація вимог директив ЄС (2014/24/ЄС, 2014/25/ЄС про закупівлі, 2014/23/ЄС про концесії);

але сектор безпеки і оборони (закупівля специфічних товарів робіт і послуг оборонного призначення) все ж такі залишається поза увагою реформ, і ось нарешті у липні 2020 року

з'являється новий закон у сфері оборонних закупівель, який кардинально змінює правила гри у цій сфері з метою імплементації вимог Директиви ЄС 2009/81/ЄС. Водночас, варто зазначити, що первинно закон мав набути чинності з січня 2021 року, але через неготовність системи його повноцінне впровадження відклали на пів року. Це означає, що попри формальну відповідність міжнародним стандартам, на практиці у 2020 року оборонні тендери ще не одразу стали прозорими – знадобився перехідний період і навчання персоналу. Крім того, інтеграція з механізмами НАТО та США вимагала часу: хоча Україна приєдналася до NSPA ще у 2016 році, перші спроби реальних закупівель через цю систему відбулися лише наприкінці 2019 році. Перехід на нові вимоги у сфері оборонних закупівель потребував створення та належного фінансування уповноваженого органу з планування оборонних закупівель (Міністерство з питань стратегічних галузей промисловості України), навчання персоналу, розробка стандартів прозорості для некласифікованих контрактів, які стали завданнями майбутнього періоду на той час;

далі успішне торування на шляху до Євроінтеграції у закупівельній сфері було перервано повномасштабним вторгненням російської федерації на територію України, як наслідок введенням воєнного стану та змінами у законодавчому полі цієї сфери, що призвело до “замороження” принципів прозорості на певний час, але поступово ситуація почала виправлятися, особливо з появою Постанови №1178, а потім Постанови №1275. Хоча варто зазначити, що після прийняття Постанови №1275 значна частина оборонних контрактів лишалася закритою для широкого оприлюднення (через питання секретності і безпеки). У країнах НАТО теж є практика засекречування закупівель у особливий період, але водночас існують жорсткі внутрішні антикорупційні запобіжники. Чи були вони впроваджені в Україні – питання дискусійне. Тому теза про “баланс між прозорістю та оперативністю” правильна як намір, але на практиці в 2022–2023 роках цей баланс часто схилявся в бік оперативності за рахунок прозорості. Все ж таки Постанова №1275, у більшості своєї, вирішувала процедурні питання, але інституційна спроможність закупівельників у військовий час залишалася викликом. Варто згадати, що стандарти НАТО у сфері оборонних закупівель передусім передбачають професіоналізацію персоналу, планування потреб та контролінг;

створення спеціалізованих державних підприємств зі закупівельної діяльності у сфері управління Міністерства оборони України – є кроком до централізації та професіоналізації оборонних закупівель. Це відповідає найкращим міжнародним практикам: у багатьох країнах НАТО існують централізовані агенції, що займаються закупівлями для військових, мають фахових експертів та налагоджені процеси (аналог – Агентство оборонних закупівель (Defence Equipment and Support, DE&S) у Великій Британії, Агентство оборонної логістики (Defense Logistics Agency, DLA) у США тощо). Водночас варто згадати подальший розвиток ситуації, щоб повніше оцінити відповідність міжнародним стандартам. У 2023–2024 роках представники НАТО радили Україні не поспішати з об'єднанням цих двох агенцій принаймні на час війни. Заява місії НАТО в Україні у жовтні 2024 року наголосила, що ДП “АОЗ” та “ДОТ” доцільно залишити окремими, аби зберегти фокус та незалежність кожної, а також щоб запровадити наглядові ради для підвищення прозорості;

далі вимоги особливого періоду потребували розширення кола замовників у сфері оборони, коли централізовані структури не встигали закривати всі запити на місцях, і хоча новий наказ Міністерства оборони України у березні 2023 року зробив, це варто згадати і потенційні ризики. Так, децентралізація без належного контролю призводить до дублювання закупівель або нераціонального витрачання коштів. У стандартах НАТО наголошується на навченості та підзвітності офіцерів, які здійснюють закупівлі. В умовах 2023 року далеко не всі військові частини мали досвідчених закупівельників, що збільшує ризик помилок або зловживань наразі ситуація все ж таки залишається складною та невирішеною, проблемою

залишається штатна посада уповноваженого з закупівель в окремих військових частина та органах військового управління та належна підготовка цих осіб.

На додачу до розглянутих нормативно-правових актів у таблиці 1 варто згадати проєкт Закону України “Про публічні закупівлі” від 23.08.2024 №11520 (законопроект) [48], який є стратегічною ініціативою, спрямованою на повне перезавантаження системи публічних закупівель та її глибоку гармонізацію з директивами ЄС після завершення воєнного стану. До його позитивних аспектів належить впровадження нових гнучких інструментів (інноваційне партнерство, динамічна система закупівель), підвищення вартісних порогів для обов’язкових конкурентних торгів, розширення використання Prozorro Market та закріплення успішних практик воєнного часу, наприклад, так зване “правило 24 годин”. Водночас документ містить суттєві ризики: скасування норми про мінімальну 70% вагу цінового критерію може призвести до суб’єктивізму, а надання Державній аудиторській службі України права блокувати платежі за договорами створює значні корупційні ризики та загрозу для виконання контрактів. Таким чином, законопроект є важливим кроком на шляху до євроінтеграції, але потребує ретельного доопрацювання для усунення ідентифікованих загроз.

Слід підсумувати, що після 2022 року, коли вже відбулося остаточне розділення нормативно-правового регулювання у сфері публічних та оборонних закупівель, нормативно-правова база у сфері закупівель розвивалась за двома паралельними напрямками. Перший – це тактичне, адаптивне регулювання в умовах воєнного стану, що реалізовувалося через численні точкові зміни до Постанови КМУ №1178. Ці зміни були спрямовані на вирішення нагальних проблем: було збільшено строки подання пропозицій на будівельні роботи для підвищення конкуренції, запроваджено механізми захисту чутливої інформації, розширено підстави для укладення прямих договорів для потреб оборони та енергетики. Водночас, для збалансування цих послаблень, було посилено вимоги до прозорості: запроваджено обов’язкове структурування тендерної документації через окремі додатки та обов’язкове оприлюднення договорів і обґрунтувань для всіх прямих закупівель з 1 вересня 2024 року, включно з механізмом відкладеної публікації для найчутливіших контрактів.

Другий напрям – це фундаментальна інституційна реформа оборонних закупівель, що стала відповіддю на корупційні ризики та неефективність. Ключовою подією стало повноцінне розгортання роботи двох спеціалізованих агенцій: ДП “Державного оператора тилу” (ДОТ), відповідального за нелетальне забезпечення (харчування, одяг, ПММ), та ДП “Агенції оборонних закупівель” (АОЗ), що займається озброєнням та військовою технікою. Ця модель покликана відокремити функцію формування політики від безпосередньої закупівлі, що є стандартом НАТО. Паралельно було законодавчо врегульовано питання прибутку в неконкурентних оборонних контрактах, щоб усунути суперечливу практику, коли будь-який прибуток виробника трактувався як збитки держави.

Висновки

В статті було проаналізовано трансформацію державної політики у сфері закупівель, зокрема змін у нормативно-правовій базі щодо публічних та оборонних закупівель, впливу міжнародних стандартів (ЄС, США, НАТО), а також визначено основні інституційні та нормативні виклики, з якими стикається Україна в цій сфері. За результатами аналізу сформульовано такі висновки:

державна політика у сфері публічних та оборонних закупівель України пройшла значний шлях реформування, наближаючись до міжнародних стандартів ЄС, НАТО та COT GPA. Основними досягненнями стали впровадження системи Prozorro, приєднання до Угоди GPA, ухвалення спеціальних законів про публічні та оборонні закупівлі, а також створення спеціалізованих закупівельних агенцій ДП “ДОТ” і ДП “АОЗ”;

військовий конфлікт та введення воєнного стану у 2022 році змусили державу перейти на спрощені процедури, що негативно вплинуло на прозорість та конкуренцію у закупівлях. Проте поступово було відновлено контрольовану конкуренцію, хоч і з певними обмеженнями;

постійні зміни до нормативно-правових актів, особливо Постанов №1178 та №1275, свідчать про гнучкість системи, але водночас створюють додаткові адміністративні труднощі й невизначеність для замовників та постачальників;

створення спеціалізованих державних агенцій відповідає міжнародним стандартам професіоналізації закупівель, однак їх ефективність залежить від прозорості процесів, якості управління та контролю за виконанням контрактів;

підвищення рівня децентралізації закупівель військовими частинами створює додаткові можливості для оперативності, але потребує посилення контролю та підвищення кваліфікації персоналу для зменшення корупційних ризиків.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Балан А. А., Буковський Д. А. Електронна система “Prozorro” як революція в системі публічних закупівель в Україні. Економіка та суспільство. 2021. №4. URL : <https://economics.net.ua/files/archive/2021/No4/16.pdf> (дата звернення: 15.05.2025).
2. Лаговська О.А., Легенчук С.Ф., Свірко С.В. Державні закупівлі в Україні: аналіз переваг і недоліків. Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. 2021. Вип. 2 (49). С. 56–60. [http://dx.doi.org/10.26642/pbo-2021-2\(49\)-56-60](http://dx.doi.org/10.26642/pbo-2021-2(49)-56-60) (дата звернення: 15.05.2025).
3. Шульган І., Слобода Н. Електронна система Prozorro як ефективний інструмент боротьби з корупцією. Вісник Національного університету “Львівська політехніка”. Серія: “Юридичні науки”. 2024. Том. 11. № 4 (44). С. 348-354. <https://doi.org/10.23939/law2024.44.348> (дата звернення 13.05.2025).
4. Річні звіти. Transparency International Ukraine, URL: <https://ti-ukraine.org/project/reports/> (дата звернення 13.05.2025).
5. Закупівлі відбудови: підсумки року та напрями удосконалення. Центр економічної стратегії. 28 травня 2025 року. URL : https://ces.org.ua/reconstruction_procurement_year_review/ (дата звернення: 15.05.2025).
6. Вплив Prozorro: яку реальну економію забезпечує електронна система. Центр вдосконалення закупівель KSE. 2022. URL : <https://cep.kse.ua/article/impact-of-prozorro/impact-of-prozorro.pdf> (дата звернення: 15.05.2025).
7. Оптимізація закупівельної діяльності: як вдосконалити підходи. Центр вдосконалення закупівель KSE. 2023. URL : <https://cep.kse.ua/article/optimization-of-procurement-activities-how-to-improve-approaches.pdf> (дата звернення: 15.05.2025).
8. За підтримки Євросоюзу ЦЕС та ІЕД провели аналіз закупівель з будівництва та відбудови, проведені державою у 2023 році. Центр економічної стратегії, Інститут економічних досліджень та політичних консультацій. 29.05.2024. URL : https://www.eeas.europa.eu/delegations/ukraine/за-підтримки-євросоюзу-цес-та-іед-провели-аналіз-закупівель-з-будівництва-та-відбудови-проведені_uk?s=232 (дата звернення: 15.05.2025).

9. Проект “Контроль витрат на відновлення”. Інститут економічних досліджень та політичних консультацій. URL : http://www.ier.com.ua/ua/Recovery_Spending_Watchdog (дата звернення: 15.05.2025).
10. НАЗК визначило 25 типових корупційних ризиків у публічних закупівлях, дата последнего обращения: URL : <https://nazk.gov.ua/uk/nazk-vyznachylo-25-typovyh-koruptsiinyh-ryzykiv-u-publichnyh-zakupivlyah/> (дата звернення 15.05.2025).
11. Корупційні ризики під час здійснення оборонних закупівель. Національне агентство з питань запобігання корупції. URL : <https://radnuk.com.ua/pravova-baza/koruptsiini-ryzyky-pid-chas-zdiysnennia-oboronnykh-zakupivel/> (дата звернення: 15.05.2025).
12. Звіт про результати аналізу щорічного звіту Міністерства економіки України, що містить аналіз функціонування системи публічних закупівель (щодо кількісних і вартісних показників закупівель у розрізі процедур і предметів закупівель, рівня конкуренції, кількості скарг) та узагальнену інформацію про результати здійснення контролю у сфері закупівель за 2023 рік. Рахункова палата України. 2024. URL : https://rp.gov.ua/upload-files/Activity/Collegium/2024/35-6_2024/Zvit_35-6_2024.pdf (дата звернення: 15.05.2025).
13. Доповідь з питань оборонних закупівель. Центр оборонних стратегій. Червень 2021. URL : <https://defence.org.ua/wp-content/uploads/doslidzhennya/CDS-Dopovid-z-pytan-oboronnykh-zakupivel-ukr.pdf> (дата звернення: 15.05.2025).
14. Стратегічний огляд оборонних закупівель Україна-НАТО. URL : <https://www.army-pro.com/wp-content/uploads/2024/10/strategichnyi-oglyad-oboronnyh-zakupivel-ukrayina-nato.pdf>
15. Аналіз виконання Стратегічного огляду оборонних закупівель Україна-НАТО. StateWatch. 03.04.2025. URL : <https://statewatch.org.ua/publications/analiz-vykonannia-stratehichnoho-ohliadu-oboronnykh-zakupivel-ukraina-nato/> (дата звернення: 15.05.2025).
16. Пантелеймоненко А., Мілька А. і Павленко О. Публічні закупівлі в Україні в умовах воєнного стану. Економіка та суспільство. 2023. вип. 51 (травень). <https://doi.org/10.32782/2524-0072/2023-51-20>.
17. Петик, Л. О., і І. В. Бацман. Публічні закупівлі в умовах воєнного стану. Проблеми сучасних трансформацій. Серія: економіка та управління. 2023. вип. 9 (вересень). <https://doi.org/10.54929/2786-5738-2023-9-08-03>.
18. Запорожець, С., Жежерун, Ю., Зелений, П., Колесник, В., Бритов, Д. і Заєць, М. Трансформація системи оборонних закупівель під впливом потреб воєнного стану. Випробування та сертифікація. 2023. №2(2), С. 82-96. <https://doi.org/10.37701/ts.02.2023.10>.
19. Новий звіт Єврокомісії щодо України: як вона оцінила наші публічні закупівлі. 2 Листопада, 2024. URL : <https://ti-ukraine.org/news/novyj-zvit-yevrokomisiyi-shhodo-ukrayiny-yak-vona-otsynyla-nashi-publichni-zakupivli/> (дата звернення: 15.05.2025).
20. Про публічні закупівлі: Закон України від 25 грудня 2015 року №922-VIII. URL : <https://zakon.rada.gov.ua/laws/show/922-19/print> (дата звернення 13.05.2025)
21. Президент підписав Закон “Про публічні закупівлі”. URL : <https://www.prostir.ua/?news=prezydent-pidpysav-zakon-pro-publichni-zakupivli>
22. Реформа державних закупівель. URL : <https://me.gov.ua/Documents/Detail?lang=uk-UA&id=38c083f3-2571-466a-9583-3b43c2804ad9&title=ReformaDerzhavnikhZakupivel> (дата звернення 13.05.2025)
23. Про нас. Історія Prozorro. URL : <https://prozorro.gov.ua/about> (дата звернення 13.05.2025)
24. Україна офіційно приєдналася до Угоди COT про державні закупівлі (GPA). URL : <https://me.gov.ua/News/Detail?lang=uk->

- [UA&title=UkrainaOfitsiinoPridnalasiaDoUgodiSotProDerzhavniZakupivli-gpa-&isSpecial=true&showMenuTree=true](#) (дата звернення: 29.05.2025).
25. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement. URL : <https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng> (дата звернення: 29.05.2025).
26. The official site of U.S. International Trade Administration (2024), “Selling to the public sector”, URL : <https://www.trade.gov/country-commercial-guides/eu-selling-public-sector> (Accessed 20 June 2025).
27. Про затвердження особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України “Про публічні закупівлі”, на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування : Постанова Кабінету Міністрів України від 12 жовтня 2022 року № 1178. URL : <https://zakon.rada.gov.ua/laws/show/1178-2022-%D0%BF> (дата звернення: 16.05.2025).
28. Куц А., Русіна К., Швадчак А. Публічні закупівлі 2023 : чим жила і як змінювалась сфера : аналітичний звіт; Transparency International Ukraine. Київ : Transparency International Ukraine, 2024. 28 с. URL : <https://ti-ukraine.org/wp-content/uploads/2024/05/Publichni-zakupivli-2023-v3.pdf> (дата звернення: 16.05.2025).
29. Панасюк О. В. Особливості визначення процедури закупівлі при здійсненні публічних закупівель в умовах воєнного стану. Юридична Україна. 19.03.2025. [https://doi.org/10.37749/2308-9639-2025-2\(265\)-5](https://doi.org/10.37749/2308-9639-2025-2(265)-5).
30. Про оборонні закупівлі: Закон України від 17 липня 2020 року № 808-IX. URL : <https://zakon.rada.gov.ua/laws/show/808-20#Text>. (дата звернення 12.05.2025).
31. Про порядок планування, формування, розміщення, контролю та звітування про оборонні закупівлі : Постанова Кабінету Міністрів України від 3 березня 2021 року № 363. URL : <https://zakon.rada.gov.ua/laws/show/363-2021-%D0%BF>. (дата звернення: 05.06.2025).
32. Про деякі питання здійснення оборонних закупівель на період дії правового режиму воєнного стану : Постанова Кабінету Міністрів України від 11 листопада 2022 року № 1275. URL : <https://zakon.rada.gov.ua/laws/show/1275-2022-%D0%BF>. (дата звернення: 05.06.2025).
33. Моніторинг закупівель ДОТ за 2024 рік: аналіз, виклики, рекомендації. 15.05.2025. URL : <https://statewatch.org.ua/publications/monitorynh-zakupivel-dot-za-2024-rik-analiz-vyklyky-rekomendatsii/> (дата звернення 11.06.2025).
34. Про нас “Агенція оборонних закупівель” Міністерства оборони – національна агенція, що забезпечує боєприпаси, БПЛА та техніку для потреб ЗСУ. URL : <https://dpa.mod.gov.ua/about-us> (дата звернення 11.06.2025).
35. Закупівельна діяльність. URL : <https://mod.gov.ua/diyalnist/zakupivelnadiyalnist> (дата звернення 11.06.2025).
36. Агенція оборонних закупівель уклала контракти з 76 виробниками БПЛА – Рустем Умеров. 16 квітня 2025. URL : <https://armyinform.com.ua/2025/04/16/agencziya-oboronnyh-zakupivel-uklala-kontrakty-z-76-vyrobnykamy-bpla-rustem-umyerov/> (дата звернення 10.06.2025).
37. Про внесення змін до Порядку використання державним підприємством Міністерства оборони України “Агенція оборонних закупівель” коштів, передбачених у державному бюджеті для здійснення закупівель товарів, робіт і послуг оборонного призначення: постанова Кабінету Міністрів України від 23 травня 2025 р. №603. URL : <https://www.kmu.gov.ua/npas/pro-rzhavnomu-biudzheti-dlia-zdiisnennia-zakupivel-tovariv-robit-i-posluh-obhennia-i-603> (дата звернення 10.06.2025).

38. Аналіз виконання Стратегічного огляду оборонних закупівель Україна-НАТО. 03.04.2025. URL : <https://statewatch.org.ua/publications/analiz-vykonannia-stratehichnoho-ohliadu-oboronnykh-zakupivel-ukraina-nato/> (дата звернення 10.06.2025).
39. Про уповноваження військових частин (установ, закладів) в системі Міністерства оборони України на здійснення оборонних закупівель та укладення державних контрактів (договорів) на період дії правового режиму воєнного стану: Наказ Міністерства оборони України від 01.03.2023 № 111/нм. URL : <https://lexinform.com.ua/militarylex/nakaz-111-nm-vid-01-03-2023-pro-upovnovazhennya-viiskovyh-chastyn-ustanov-zakladiv-v-systemi-ministerstva-oborony-ukrayiny-na-zdiysnennya-oboronnykh-zakupivel-ta-ukladennya-derzhavnyh-kontraktiv-dogovo/> (дата звернення 12.06.2025).
40. Міноборони розробило нові методичні рекомендації для закупівельників у військових частинах. 27 грудня 2024. URL : <https://mod.gov.ua/news/minoboroni-rozrobilo-novi-metodichni-rekomendaciyi-dlya-zakupivelnikiv-u-viiskovih-chastinah> (дата звернення 12.06.2025).
41. В Армія+ стартував найбільший навчальний курс про оборонні закупівлі. 14 травня 2025. URL : <https://mod.gov.ua/news/v-armiya-startuvav-najbilshij-navchalnij-kurs-pro-oboronni-zakupivli> (дата звернення 12.06.2025).
42. The official site of White & Case LLP (2025), “Navigating NATO Procurement: Legal and Regulatory Considerations for Companies in Finland & Sweden”, URL : <https://www.whitecase.com/insight-alert/navigating-nato-procurement-legal-and-regulatory-considerations-companies-finland> (Accessed 20 June 2025).
43. The official site of GOV.UK (2024), “Navigating NATO Procurement”, URL : <https://www.gov.uk/government/publications/navigating-nato-procurement/navigating-nato-procurement> (Accessed 20 June 2025).
44. The official site of U.S. Department of Defense (2025), “Fact Sheet on Efforts of Ukraine Defense Contact Group National Armaments Directors”, URL : <https://www.defense.gov/News/Releases/Release/Article/4026238/fact-sheet-on-efforts-of-ukraine-defense-contact-group-national-armaments-direc/> (Accessed 20 June 2025).
45. Про концесію: Закон України від 3 жовтня 2019 року №155-IX. URL : <https://zakon.rada.gov.ua/laws/show/155-20#Text> (дата звернення 13.05.2025)
46. Деякі питання здійснення оборонних закупівель товарів, робіт і послуг в умовах воєнного стану : Постанова Кабінету Міністрів України від 28 лютого 2022 року №169. URL : <https://zakon.rada.gov.ua/laws/show/169-2022-%D0%BF#Text> (дата звернення 20.06.2025).
47. Деякі питання здійснення оборонних закупівель службою державного замовника : Постанова Кабінету Міністрів України від 16 травня 2023 року №494. URL : <https://zakon.rada.gov.ua/laws/show/494-2023-%D0%BF#Text> (дата звернення 20.06.2025).
48. Проект Закону про публічні закупівлі від 23.08.2024 №11520. URL : <https://itd.rada.gov.ua/billInfo/Bills/Card/44788> (дата звернення 20.06.2025).

References

1. Balan, A. A., & Bukovskyi, D. A. (2021). Elektronna systema Prozorro yak revoliutsiia v systemi publichnykh zakupivel v Ukraini [The Prozorro electronic system as a revolution in Ukraine’s public procurement system]. *Ekonomika ta suspilstvo*, (4). Retrieved May 15, 2025, Available from : <https://economics.net.ua/files/archive/2021/No4/16.pdf>
2. Lahovska, O. A., Lehenchuk, S. F., & Svirko, S. V. (2021). Derzhavni zakupivli v Ukraini: analiz perevah i nedolikiv [Public procurement in Ukraine: analysis of advantages and

- disadvantages]. Problemy teorii ta metodologii bukhalterskoho obliku, kontroliu i analizu, (2(49)), 56–60. [https://doi.org/10.26642/pbo-2021-2\(49\)-56-60](https://doi.org/10.26642/pbo-2021-2(49)-56-60)
3. Shulhan, I., & Sloboda, N. (2024). Elektronna systema Prozorro yak efektyvnyi instrument borotby z koruptsiieiu [The Prozorro electronic system as an effective tool against corruption]. Visnyk Natsionalnoho universytetu "Lvivska politehnika", Seriya: Yurydychni nauky, 11(4(44)), 348–354. <https://doi.org/10.23939/law2024.44.348>
4. Transparency International Ukraine. (2025). Richni zvity [Annual reports]. Retrieved May 13, 2025, Available from : <https://ti-ukraine.org/project/reports/>
5. Tsentralna ekonomichna stratehiya. (2025, May 28). Zakupivli vidbudovy: pidsumky roku ta napriamy udoskonalennia [Reconstruction procurement: year summary and improvement directions]. Retrieved May 15, 2025, Available from : https://ces.org.ua/reconstruction_procurement_year_review/
6. KSE. (2022). Vplyv Prozorro: yaku realnu ekonomiiu zabezpechuie elektronna systema [The impact of Prozorro: real savings provided by the electronic system]. Retrieved May 15, 2025, Available from : <https://cep.kse.ua/article/impact-of-prozorro/impact-of-prozorro.pdf>
7. KSE. (2023). Optymizatsiia zakupivelnoi diialnosti: yak vdoskonalaty pidkhody [Optimization of procurement activities: how to improve approaches]. Retrieved May 15, 2025, Available from : <https://cep.kse.ua/article/optimization-of-procurement-activities-how-to-improve-approaches.pdf>
8. Tsentralna ekonomichna stratehiya, & Instytut ekonomichnykh doslidzhen ta politychnykh konsultatsii. (2024, May 29). Za pidtrymky Yevrosoiuzu TsES ta IED provely analiz zakupivel z budivnytstva ta vidbudovy, provedeni derzhavoiu u 2023 rotsi [With EU support, CES and IER conducted an analysis of construction and reconstruction procurements conducted by the state in 2023]. Retrieved May 15, 2025, Available from : https://www.eeas.europa.eu/delegations/ukraine/за-підтримки-євросоюзу-цес-та-іед-провели-аналіз-закупівель-з-будівництва-та-відбудови-проведені_uk?s=232
9. Instytut ekonomichnykh doslidzhen ta politychnykh konsultatsii. (2025). Proiekt "Kontrol vytrat na vidnovlennia" [Recovery Spending Watchdog project]. Retrieved May 15, 2025, Available from : http://www.ier.com.ua/ua/Recovery_Spending_Watchdog
10. NAZK. (2025). NAZK vyznachylo 25 typovykh koruptsiinykh ryzykiv u publichnykh zakupivliakh [NAZK identified 25 typical corruption risks in public procurement]. Retrieved May 15, 2025, Available from : <https://nazk.gov.ua/uk/nazk-vyznachylo-25-typovyh-koruptsiinyh-ryzykiv-u-publichnyh-zakupivlyah/>
11. Natsionalne ahentstvo z pytan zapobihannia koruptsii. (2025). Koruptsiini ryzyky pid chas zdiisnennia oboronnykh zakupivel [Corruption risks during defense procurement]. Retrieved May 15, 2025, Available from : <https://radnuk.com.ua/pravova-baza/koruptsiini-ryzyky-pid-chas-zdiisnennia-oboronnykh-zakupivel/>
12. Rakhunkova palata Ukrainy. (2024). Zvit pro rezultaty analizu shchorichnoho zvit Ministerstva ekonomiky Ukrainy za 2023 rik [Report on the results of the analysis of the Ministry of Economy's annual report for 2023]. Retrieved May 15, 2025, Available from : https://rp.gov.ua/upload-files/Activity/Collegium/2024/35-6_2024/Zvit_35-6_2024.pdf
13. Tsentralna ekonomichna stratehiya. (2021, June). Dopovid z pytan oboronnykh zakupivel [Report on defense procurement issues]. Retrieved May 15, 2025, Available from : <https://defence.org.ua/wp-content/uploads/doslidzhennya/CDS-Dopovid-z-pytan-oboronnykh-zakupivel-ukr.pdf>
14. Army Pro. (2024). Stratehichniy ohliad oboronnykh zakupivel Ukraina-NATO [Strategic Review of Defense Procurement Ukraine-NATO]. Available from : <https://www.army-pro.com/wp-content/uploads/2024/10/strategichnyi-oglyad-oboronnyh-zakupivel-ukrayina-nato.pdf>

15. StateWatch. (2025, April 3). Analiz vykonannia Stratehichnoho ohliadu oboronnykh zakupivel Ukraina-NATO [Analysis of the implementation of the Strategic Review of Defense Procurement Ukraine-NATO]. Retrieved May 15, 2025, Available from : <https://statewatch.org.ua/publications/analiz-vykonannia-stratehichnoho-ohliadu-oboronnykh-zakupivel-ukraina-nato/>
16. Panteleimonenko, A., Milka, A., & Pavlenko, O. (2023). Publichni zakupivli v Ukraini v umovakh voiennoho stanu [Public procurement in Ukraine under martial law]. *Ekonomika ta suspilstvo*, (51). <https://doi.org/10.32782/2524-0072/2023-51-20>
17. Petyk, L. O., & Batsman, I. V. (2023). Publichni zakupivli v umovakh voiennoho stanu [Public procurement under martial law]. *Problemy suchasnykh transformatsii. Seria: Ekonomika ta upravlinnia*, (9). <https://doi.org/10.54929/2786-5738-2023-9-08-03>
18. Zaporozhets, S., Zhezherun, Yu., Zelenyi, P., Kolesnyk, V., Brytov, D., & Zaiets, M. (2023). Transformatsiia systemy oboronnykh zakupivel pid vplyvom potreb voiennoho stanu [Transformation of the defense procurement system influenced by martial law requirements]. *Vyprovuvannia ta sertyfikatsiia*, 2(2), 82–96. <https://doi.org/10.37701/ts.02.2023.10>
19. Transparency International Ukraine. (2024, November 2). Novyi zvit Yevrokomisii shchodo Ukrainy: yak vona otsynyla nashi publichni zakupivli [New report of the European Commission on Ukraine: Assessment of public procurement]. Retrieved May 15, 2025, Available from : <https://ti-ukraine.org/news/novyj-zvit-yevrokomisiyi-shhodo-ukrayiny-yak-vona-otsynyla-nashi-publichni-zakupivli/>
20. Verkhovna Rada Ukrainy. (2015). Pro publichni zakupivli [On Public Procurement] (Law No. 922-VIII). Retrieved May 13, 2025, Available from : <https://zakon.rada.gov.ua/laws/show/922-19/print>
21. Prostir.ua. (n.d.). Prezydent pidpysav zakon "Pro publichni zakupivli" [The President signed the law "On Public Procurement"]. Available from : <https://www.prostir.ua/?news=prezydent-pidpysav-zakon-pro-publichni-zakupivli>
22. Ministry of Economy of Ukraine. (n.d.). Reforma derzhavnykh zakupivel [Public procurement reform]. Retrieved May 13, 2025, Available from : <https://me.gov.ua/Documents/Detail?lang=uk-UA&id=38c083f3-2571-466a-9583-3b43c2804ad9&title=ReformaDerzhavnikhZakupivel>
23. Prozorro. (n.d.). Pro nas. Istoriia Prozorro [About us. History of Prozorro]. Retrieved May 13, 2025, Available from : <https://prozorro.gov.ua/about>
24. Ministry of Economy of Ukraine. (2025, May 29). Ukraina ofitsiino pryednalasia do Uhody SOT pro derzhavni zakupivli (GPA) [Ukraine officially joined the WTO Agreement on Government Procurement (GPA)]. Available from : <https://me.gov.ua/News/Detail?lang=uk-UA&title=UkrainaOfitsiinoPridnalasiaDoUgodiSotProDerzhavniZakupivli-gpa-&isSpecial=true&showMenuTree=true>
25. European Parliament and Council. (2014). Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement. Retrieved May 29, 2025, Available from : <https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng>
26. U.S. International Trade Administration. (2024). Selling to the public sector. Retrieved June 20, 2025, Available from : <https://www.trade.gov/country-commercial-guides/eu-selling-public-sector>
27. Cabinet of Ministers of Ukraine. (2022, October 12). Pro zatverdzhennia osoblyvostei zdiisnennia publichnykh zakupivel tovariv, robit i posluh dlia zamovnykiv... [Resolution No. 1178]. Retrieved May 16, 2025, Available from : <https://zakon.rada.gov.ua/laws/show/1178-2022-%D0%BF>

28. Kuts, A., Rusina, K., & Shvadchak, A. (2024). Publichni zakupivli 2023: chym zhyla i yak zminiualas sfera [Public Procurement 2023: developments and changes]. Transparency International Ukraine. Retrieved May 16, 2025, Available from : <https://ti-ukraine.org/wp-content/uploads/2024/05/Publichni-zakupivli-2023-v3.pdf>
29. Panasniuk, O. V. (2025). Osoblyvosti vyznachennia protsedury zakupivli pry zdiisnenni publichnykh zakupivel v umovakh voiennoho stanu [Features of determining procurement procedures under martial law]. Yurydychna Ukraina. [https://doi.org/10.37749/2308-9639-2025-2\(265\)-5](https://doi.org/10.37749/2308-9639-2025-2(265)-5)
30. Verkhovna Rada Ukrainy. (2020). Pro oboronni zakupivli [On Defense Procurement] (Law No. 808-IX). Retrieved May 12, 2025, Available from : <https://zakon.rada.gov.ua/laws/show/808-20#Text>
31. Cabinet of Ministers of Ukraine. (2021, March 3). Pro poriadok planuvannia, formuvannia, rozmishchennia, kontroliu ta zvituvannia pro oboronni zakupivli [Resolution No. 363]. Retrieved June 5, 2025, Available from : <https://zakon.rada.gov.ua/laws/show/363-2021-%D0%BF>
32. Cabinet of Ministers of Ukraine. (2022, November 11). Pro deiaki pytannia zdiisnennia oboronnykh zakupivel... [Resolution No. 1275]. Retrieved June 5, 2025, Available from : <https://zakon.rada.gov.ua/laws/show/1275-2022-%D0%BF>
33. StateWatch. (2025, May 15). Monitorynh zakupivel DOT za 2024 rik: analiz, vyklyky, rekomendatsii [DOT procurement monitoring for 2024: analysis, challenges, recommendations]. Retrieved June 11, 2025, Available from : <https://statewatch.org.ua/publications/monitorynh-zakupivel-dot-za-2024-rik-analiz-vyklyky-rekomendatsii/>
34. Ahenziia oboronnykh zakupivel Ministerstva oborony Ukrainy. (n.d.). Pro nas [About us]. Retrieved June 11, 2025, Available from : <https://dpa.mod.gov.ua/about-us>
35. Ministerstvo oborony Ukrainy. (n.d.). Zakupivelna diialnist [Procurement activity]. Retrieved June 11, 2025, Available from : <https://mod.gov.ua/diialnist/zakupivelna-diialnist>
36. ArmyInform. (2025, April 16). Ahenziia oboronnykh zakupivel uklala kontrakty z 76 vyrobnykamy BPLA – Rustem Umierov [Defense Procurement Agency signed contracts with 76 UAV manufacturers – Rustem Umierov]. Retrieved June 10, 2025, Available from : <https://armyinform.com.ua/2025/04/16/agencziya-oboronnykh-zakupivel-uklala-kontrakty-z-76-vyrobnykamy-bpla-rustem-umyerov/>
37. Cabinet of Ministers of Ukraine. (2025, May 23). Pro vnesennia zmin do Poriadku vykorystannia koshtiv DP “Ahenziia oboronnykh zakupivel” [Resolution No. 603]. Retrieved June 10, 2025, Available from : <https://www.kmu.gov.ua/npas/pro-rzhavnomu-biudzheti-dlia-zdiisnennia-zakupivel-tovariv-robit-i-posluh-obhennia-i-603>
38. StateWatch. (2025, April 3). Analiz vykonannia Stratehichnoho ohliadu oboronnykh zakupivel Ukraina-NATO [Analysis of the implementation of the Strategic Review of Defense Procurement Ukraine-NATO]. Retrieved June 10, 2025, Available from : <https://statewatch.org.ua/publications/analiz-vykonannia-stratehichnoho-ohliadu-oboronnykh-zakupivel-ukraina-nato/>
39. Ministerstvo oborony Ukrainy. (2023, March 1). Pro upovnovazhennia viiskovykh chastyn (ustanov, zakladiv) na zdiisnennia oboronnykh zakupivel [Order No. 111/nm]. Retrieved June 12, 2025, Available from : <https://lexinform.com.ua/militarylex/nakaz-111-nm-vid-01-03-2023-pro-upovnovazhennya-viiskovykh-chastyn-ustanov-zakladiv-v-systemi-ministerstva-oborony-ukrayiny-na-zdiisnennya-oboronnykh-zakupivel-ta-ukladennya-derzhavnykh-kontraktiv-dogovo/>
40. Ministerstvo oborony Ukrainy. (2024, December 27). Minoborony rozroblylo novi metodychni rekomendatsii dlia zakupivelnykh u viiskovykh chastynakh [The Ministry of Defense

- developed new methodological recommendations for military procurement specialists]. Retrieved June 12, 2025, Available from : <https://mod.gov.ua/news/minoboroni-rozrobilo-novi-metodichni-rekomendaciyi-dlya-zakupivelnikiv-u-vijskovih-chastinah>
41. Ministerstvo oborony Ukrainy. (2025, May 14). V Armiia+ startuvav naibilshyi navchalnyi kurs pro oboronni zakupivli [Armiia+ launched the largest training course on defense procurement]. Retrieved June 12, 2025, Available from : <https://mod.gov.ua/news/v-armiya-startuvav-naibilshij-navchalnij-kurs-pro-oboronni-zakupivli>
42. White & Case LLP. (2025). Navigating NATO Procurement: Legal and regulatory considerations for companies in Finland & Sweden. Retrieved June 20, 2025, Available from : <https://www.whitecase.com/insight-alert/navigating-nato-procurement-legal-and-regulatory-considerations-companies-finland>
43. GOV.UK. (2024). Navigating NATO Procurement. Retrieved June 20, 2025, Available from : <https://www.gov.uk/government/publications/navigating-nato-procurement/navigating-nato-procurement>
44. U.S. Department of Defense. (2025). Fact sheet on efforts of Ukraine Defense Contact Group National Armaments Directors. Retrieved June 20, 2025, Available from : <https://www.defense.gov/News/Releases/Release/Article/4026238/fact-sheet-on-efforts-of-ukraine-defense-contact-group-national-armaments-direc/>
45. Verkhovna Rada Ukrainy. (2019). Pro kontsesiiu [On Concession] (Law No. 155-IX). Retrieved May 13, 2025, Available from : <https://zakon.rada.gov.ua/laws/show/155-20#Text>
46. Cabinet of Ministers of Ukraine. (2022, February 28). Deiaki pytannia zdiisnennia oboronnykh zakupivel tovariv, robit i posluh v umovakh voiennoho stanu [Resolution No. 169]. Retrieved June 20, 2025, Available from : <https://zakon.rada.gov.ua/laws/show/169-2022-%D0%BF#Text>
47. Cabinet of Ministers of Ukraine. (2023, May 16). Deiaki pytannia zdiisnennia oboronnykh zakupivel sluzhboiu derzhavnoho zamovnyka [Resolution No. 494]. Retrieved June 20, 2025, Available from : <https://zakon.rada.gov.ua/laws/show/494-2023-%D0%BF#Text>
48. Verkhovna Rada Ukrainy. (2024, August 23). Proiekt Zakonu pro publichni zakupivli №11520 [Draft Law on Public Procurement No. 11520]. Retrieved June 20, 2025, Available from : <https://itd.rada.gov.ua/billInfo/Bills/Card/44788>

Сторітелінг в оборонному секторі

Storytelling in the Defense Sector

Костянтин Ніжейко

Corresponding author: доктор філософії з міжнародних економічних відносин, старший викладач, e-mail: k.nizheyko@knute.edu.ua, ORCID: 0000-0002-2925-1140

Олександра Лендел

здобувач ОС “Марістр”, e-mail: o.lendel_fmtp_4m_24_m_z@knute.edu.ua, ORCID: 0009-0005-9774-5272

Kostyantyn Nizheiko

Corresponding author: PhD in International Economic Relations, Senior Lecturer, e-mail: k.nizheyko@knute.edu.ua, ORCID: 0000-0002-2925-1140

Oleksandra Lendel

Master's degree student, e-mail: o.lendel_fmtp_4m_24_m_z@knute.edu.ua, ORCID: 0009-0005-9774-5272

Державний торговельно-економічний університет, м. Київ, Україна

State University of Trade and Economics, Kyiv, Ukraine

Received: July 30, 2025 | **Revised:** August 11, 2025 | **Accepted:** August 31, 2025

JEL Classification: D91, F52, E65, M33.

DOI: <https://doi.org/10.33445/sds.2025.15.4.21>

Мета роботи. Ідентифікація комунікативних та інформаційно-психологічних аспектів застосування сторітелінгу як інструменту впливу у військово-промисловій сфері та сфері національної безпеки.

Результати дослідження. Подано загальне визначення сторітелінгу, його функції та роль у формуванні емоційного зв'язку між аудиторією та комунікатором. Особливу увагу приділено аналізу оборонної діяльності в контексті сучасної інформаційної війни, де сторітелінг використовується як ефективний засіб психологічного впливу, мобілізації підтримки та формування позитивного іміджу військових структур. Окреслено актуальні тенденції застосування сторітелінгу у військових комунікаціях, зокрема в межах стратегічних комунікацій, інформаційних кампаній та операцій впливу. Досліджено типові тематики військових наративів: героїзм, жертвність, братерство, боротьба за незалежність, захист цінностей. Визначено особливості військового сторітелінгу, такі як емоційна насиченість, апеляція до національної ідентичності, візуально-звукова виразність і адаптація до різних платформ (соціальні мережі, відео, блоги, документальні формати тощо).

Оригінальність. Систематизовано сторітелінг як цілісний комунікаційний інструмент в оборонному секторі, що поєднує психологічний, маркетинговий та стратегічний виміри. Запропоновано структурований механізм використання сторітелінгу для впливу на публічну думку, державні рішення та позиціонування продукції ВПК у міжнародному середовищі. Обґрунтовані основні кроки для практичного впровадження сторітелінгу у стратегії українських компаній оборонного сектору.

Тип статті. концептуальний.

Purpose. To identify the communicative and informational-psychological aspects of storytelling as a tool of influence in the military-industrial sphere and national security.

Findings. A general definition of storytelling, its functions, and role in forming an emotional connection between the audience and the communicator are provided. Particular attention is paid to the analysis of defense activities in the context of modern information warfare, where storytelling is used as an effective means of psychological influence, mobilization of support, and formation of a positive image of military structures. Current trends in the use of storytelling in military communications, particularly in strategic communications, information campaigns, and influence operations, are outlined. Typical themes of military narratives are explored: heroism, sacrifice, brotherhood, struggle for independence, and defense of values. The features of military storytelling are identified, such as emotional intensity, appeal to national identity, visual and audio expressiveness, and adaptation to various platforms (social networks, video, blogs, documentary formats, etc.).

Originality. The study presents in a systematized storytelling as a comprehensive communication tool in the defense sector, combining psychological, marketing, and strategic dimensions. It proposes a structured mechanism for using storytelling to influence public opinion, government decisions, and the positioning of defense industry products in the international environment. The main steps for the practical implementation of storytelling in the strategies of Ukrainian defense sector companies are substantiated.

Paper type. conceptual.

Ключові слова: сторітелінг, національна безпека, військова комунікація, інформаційна війна, стратегічні наративи, оборонний сектор.

Key words: storytelling, national security, military communication, information warfare, strategic narratives, defense sector.

Вступ

У умовах стрімкого розвитку інформаційних технологій та цифрової комунікації сторітелінг, тобто мистецтво передавання інформації через історії, набуває особливої актуальності навіть у таких специфічних і традиційно закритих сферах, як оборонний сектор. Застосування сторітелінгу в цій сфері обумовлено необхідністю досягнення низки важливих цілей національної безпеки держави, серед яких — формування національних оборонних наративів, побудова довіри до виробників озброєння, посилення морально-психологічної стійкості військових, ефективна комунікація із зовнішніми партнерами та просування продукції на міжнародному ринку.

В умовах війни нового типу, коли бойові дії супроводжуються потужними інформаційними кампаніями, розповіді про реальне застосування озброєння, його ефективність у конкретних бойових ситуаціях та історії військовослужбовців, які завдяки цій техніці змогли виконати завдання або врятувати життя, мають надзвичайне значення. Вони не лише мотивують особовий склад і зміцнюють бойовий дух, а й слугують вагомим аргументом для міжнародних партнерів, демонструючи спроможність держави захищатися і водночас раціонально використовувати надану допомогу. Крім того, у глобальній конкуренції на ринку озброєнь важливу роль відіграє здатність країни або компанії презентувати свою продукцію не лише через технічні характеристики, а й через переконливі історії успішного бойового застосування. Такі історії допомагають створити унікальний бренд вітчизняної продукції військового призначення, підвищують її привабливість для потенційних замовників і можуть бути вирішальними при укладанні контрактів. Водночас сторітелінг є ефективним інструментом публічної дипломатії, оскільки дозволяє доносити до міжнародної спільноти правдиву, емоційно наповнену інформацію про оборонний сектор, цінності, які захищає держава, і потреби, що обґрунтовані реальними історіями. Усе це свідчить про те, що сторітелінг в оборонному секторі є не просто елементом комунікації, а стратегічним інструментом інформаційної та безпекової політики, який допомагає в створенні сильного емоційного зв'язку між брендом та її цільовою аудиторією. В контексті функціонування військово-промислового комплексу, сторітелінг використовується як інструмент маркетингу B2G% має вплив на формування іміджу компаній, просування нових зразків озброєння, а також впливу на громадську думку – як урядів різних країн, потенційних партнерів, так і військових та цивільних.

Теоретичні основи дослідження

Тема сторітелінгу в оборонному секторі наразі не є широко дослідженою, проте вона висвітлюється у працях з інформаційної війни, комунікаційних стратегій у сфері безпеки, а також у контексті військової пропаганди та стратегічних наративів. Так наявні публікації підтверджують, що стратегічні наративи активно інтегрують у військову стратегію, оскільки вони формують зв'язок між намірами, діями й сприйняттям громадськості. Зокрема, Блас у статті “Beyond Storytelling” наголошує, що стратегічні наративи стають обов'язковими в умовах геополітичних конфліктів (як-от російсько-українська війна), оскільки вони допомагають пояснювати зміст операцій і зміцнювати легітимність збройних дій (Blas, 2023).

Інший важливий напрям — FICINT (fictional intelligence або “useful fiction”), що поєднує наукову аналітику та художнє оповідання. Цей підхід отримав популярність завдяки авторам типу О. Коула та П.В. Сінгера, які створюють сценарії майбутніх війн, що стимулюють уяву військових та політиків (Singer & Cole, 2020). Слід зазначити практика FICINT активно розвиваються останні три роки: науковці й практики США й Австралії використовують цей метод для навчання військових та трансляції складних технологічних ідей через захопливі історії (National Defence, 2025). Крім того, дослідження НАТО (2024) свідчать про еволюцію наративів від описових до стратегічних, які стали невід'ємною частиною тактики й операцій – особливо в контексті когнітивного виміру війни (Saari, et al., 2024).

Що стосується української наукової спільноти, то з початком збройної агресії російської федерації проти України у 2014 році, включно з анексією Криму та бойовими діями на Сході країни, зросла увага до питань інформаційного супроводу оборонних процесів, зокрема – комунікаційних стратегій та наративів у сфері ВПК. Але не зважаючи на це в українській науковій спільноті майже відсутні дослідження, присвячених питанням трансформації публічного образу оборонної промисловості, ролі сторітелінгу у просуванні українських оборонних технологій на зовнішні ринки, а також впливу стратегічних наративів на розвиток військово-технічної співпраці з партнерами з ЄС та НАТО. Серед наявних публікацій можна відзначити лише напрацювання

Г. Охріменко та І. Приходько (Охріменко та Приходько, 2023), а також О. Скрыбіна, І. Євсєєва, К. Халіманенко, В. Дембіцького (Скрыбін та ін., 2024).

Постановка проблеми

Сучасний оборонний сектор усе активніше застосовує сторітелінг як інструмент формування стратегічних наративів, здатних впливати на громадську думку, легітимізувати військові рішення та підвищувати довіру до інновацій у сфері безпеки. Це зумовлює необхідність дослідження особливостей сторітелінгу в оборонному секторі як нового елементу безпекового дискурсу та публічної взаємодії. Тому метою дослідження є ідентифікація комунікативних та інформаційно-психологічних аспектів застосування сторітелінгу як інструменту впливу у військово-промисловій сфері та сфері національної безпеки.

Результати

У сучасному світі інформація є важливим чинником впливу. У області озброєння, де зазвичай домінують технічні якості та стратегічні розрахунки, все більшого значення набуває сторітелінг – мистецтво створення та розповіді історій. На перший погляд, поєднання такої практичної сфери з емоційним засобом наративу може виглядати неочевидним. Але правильне використання розповіді у області озброєння має великий потенціал для досягнення різних цілей: від формування думки людей до отримання інвестицій й впливу на міжнародні зв'язки.

Сторітелінг — це метод передачі інформації у вигляді зв'язної та емоційно забарвленої історії. Його мета — не тільки інформувати, а й викликати емоції: співпереживання, довіру або мотивацію. Історія може стати сильнішою за сухі факти, оскільки вона впливає на підсвідомий рівень і активізує емоційне мислення аудиторії.

Військова діяльність є занадто складною та прихованою, оскільки інформація, що пов'язана з виробництвом, використанням та продажом зброї, часто вважається конфіденційною, проте оточується дискусіями. У цьому контексті сторітелінг допомагає донести складні ідеї в легко запам'ятовуючій формі, що надає йому особливого значення.

Спосіб комунікації оборонної промисловості значно змінився за останні 15 років. Зокрема, спостерігалось значне зростання використання сторітелінгу як інструменту впливу на громадську думку, залучення нових співробітників, просування технологічних рішень і формування лояльності до бренду. В таблиці нижче представлена умовна динаміка зростання кількості рекламних роликів, публікацій у соцмережах, фільмів, презентацій тощо, створених або на замовлення оборонних компаній з 2010 по 2025 роки.

Таблиця 1 – Тенденції використання сторітелінгу в оборонному секторі

2010-2015 роки: Початковий етап цифрової трансформації	2016-2020 роки: Поширення цифрового контент-маркетингу	2021-2025 роки: Залучення новітніх технологій
Оборонні компанії традиційно використовують закриті канали комунікації, орієнтуючись на урядових замовників та військових. Зростаюча роль цифрових платформ почала впливати на стратегії комунікації.	Основними інструментами комунікації стають соціальні мережі, відео, блоги, інфографіка тощо. Компанії, такі як Raytheon Technologies і Northrop Grumman, активно використовують сторітелінг для демонстрації технологічних досягнень і залучення громадськості.	Популярним стає використання штучного інтелекту, доповненої реальності для створення персоналізованого контенту. Активно застосовуються соціальні мережі для взаємодії з громадськістю та підвищення прозорості діяльності.

Джерело: складено авторами за відкритими даними

Дані показують, що сторітелінг поступово зріс у першій половині 2010-х років, швидко розвивався після 2016 року на тлі загострення геополітичних конфліктів і активізувався після 2020 року, коли цифрова трансформація набула чинності. До 2025 року сторітелінг стане одним із ключових інструментів публічної комунікації в секторі безпеки та оборони.

Однією з головних особливостей сторітелінгу в сфері озброєння виступає мета у формуванні певного наративу. В залежності від цілей, історії можуть привертати увагу та наголошувати на наступних ідеях:

1. Потреба модернізації та оновленні армії (історії про наявне застаріле та невідповідне обладнання та озброєння, в порівнянні з успішними прикладами сучасних розробок, що можуть переконати державні органи та громадськість у потребі інвестицій у нові технології).

2. Пріоритети наявності та використання конкретних видів озброєння (успішні історії про використання певної зброї та досягнення певних цілей в реальних ситуаціях можуть підвищити інтерес для її придбання потенційними покупцями).

3. Мужність, хоробрість та відвага військовослужбовців (історії про військову службу, підготовку на високому рівні, готовність до будь-якого супротиву, формують позитивні враження про стійкий характер військових, що має вплив на зміцнення зв'язку між армією та громадським населенням, підвищуючи авторитет військової діяльності).

4. Забезпечення національної безпеки (історії про потенційні загрози для держави та суспільства, ефективність використання всього або певного виду озброєння для їх подолання чи недопущення, мають на меті обґрунтування витрат на оборону та військово-промисловий комплекс, оскільки дані витрати є інвестицією у власну безпеку).

Виходячи з аналізу тенденцій за 2024 рік, в тому числі в контексті війни в Україні, зростання оборонних витрат у Європі та США, а також впливу новітніх технологій на комунікаційні стратегії, можна виділити співвідношення ключових тем, які найчастіше зустрічаються у військовому сторітелінгу. Найбільшу частку займають теми героїзму та патріотизму — вони забезпечують глибокий емоційний зв'язок із аудиторією та стимулюють лояльність до військових структур. Також помітну частину займають наративи загрози, що підсилюють відчуття небезпеки та потреби в захисті. Технічні теми, як-от інновації або безпека, менш емоційні, але виконують раціональну функцію переконання (рис. 1).

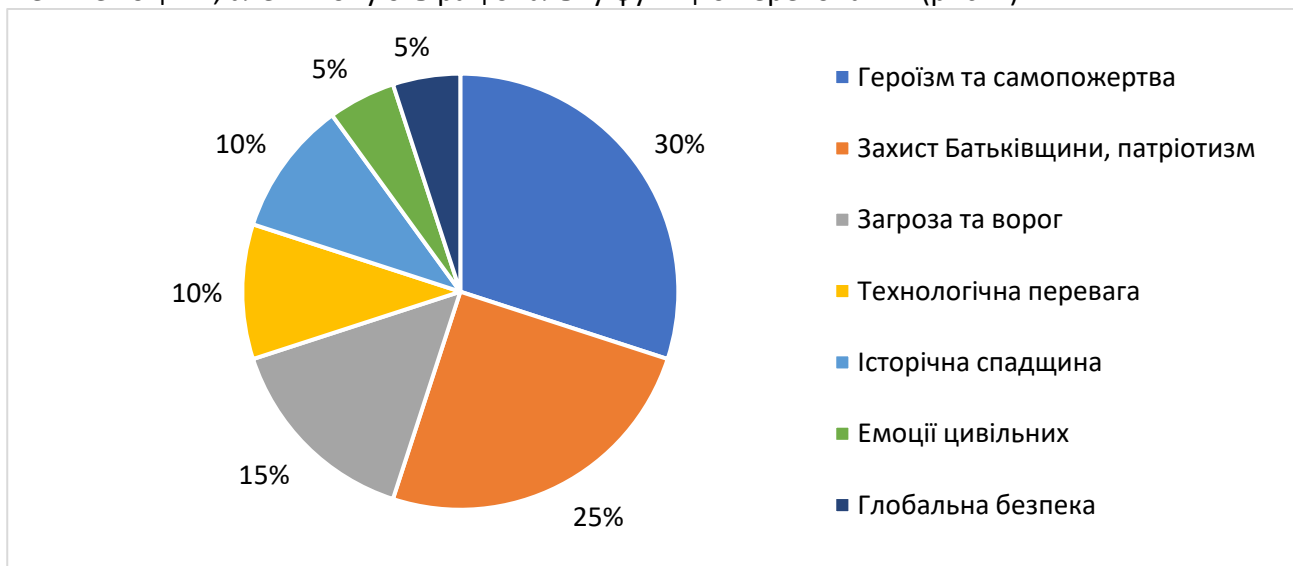


Рисунок 1 – Співвідношення тематик у військових наративах

Джерело: складено авторами

Сторітелінг у військовій сфері вважається досить складним явищем, яке вимагає глибокого розуміння теми, дотримання вимог безпеки, врахування етичних норм та

відповідного використання емоційної сили наративу. Оскільки кожна історія може бути як позитивно, так і негативно вплинула на суспільну думку, політичні рішення та навіть хід війни. Виходячи з цього, військових сторітелінг має свої унікальні та специфічні риси для його використання (табл. 2).

Таблиця 2 – Особливості військового сторітелінгу

Ознака	Його характеристика
Співвідношення між правдою та пропагандою	Не в залежності від того, що історії мають нести емоційне, мотивуюче забарвлення, бути переконливими, вони в першу чергу мають бути правдоподібними. Перебільшення пропаганди може викликати недовіру, маючи зворотній ефект.
Дотримання конфіденційності	У використанні військового сторітелінгу важливо уникати витоку інформації. Історії, що подаються суспільству, мають бути узгоджені для забезпечення безпеки. Не можна зазначати місця розташування військових, назви та місця важливо стратегічних об'єктів або деталі операцій. Дані обмеження вказують на головній цілі – зосередження на людському аспекті історії.
Емоційний та моральний вплив на суспільство	Історії про війну завжди дуже емоційні, вони мають втрати, біль, страх, надію та героїзм. Військові історії можуть як надихати, так і бути психологічно важко сприйнятими. Саме тому важливо донести інформацію правильно, щоб ні в якому разі не романтизувати війну, не знецінювати страждання, не перетворювати біду на сенсацію.
Зв'язок з національною ідентичністю	Військовий сторітелінг має відповідати національному контексту (захист Батьківщини, використання національних символів – прапору, гімну, гербу, зв'язок з історією та подіями минулого). Це домагає створювати великі наративи, будуючи загальну історію боротьби за незалежність та свободу і захисту країни.
Використання візуальних засобів	Візуальний контент допомагає в збереженні довіри глядача. Відеоматеріал, фотографії можуть мати набагато більший вплив та переконливість історій про озброєння. Окрім цього вони додають більшого емоційного забарвлення кожній історії.
Націленість на певну цільову аудиторію	Військові історії мають різну мету, в залежності від їхніх слухачів, відповідно мають адаптуватися: посилення мотивації та важливості підтримки армії для громадян, підтримка бойового духу, відчуття єдності з народом для військових, демонстрація героїзму військових та переконання у правильності дій з боку держави для іноземної аудиторії.

Джерело: складено авторами

В сучасний період сторітелінг активно використовується у різних аспектах, пов'язаних з військовою діяльністю, оборонною промисловістю та озброєння. Найпоширеніший приклад, з яким стикається нині кожен, це історії в соціальних мережах та медіа про бойові дії, військових, їхніх побратимів, особисті переживання, втрати та перемоги, озброєння, яке допомогло видити (наприклад, історія в Facebook від командира підрозділу про український БТР, який витримав пряме влучання, що зберегло життя всім військовим). Також в мережі Інтернет та на телебаченні з'явилася велика кількість військових фільмів та роликів про військові підрозділи, життя військових, їхній шлях та досягнення (наприклад, відео, які показують, як звичайна людина, фахівець в своїй справі, кардинально змінює сферу, вступивши до лав Збройних Сил України). Активно використовують сторітелінг і військові частини для формування іміджу армії та рекрутингу. Історії про військових, їхнє життя до та після, переваги певної бригади, використовують для залучення нових людей в команду. Щодо зв'язку з військовою технікою, наразі існує велика кількість експозицій та виставок у військових музеях і не тільки. Окрім технічного опису озброєння, згадується також хто створив цю техніку, як вона працювала під час бойових дій і як допомогла армії забезпечити перевагу чи навіть

врятувати життя. Самі виробники військової техніки залучають сторітелінг для зовнішньої комунікації. Наприклад, оборонні компанії “Укроборонпром”, “Baykar”, “Rheinmetall” публікують не лише характеристики озброєння, вони також публікують особисті історії виробників та випробувачів, відеоролики створення техніки від перших кроків до використання в бойових діях, показують історії збереження життя військових за їх допомогою (див. наприклад (Baykar, 2022; NEW EASTERN EUROPE, 2025).

На рисунку 2 представлено механізм використання сторітелінгу в оборонному секторі, який ілюструє ключові етапи — від формування наративів до досягнення стратегічних цілей.

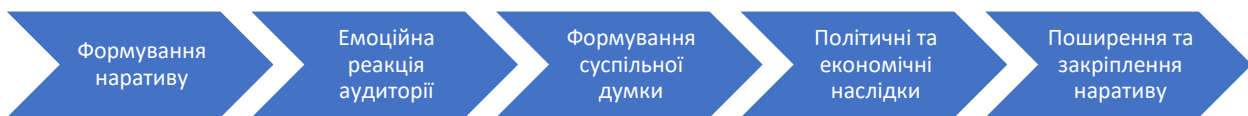


Рисунок 2 – Механізм використання сторітелінгу в оборонному секторі

Джерело: розроблено авторами

Центральним елементом цього процесу є змістовне та емоційне відображення реальних історій, здатних викликати цільову емоційну реакцію в аудиторії. Такі наративи виконують роль каталізаторів інформаційного впливу, оскільки не лише передають фактичні відомості про події, продукцію або дії військових структур, а й забезпечують глибоке залучення, емпатію та ідентифікацію з образами героїв, технологій або ідей.

Емоційний вплив на аудиторії забезпечує трансформацію окремого наративу в засіб формування колективної думки в сфері національної безпеки. В умовах російсько-української війни саме суспільна думка має стати фундаментом політичних рішень щодо розподілу бюджетних ресурсів, пріоритетів державного оборонного замовлення або легітимації стратегічних альянсів. Таким чином, сторітелінг в оборонному секторі виконує функцію не лише комунікаційного інструменту, а й непрямого важеля впливу на прийняття рішень у сфері безпеки та оборони.

Крім того, закріплення військових наративів у масовій культурі — через фільми, документалістику, соціальні мережі або навіть ігрову індустрію — сприяє формуванню стійких образів, що резонують з архетипами сили, захисту, технологічної переваги. Такий наративний контент часто набуває вірусного характеру, повторюється, варіюється та вбудовується в ширший інформаційний простір, створюючи ефект позитивного зворотного зв'язку. У результаті сторітелінг перетворюється на потужний мультиплатформенний інструмент стратегічних комунікацій, що здатний забезпечити довготривалий емоційний і політичний резонанс для формування ідеології національної єдності, підтримки вітчизняних оборонних стратегій та посилення міжнародного позиціонування українських оборонних компаній.

Висновки

Отже сторітелінг — це не лише спосіб подачі певної інформації, це повноцінний інструмент формування свідомості та впливу, особливо в сфері військової діяльності. Через правдиві, емоційні розповіді формується не тільки ставлення до війни, армії або техніки, а також цінності суспільства, моральна готовність та віра у перемогу. Відповідно у часи війни правильно побудована історія може не тільки зачепити слухача, вона здатна мобілізувати, навчити, об'єднати та врятувати.

Сторітелінг в оборонному секторі поступово трансформується зі звичайного інструменту комунікації у стратегічний ресурс впливу, що охоплює водночас емоційну, інституційну та економічну площини. Його ефективне використання дозволяє створювати символічний капітал військової та оборонної продукції, посилюючи суб'єктивне сприйняття її цінності як на внутрішньому, так і на зовнішньому рівні. Наративи, що народжуються з реального бойового

досвіду, персональних історій військовослужбовців або виробників, стають не просто засобом інформування, а цілісною системою передачі значень, яка формує довіру, мобілізує підтримку, створює репутаційні переваги та в цілому посилює національну безпеку.

В умовах інформаційно-психологічної війни, у якій Україна перебуває з 2014 року, сторітелінг стає не лише інструментом переконання або маркетингу, а засобом відстоювання суб'єктності держави в глобальному безпековому середовищі. Історії, які демонструють ефективність озброєння, моральну перевагу воїнів чи адаптивність оборонної промисловості, формують впізнавану візуальну та змістову ідентичність українського ВПК, сприяючи його просуванню на міжнародних ринках і підвищенню переговорної сили у сфері військово-технічного міжнародного співробітництва.

Крім того, наративи, що ґрунтуються на реальному бойовому досвіді, не лише сприяють формуванню іміджу окремих компаній або технологій, але й підсилюють загально-національний бренд безпеки та оборони. Саме тому сторітелінг доцільно розглядати як інструмент національної безпеки – такий, що поєднує медійні технології, цільову психологічну дію, маркетингову логіку та політичну прагматику.

В контексті розвитку українського оборонного сектору в умовах російсько-української війни важливо не лише технологічне нарощування потенціалу, а й вміння супроводжувати це розвитком ефективних стратегічних наративів. Це вимагає підготовки фахівців, здатних мислити як інженери, так і комунікатори, а також формування інституційної культури комунікації в оборонному секторі, орієнтованої на відкритість, репутаційну відповідальність і цілеспрямовану побудову національної безпекової ідентичності. Отже відповідно до отриманих результатів дослідження нами запропоновано основні кроки для практичного впровадження сторітелінгу у стратегії українських компаній оборонного сектору:

- обов'язкова розробка внутрішнього протоколу перевірки контенту на предмет витоку чутливої інформації (місця, об'єкти, технічні характеристики);

- проведення тренінгів з етичного сторітелінгу для PR-фахівців та контент-мейкерів компанії - щоб уникнути маніпуляцій, романтизації війни, пропаганди;

- систематизація реальних історій бойового застосування техніки, її ролі у збереженні життя, успішному виконанні місій;

- використання досвіду користувачів техніки (user experience) – історії від військових, інженерів, інструкторів (із дотриманням заходів безпеки та конфіденційності);

- побудова презентацій та публічних виступів у форматі “реальний виклик – наше рішення – доказ ефективності”;

- вбудовування сторітелінгу в корпоративні стенди на виставках: стенди повинні розповідати історію, а не просто демонструвати ТТХ;

- активне використання соціальних мереж: LinkedIn, X (ex-Twitter), YouTube, Instagram – для створення коротких історій, серій, реактивних постів;

- просування українського оборонного сектору як ціннісного бренду, що боронить не лише Україну, а й принципи свободи та партнерства в регіоні.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

Blas, N. (2023). Beyond storytelling. *Æther: A Journal of Strategic Airpower & Spacepower*, 2(1), 46-57. Available from : <https://www.airuniversity.af.edu/Portals/10/ÆtherJournal/Journals/Volume-2 Number-1/Blas-Beyond-Storytelling.pdf>

- Singer, P. W., & Cole, A. (2020). *Burn-in: A Novel of the Real Robotic Revolution*. Mariner Books.
- National Defence (2025). Startup Helps Officers Explain Future Warfare Through Storytelling. Available from : <https://www.nationaldefensemagazine.org/articles/2022/12/16/startup-helps-officers-explain-future-warfare-through-storytelling>
- Saari, D., Häkkinen, T., & Moilanen, P. (2024). A Comprehensive Analysis of Narratives within NATO's Doctrines. In *Proceedings of the European Conference on Cyber Warfare and Security* (Vol. 23, No. 1). Academic Conferences International Ltd. Available from : <https://pdfs.semanticscholar.org/781a/d69e9845867a1f550861f71bf0fa685954f4.pdf>
- Охріменко, Г. В., & Приходько, І. П. (2023). Digital-сторітелінг на теренах медійного простору: аналіз контентоутворення. *Інформація та соціум*, 58-60. Available from : <https://ijas.donnu.edu.ua/article/view/14559>
- Скрябін, О., Євсєєв, І., Халіманенко, К., & Дембіцький, В. (2024). Використання радянською пропагандою комунікативно-пропагандистських технологій впливу для формування "образу США" під час холодної війни. *Вісник Національного університету оборони України*, 141-151. <https://doi.org/10.33099/2617-6858-2024-82-6-141-151>.
- Baykar (2022). Turkish drones have become a symbol of the Ukrainian resistance. Available from : <https://baykartech.com/en/press/turkish-drones-have-become-a-symbol-of-the-ukrainian-resistance/>
- New Eastern Europe (2025) Securing stability: powering Ukraine's defence production surge. Available from : <https://neweasterneurope.eu/2024/07/26/securing-stability-powering-ukraines-defence-production-surge/>

References

- Blas, N. (2023). Beyond storytelling. *Æther: A Journal of Strategic Airpower & Spacepower*, 2(1), 46-57. Available from : [https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-2 Number-1/Blas-Beyond-Storytelling.pdf](https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-2%20Number-1/Blas-Beyond-Storytelling.pdf)
- Singer, P. W., & Cole, A. (2020). *Burn-in: A Novel of the Real Robotic Revolution*. Mariner Books.
- National Defence (2025). Startup Helps Officers Explain Future Warfare Through Storytelling. Available from : <https://www.nationaldefensemagazine.org/articles/2022/12/16/startup-helps-officers-explain-future-warfare-through-storytelling>
- Saari, D., Häkkinen, T., & Moilanen, P. (2024). A Comprehensive Analysis of Narratives within NATO's Doctrines. In *Proceedings of the European Conference on Cyber Warfare and Security* (Vol. 23, No. 1). Academic Conferences International Ltd. Available from : <https://pdfs.semanticscholar.org/781a/d69e9845867a1f550861f71bf0fa685954f4.pdf>
- Okhrymenko, H. V., & Prykhodko, I. P. (2023). Digital storytelling in the media space: An analysis of content creation. *Informatsiia ta Sotsium*, 58-60. Available from : <https://ijas.donnu.edu.ua/article/view/14559>.
- Skriabin, O., Yevsieiev, I., Khalimanenko, K., & Dembitskyi, V. (2024). The use of communicative and propaganda technologies of influence by Soviet propaganda to form the "image of the USA" during the Cold War. *Visnyk Natsionalnoho Universytetu Oborony Ukrainy*, 141-151. <https://doi.org/10.33099/2617-6858-2024-82-6-141-151>.
- Baykar (2022). Turkish drones have become a symbol of the Ukrainian resistance. Available from : <https://baykartech.com/en/press/turkish-drones-have-become-a-symbol-of-the-ukrainian-resistance/>
- New Eastern Europe (2025) Securing stability: powering Ukraine's defence production surge. Available from : <https://neweasterneurope.eu/2024/07/26/securing-stability-powering-ukraines-defence-production-surge/>

Матриця прийняття рішень – як інструмент обґрунтування шляхів забезпечення необхідного рівня оборонної достатності держави

Decision Matrix as a Tool for Substantiating Options to Ensure Sufficient National Defense Capacity

Олег Семененко ^A

Corresponding author: д. військ. н., професор, заступник начальника науково-дослідного інституту з наукової роботи, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Марина Абрамова ^A

к. екон. н., старший дослідник, провідний науковий співробітник, e-mail: elaira3@gmail.com, ORCID: 0000-0001-7644-9988

Поліна Толок ^B

к. екон. н., начальник кафедри оборонного менеджменту, e-mail: tolok100@meta.ua, ORCID: 0000-0002-2481-8152

Ольга Таран ^C

старший науковий співробітник, e-mail: olgataran@ukr.net, ORCID: 0000-0002-9143-5821

Олег Тарасов ^C

к. військ. н., доцент, Кафедра військової підготовки Національного авіаційного університету, e-mail: tarasovo@ukr.net, ORCID: 0000-0002-6763-8653

Марія Ярмольчик ^C

доктор філософії, начальник науково-дослідної лабораторії, e-mail: LinkinFan357@ukr.net, ORCID: 0000-0001-9917-0189

Oleh Semenenko ^A

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

Maryna Abramova ^A

PhD (Econom.), Senior Researcher, Leading Research Scientist, e-mail: elaira3@gmail.com, ORCID: 0000-0001-7644-9988

Polina Tolok ^B

PhD (Econom.), Head of the Department of Defense Management, e-mail: tolok100@meta.ua, ORCID: 0000-0002-2481-8152

Olha Taran ^C

Senior Research Fellow, e-mail: olgataran@ukr.net, ORCID: 0000-0002-9143-5821

Oleh Tarasov ^C

Candidate of Military Sciences, Associate Professor, e-mail: tarasovo@ukr.net, ORCID: 0000-0002-6763-8653

Mariia Yarmolchik ^C

Doctor of Philosophy, head of the research laboratory, e-mail: LinkinFan357@ukr.net, ORCID: 0000-0001-9917-0189

^AЦентральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна

^BНаціональний університет оборони України, Київ, Україна

^CКафедра військової підготовки Державного університету "Київський авіаційний університет", м. Київ, Україна

^ACentral Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

^BNational Defence University of Ukraine, Kyiv, Ukraine

^CDepartment of Military Training, State University "Kyiv Aviation University", Kyiv, Ukraine

Received: July 30, 2025 | Revised: August 11, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.22>

Мета роботи. Висвітлення результатів застосування науково обґрунтованого інструменту підтримки прийняття рішень у сфері управління оборонними ресурсами, який дозволяє комплексно оцінювати стан оборонної достатності, виявляти її слабкі місця та пропонувати ефективні шляхи їх усунення.

Метод дослідження. Аналіз, синтез, порівняння, формалізації та оцінювання матеріалу, абстрагування та кон'юнктурного аналізу (мислення).

Результати дослідження. Створення науково обґрунтованого інструменту (Матриці рішень) підтримки управлінських рішень для забезпечення оборонної достатності держави, який дозволяє оцінити критичні слабкі місця, визначити пріоритетні напрями розвитку та запропонувати конкретні управлінські сценарії підвищення рівня оборонної достатності держави шляхом концентрації ресурсів на найбільш уразливих сферах національного господарства.

Теоретична цінність дослідження. Результати дослідження можуть бути використані для удосконалення теоретичних підходів до формування системи критеріїв і показників оборонної достатності держави та оптимізації стратегічного управління оборонними ресурсами в умовах гібридних загроз.

Тип статті. Теоретичний.

Purpose. Highlight the results of a numerical experiment on decision-making in defence resource management. This allows for a comprehensive assessment of the current state of defence sufficiency, identifying weaknesses and proposing ways to address them effectively.

Method. Analysis, synthesis, comparison, formalization and evaluation of the material, abstraction and conjunctural analysis (thinking).

Findings. The creation of a scientifically based tool (the Decision Matrix) to support management decisions and ensure the defence sufficiency of the state. This tool allows critical weaknesses to be assessed, priority areas of development to be identified, and specific management scenarios to be proposed in order to increase the level of defence sufficiency by concentrating resources on the most vulnerable areas of the national economy.

Theoretical implications. The results of the study can be used to improve theoretical approaches to the formation of a system of criteria and indicators of the state's defence sufficiency and optimisation of strategic management of defence resources in the context of hybrid threats.

Paper type. Theoretical.

Ключові слова: оборонна достатність, управлінські рішення, критерії оцінювання, балансова модель, національне господарство.

Key words: defence sufficiency, management decisions, assessment criteria, balance sheet model, national economy.

Вступ

Для гарантованого забезпечення належного рівня національної безпеки держава має завчасно вживати заходів, достатніх та адекватних характеру і масштабам сучасних воєнних загроз. Попри критичну важливість оборонної достатності, поняття цього явища і методи його досягнення досі не мають чіткого визначення в науці, а саме: бракує однозначно визначених складових, методик розрахунку її рівня та навіть законодавчо закріпленого визначення терміну “оборонної достатності”.

Теоретичні основи дослідження

У сучасних дослідженнях питання забезпечення ОД держави активно обговорюється у контексті гібридних загроз та зростаючої ролі технологічних інновацій. Зокрема, у звіті Stockholm International Peace Research Institute зазначено, що країни зосереджують увагу на розвитку передових технологій, кіберзахисту та удосконаленні систем раннього попередження для підвищення обороноздатності [2]. Дослідження RAND Corporation підкреслюють необхідність інтеграції цивільних і військових ресурсів для формування більш стійкої оборонної системи [3], автори вказують на важливість стратегічного партнерства та міжнародної кооперації у зміцненні національної безпеки. На противагу, у науковій статті, опублікованій в Journal of Defense Modeling and Simulation, запропоновано використовувати методи багатокритеріального аналізу для оптимізації процесів прийняття рішень щодо розподілу оборонних ресурсів [4], такий підхід корелює з використанням методу аналізу ієрархій Сааті, який було застосовано у даному дослідженні.

Також варто відзначити аналітичну доповідь Європейського оборонного агентства, де наголошується на важливості інвестування в людський капітал, освіту та підготовку персоналу для зміцнення оборонного потенціалу [5]. Водночас, у роботі українських авторів акцент зроблено на необхідності балансування між витратами на оборону та соціально-економічними потребами держави, що є особливо актуальним для країн із обмеженим бюджетом [6]. А зміни у характері загроз та ресурсні обмеження зумовили появу сучасних підходів до оборонного планування та оцінювання спроможностей. Зокрема, оборонне планування на основі спроможностей [7], поширене серед країн НАТО, враховує широкий спектр можливих кризових сценаріїв та дозволяє раціонально розподіляти обмежені оборонні ресурси на пріоритетні спроможності. Цей підхід фактично є стратегічним плануванням в умовах невизначеності, спрямованим на формування сил оборони, здатних реагувати на широкий спектр сучасних викликів у межах наявних економічних обмежень. Паралельно, у сфері оборонного менеджменту все більше застосовуються методи підтримки управлінських рішень, що базуються на багатокритеріальному аналізі [8]. Такі методи, як аналіз ієрархій чи техніка компромісного ранжування (наприклад, TOPSIS), передбачають побудову матриці рішень із визначенням релевантних критеріїв та їхніх ваг для оцінки альтернатив. Умови динамічних змін і множинності критеріїв ефективності підкреслюють важливість використання подібних багатокритеріальних підходів при виробленні оборонних рішень.

Таким чином, аналіз актуальних досліджень за даною тематикою підтверджує значущість розроблення комплексного підходу до оцінювання та забезпечення ОД, що враховує не тільки техніко-економічні, соціально-політичні та морально-психологічні аспекти, а й можливості національного господарства країни.

Постановка проблеми

За сучасних умов геополітичної нестабільності, яка супроводжується зростанням гібридних загроз, гостро постає завдання забезпечення належного рівня оборонної достатності (ОД), що виступає ключовою складовою забезпечення національної безпеки, оскільки саме від рівня

сформованості оборонного потенціалу залежить здатність країни протидіяти як зовнішнім, так і внутрішнім викликам. Тому завдання розробки ефективних підходів до обґрунтування шляхів забезпечення необхідного рівня ОД та визначення пріоритетних напрямів її розвитку зумовлена й обмеженістю ресурсів, що виділяються на оборону, а також нагальною потребою у підвищенні ефективності управлінських рішень. Оскільки наявні підходи до оцінювання ОД здебільшого зосереджуються на окремих аспектах, таких як техніко-економічні, військово-організаційні чи соціально-політичні, без урахування їх комплексної взаємодії та інтеграції в єдину систему [1] – це створює ситуацію, за якої формується фрагментарне бачення забезпечення обороноздатності та обмежуються можливості для вироблення збалансованих і стратегічно виважених рішень, спрямованих на розвиток оборонного потенціалу держави. У зв'язку з цим актуальною науковою проблемою є створення методики, яка б дозволяла забезпечувати системний підхід до висвітлення проблематики підвищення ефективності управлінських рішень для досягнення необхідного рівня ОД держави.

Результати

Проведене дослідження складається із п'яти складових: визначення критеріїв, що мають вплив на стан ОД; визначення інтегральних значень елементів груп показників ОД; формування матриці груп показників ОД за сферами їх реалізації; визначення виду проблематики забезпечення ОД; визначення шляхів забезпечення необхідного рівня ОД (рис. 1).

На першому етапі проведення дослідження було реалізовано комплекс заходів, спрямованих на визначення ключових критеріїв, за котрими здійснюється оцінювання стану основних груп показників ОД держави, що стало можливим завдяки використанню методу аналізу ієрархій Сааті, який дозволяє систематизувати процес прийняття рішень шляхом формалізації експертних оцінок та побудови матриці парних порівнянь для встановлення відносної вагомості кожного з виділених критеріїв.

Застосування зазначеного методу було обумовлено необхідністю створення обґрунтованої методологічної основи для подальшого проведення кількісного аналізу, яка б враховувала не лише техніко-економічні аспекти, а й соціально-політичні та морально-психологічні чинники, що мають істотний вплив на рівень ОД за сучасних умов гібридних загроз та високої динаміки змін безпекового середовища.

Під час дослідження було визначено сім інтегральних критеріїв, до яких увійшли: критерій захисту, що відображає здатність держави забезпечувати безпеку своїх територій, населення та критичної інфраструктури від зовнішніх та внутрішніх загроз; критерій спроможностей, що характеризує наявність ресурсів, техніки, озброєння, підготовленого персоналу та організаційних структур для ефективного ведення оборонних операцій; критерій розвитку, який охоплює процеси постійного удосконалення оборонного потенціалу за рахунок модернізації технологій, професійної підготовки та впровадження інновацій; критерій стійкості, що визначає здатність оборонної системи протистояти довготривалим викликам, зберігати функціональність у кризових ситуаціях та швидко відновлюватися після негативних впливів; критерій підтримки, який відображає рівень політичної, економічної та соціальної бази для стабільного фінансування, логістичного забезпечення та мобілізації громадської підтримки; критерій незламності, який стосується морально-психологічної готовності населення та Збройних Сил до опору навіть у надскладних умовах; а також критерій взаємодії, що включає координацію між державними структурами, міжнародними партнерами та громадянським суспільством для забезпечення ефективної оборони.

Результати обробки експертних оцінок дозволили сформувати квадратну матрицю парних порівнянь розмірністю "7×7", у якій діагональні елементи дорівнювали одиниці, а кожен позадіагональний елемент відображав ступінь відносної важливості одного критерію над іншим, що дозволило провести нормалізацію значень за формулою, у якій кожен елемент стовпця ділився на суму цього стовпця для забезпечення коректності подальшого розрахунку середніх вагових коефіцієнтів.

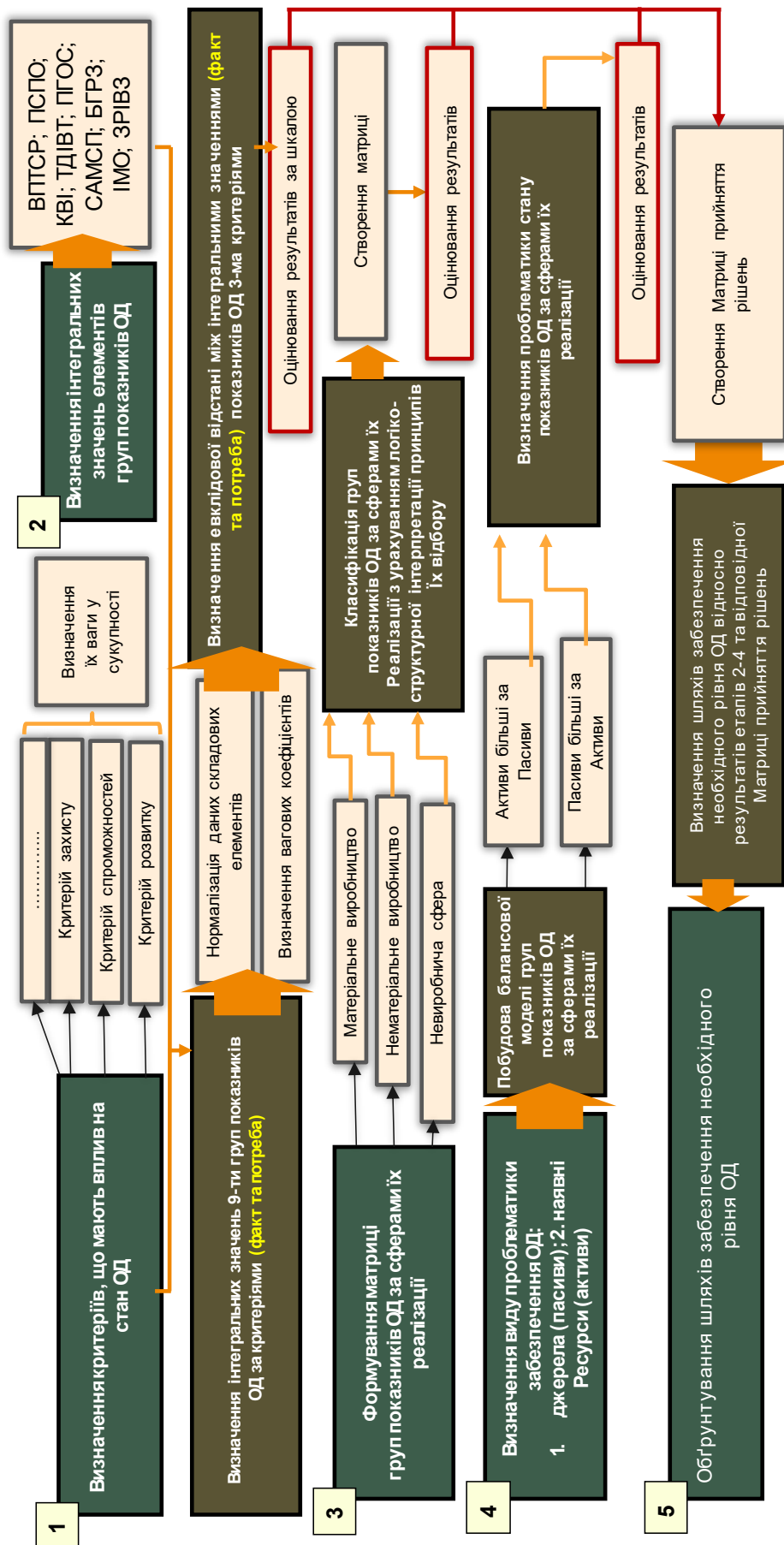


Рисунок 1 – Послідовність проведення дослідження

У результаті нормалізації та обчислення середніх значень по рядках було визначено вектор пріоритетів, що відображає частку кожного критерію у загальній структурі оцінки, де найбільші значення отримали критерій розвитку (0,35), критерій спроможностей (0,32) та критерій захисту (0,21), які разом формують понад 88% сумарної ваги, що вказує на їх визначальний вплив на загальний рівень ОД держави, тоді як решта критеріїв – стійкість (0,09), підтримка (0,07), незламність (0,05) та взаємодія (0,04) – мають нижчу відносну вагомість, але залишаються важливими для забезпечення комплексності підходу. Таким чином, проведений етап дозволив не лише кількісно визначити пріоритети серед різних чинників, що впливають на стан ОД, а й створив підґрунтя для подальшого вдосконалення методики оцінювання, що у перспективі сприятиме підвищенню ефективності управлінських рішень шляхом концентрації ресурсів та зусиль на найбільш значущих напрямках (рис. 2).

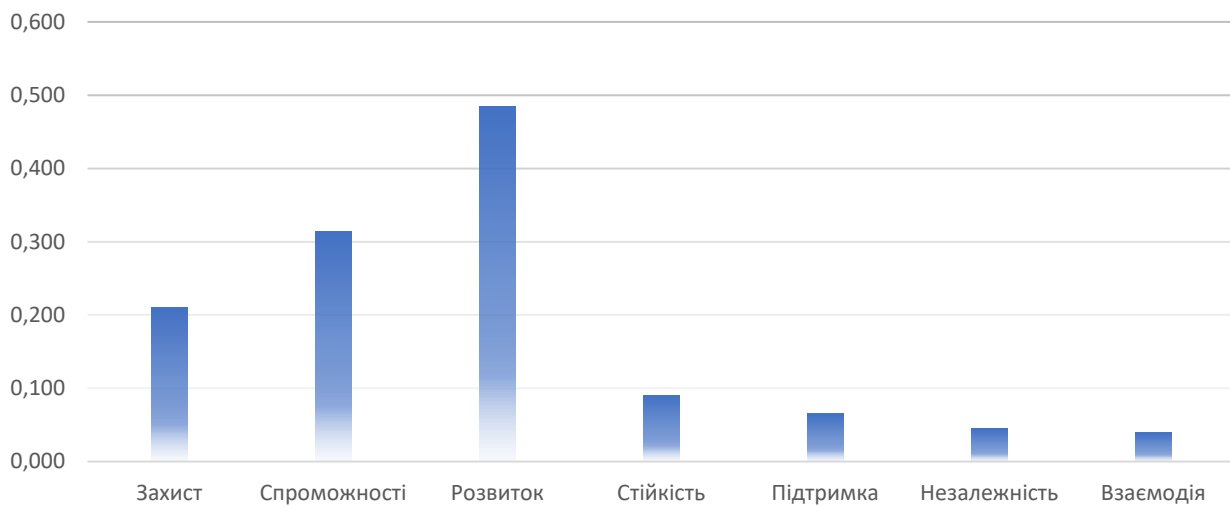


Рисунок 2 – Результати оцінювання ваги критеріїв на стан показників ОД

Джерело: результати розрахунків авторів

На другому етапі методики було проведено комплексну ідентифікацію та оцінювання дев'яти основних груп показників системи забезпечення необхідного рівня (СЗНР) ОД України за останні 5 років. Зокрема, до аналізу включено такі групи: передові технології спостереження та розвідки (ВПТСР), перспективні системи протиракетної оборони (ПСПО), заходи кібербезпеки для захисту військової інфраструктури (КВІ), технологічні досягнення та інновації у військовій техніці (ТДІВТ), підготовка та готовність особового складу (ПГОС), стратегічні альянси і міжнародні системи підтримки (САМСП), бойова готовність та час реагування на загрози (БГРЗ), інновації та модернізація обладнання (ІМО), а також збір розвідувальної інформації та виявлення загроз (ЗРІВЗ).

Для відбору складових за кожною групою було використано метод анкетування із залученням 20 експертів галузі воєнної безпеки, що дозволило отримати усереднені оцінки з високим ступенем достовірності.

Цей етап було реалізовано для того, щоб здійснити кількісну оцінку спроможностей, рівня захисту та перспектив розвитку зазначених груп показників ОД шляхом визначення інтегральних значень за трьома критеріями оцінювання ($K_p 1$ – спроможності, $K_p 2$ – захист, $K_p 3$ – розвиток). Нормалізація вихідних даних у межах інтервалу $[0;1]$ дала змогу уніфікувати різнорідні показники та забезпечити порівнянність їхніх значень, незалежно від відмінностей у одиницях вимірювання.

У результаті проведених розрахунків було визначено інтегральні значення для кожної групи як у фактичному стані, так і у прогнозованій потребі. Наприклад, для групи ВПТСР інтегральне значення за Критерієм 1 (спроможності) становило 0,5052 (факт) проти 0,4155

(потреба), за Критерієм 2 (захист) – 0,3992 (факт) проти 0,4759 (потреба), а за Критерієм 3 (розвиток) – 0,6541 (факт) проти 0,3040 (потреба). Аналогічні обчислення проведені для всіх інших груп показників.

Для оцінки відхилень між фактичними та цільовими значеннями було застосовано метод обчислення евклідової відстані у тривимірному просторі критеріїв, що дозволило кількісно визначити розрив між поточним станом та потребою. Застосування цього підходу необхідне для того, щоб виявити найбільш проблемні напрямки забезпечення ОД України, а також сформулювати пріоритети для подальшого розвитку і вдосконалення військових, організаційних та інфраструктурних компонентів. За отриманими результатами було складено шкалу оцінювання, яка вказує на рівень проблемності кожної групи: так, групи ТДІВТ (значення відстані 0,1853) та БГРЗ (0,2070) отримали оцінку “відмінно”, КВІ (0,2536) та ПСПО (0,2905) – “добре”, а ЗРІВЗ (0,7658) та ПГОС (0,5423) – “дуже низько” (рис. 3).



Рисунок 3 – Результати оцінювання рівня проблематики функціонування груп показників ОД відповідно до розрахунку евклідових відстаней

Джерело: результати розрахунків авторів

Таким чином, другий етап дозволив отримати комплексну, кількісно обґрунтовану картину стану ОД України, виявивши як сильні сторони, що не потребують значних ресурсних вкладень, так і критичні слабкі місця, котрі потребують негайного втручання для запобігання ризикам функціональної неефективності у випадку загроз національній безпеці.

На третьому етапі реалізації методики було здійснено класифікацію та систематизацію основних груп показників, що визначають рівень ОД України, за сферами національного господарства.

Для цього проведено розподіл показників за трьома ключовими сферами: матеріальне виробництво (яке охоплює створення матеріальних благ, таких як техніка, зброя, інфраструктура), нематеріальне виробництво (що включає створення послуг, знань, інформаційних ресурсів та підготовку кадрів) та невиробничу сферу (яка забезпечує функціонування суспільства завдяки управлінню, освіті, обороні, медицині тощо). Було застосовано підхід експертного оцінювання та створено семантичну матрицю для відображення взаємозв'язків між окремими групами показників та зазначеними сферами, що дозволило візуалізувати концентрацію елементів системи ОД та ідентифікувати потенційні прогалини у забезпеченні.

Реалізація цього етапу була спрямована на обґрунтування шляхів покращення рівня ОД України шляхом визначення слабких місць у забезпеченні різних секторів національного господарства. Такий підхід дозволяє встановити, яка саме сфера вимагає пріоритетної уваги для підвищення ефективності оборонної системи держави, а також які групи показників потребують найбільшого доопрацювання та фінансування.

За результатами проведених розрахунків було встановлено, що середнє значення інтегральних показників для матеріального виробництва становить 0,2641, для нематеріального виробництва – 0,2594, а для невиробничої сфери – 0,2950.

Усі зазначені значення знаходяться на низькому рівні, що за шкалою оцінювання (0,00 – 0,30 – низький рівень) свідчить про критичний стан забезпечення ОД та обмежені можливості системи виконувати необхідні функції. Найменший рівень уваги, згідно з отриманими даними, спостерігається у сфері нематеріального виробництва (0,2594), що особливо небезпечно, оскільки саме ця сфера є фундаментальною для розвитку знань, підготовки кадрів та створення інформаційно-аналітичних ресурсів.

Проведення цього етапу є вкрай важливим для подальшого формування стратегій забезпечення ОД України, оскільки він дозволяє визначити пріоритетні напрями фінансування та організаційно-управлінських рішень, спрямованих на усунення дисбалансів між сферами та посилення слабких ланок у системі ОД (рис. 4).

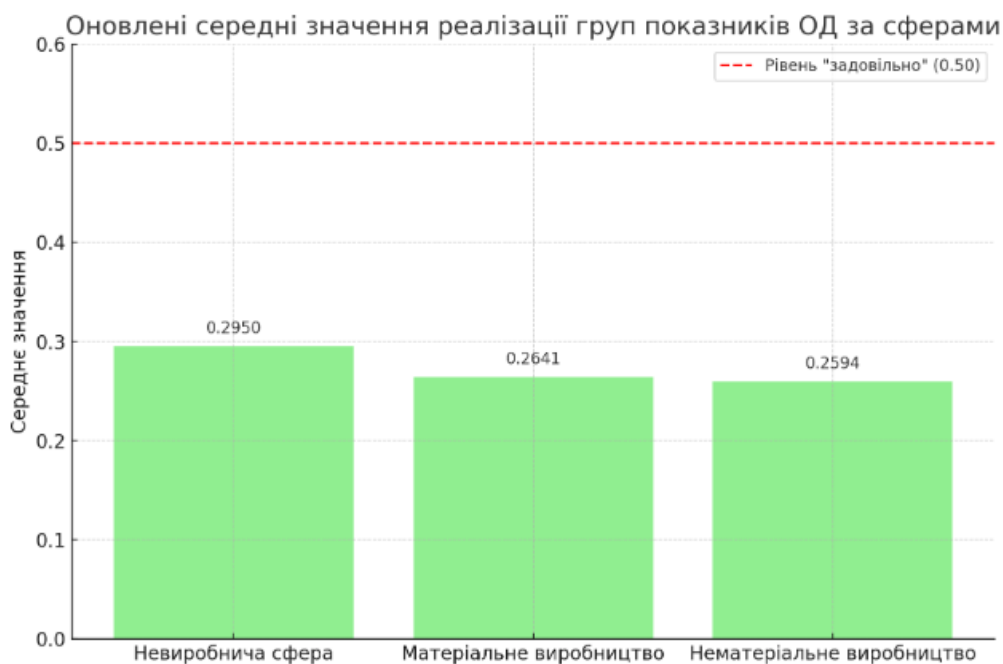


Рисунок 4 – Результати оцінювання важливості у функціонуванні сфер забезпечення ОД України

Джерело: результати розрахунків авторів

На четвертому етапі дослідження було здійснено побудову балансової моделі, що базується на застосуванні балансового методу зіставлення активів та пасивів у трьох сферах національного господарства: невиробничій, матеріальній та нематеріальній. Такий методологічний підхід дозволив визначити структурно-функціональні особливості забезпечення ОД на рівні країни або організації, шляхом виявлення співвідношення між наявними ресурсами (активами) та джерелами їх фінансування (пасивами).

Метою цього етапу було отримання аналітичної картини про ресурсну базу у зазначених сферах, а також виявлення потенційних дисбалансів, які можуть свідчити про надмірну залежність певних секторів від зовнішніх джерел підтримки чи, навпаки, про

надлишкову концентрацію на внутрішніх потужностях. Таке дослідження є важливим для формування ефективної стратегії управління оборонними ресурсами та забезпечення стійкості у разі змін зовнішнього середовища.

Результати побудови моделі засвідчили різноспрямовані тенденції. Зокрема, у сфері матеріального виробництва встановлено домінування активів над пасивами, що свідчить про значну концентрацію ресурсів на наявних виробничих потужностях. У відсотковому вираженні співвідношення активів до пасивів у цій сфері становило понад 65% на користь активів, що вказує на відносну незалежність від зовнішніх джерел фінансування, але одночасно може означати ризики пов'язані з недофінансуванням інноваційних напрямів та обмежену гнучкість системи.

Натомість у сферах невиробничій та нематеріального виробництва спостерігалось переважання пасивів над активами: у першій сфері пасиви перевищують активи на 20–25%, а у другій – на 15–18%, що свідчить про високу залежність цих секторів від зовнішньої допомоги та міжнародних альянсів.

Подібна диспропорція може бути критичним сигналом для прийняття управлінських рішень, оскільки у разі скорочення зовнішньої підтримки ці сфери можуть зазнати суттєвих втрат у функціональності та стійкості.

Отримані результати дають змогу ідентифікувати слабкі місця у структурі ресурсного забезпечення та визначити напрями, які потребують першочергового зміцнення, включаючи інвестиції у передові технології, підвищення кадрового потенціалу та розвиток інфраструктури.

На заключному етапі Методики є доцільним впровадження цілісної Матриці прийняття рішень, яка б ґрунтувалася на ретельному зіставленні ключових етапів Методики (рис. 5), що визначають ефективність та релевантність управлінських дій у сфері безпеки.

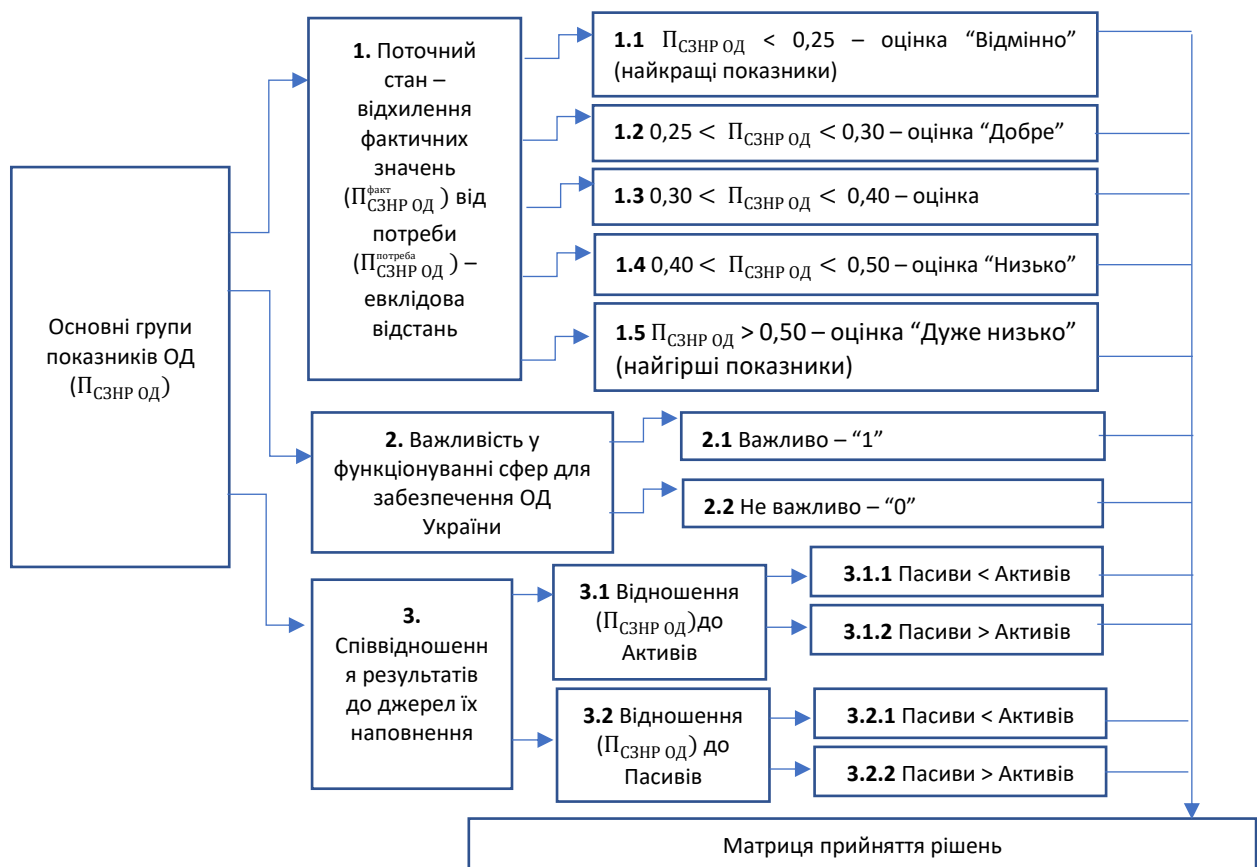


Рисунок 5 – Графічна інтерпретація алгоритму формування Матриці прийняття рішень для обґрунтування шляхів забезпечення необхідного рівня ОД

Джерело: доробок авторів

Поєднання зазначених чинників створює підґрунтя для побудови Матриці прийняття рішень (табл 1), у якій на перетині різних комбінацій значень (стан, важливість, баланс ресурсів) формуються стратегічні рекомендації щодо подальших дій – від підтримки поточного стану та цільового інвестування у розвиток до реструктуризації ресурсів або тимчасової консервації відповідного напрямку.

Внаслідок застосування такого прийому стає можливим формулювання конкретних цільових заходів. До них можуть належати, зокрема, зміна структури фінансування, перерозподіл ресурсів між більш і менш пріоритетними напрямками, впровадження освітніх програм для персоналу, модернізація технічного парку, активізація міжнародного співробітництва або, за потреби, оптимізація функціонування системи через тимчасове призупинення реалізації малоефективних ініціатив тощо.

Таким чином, результати п'ятого етапу не лише дозволяють сформулювати обґрунтовану позицію щодо подальших кроків державної політики у сфері оборони, але й забезпечують створення гнучкої, адаптивної та динамічно оновлюваної дорожньої карти стратегічного планування, яка враховує реальний стан, наявні можливості, зовнішні загрози та внутрішні обмеження, з метою досягнення стійкого і цілеспрямованого підвищення рівня ОД країни в умовах постійних змін безпекового середовища.

Отже проводиться обґрунтування шляхів забезпечення необхідного рівня ОД за можливими 56-ма варіантами у Матриці прийняття рішень (за трьома параметрами: евклідова відстань фактичних даних від планових, важливість для розвитку сфери національного господарства, відношення до пасивів чи активів) – табл. 2.

$$\text{Шлях} = f(\Pi_{\text{СЗНР ОД}}^{\text{ЕвВід}}, \text{Матриця В}, \delta),$$

де f – це мапінг із простору $\Pi_{\text{СЗНР ОД}}^{\text{ЕвВід}} \cdot \text{Матриця В} \cdot \delta$ у множину $\{1, 2, \dots, 5, 6\}$, відповідно до таблиці рішень.

Таблиця 1 – Матриця прийняття рішень щодо обґрунтування шляхів забезпечення необхідного рівня ОД

Шлях	Стан	Важливість	Джерело	Інтерпретація	Загальні дії
1	1.1	2.1	3.1.1	Відмінно, важливо, Активи > Пасивів	Підтримувати стан, інвестувати в розвиток
2	1.1	2.1	3.1.2	Відмінно, важливо, Пасиви > Активів	Оптимізувати баланс, зменшити залежність від пасивів
3	1.1	2.1	3.2.1	Відмінно, важливо, Пасиви < Активів	Зміцнити активну частину, уникати накопичення пасивів
4	1.1	2.1	3.2.2	Відмінно, важливо, Пасиви > Активів	Посилити стабільність джерел фінансування
5	1.1	2.2	3.1.1	Відмінно, неважливо, Активи > Пасивів	Підтримувати, без пріоритетного фінансування
6	1.1	2.2	3.1.2	Відмінно, неважливо, Пасиви > Активів	Утримання поточного рівня, уникати надлишкових витрат
7	1.1	2.2	3.2.1	Відмінно, неважливо, Пасиви < Активів	Легкий моніторинг, втручання не потрібне
8	1.1	2.2	3.2.2	Відмінно, неважливо, Пасиви > Активів	Контроль на випадок зростання ризиків
9	1.2	2.1	3.1.1	Добре, важливо, Активи > Пасивів	Локальна оптимізація, укріплення ресурсної бази
10	1.2	2.1	3.1.2	Добре, важливо, Пасиви > Активів	Зниження навантаження пасивів, перерозподіл фондів
11	1.2	2.1	3.2.1	Добре, важливо, Пасиви < Активів	Удосконалити розподіл активів, модернізація

Шлях	Стан	Важли- вість	Джерело	Інтерпретація	Загальні дії
12	1.2	2.1	3.2.2	Добре, важливо, Пасиви > Активів	Фінансова реструктуризація, зниження ризиків
13	1.2	2.2	3.1.1	Добре, неважливо, Активи > Пасивів	Підтримка стабільності, без активного втручання
14	1.2	2.2	3.1.2	Добре, неважливо, Пасиви > Активів	Запобігання розбалансованості, заощадження
15	1.2	2.2	3.2.1	Добре, неважливо, Пасиви < Активів	Моніторинг, без нарощування обсягів
16	1.2	2.2	3.2.2	Добре, неважливо, Пасиви > Активів	Зберігати контроль, уникати надмірного розширення
17	1.3	2.1	3.1.1	Задовільно, важливо, Активи > Пасивів	Оптимізувати розподіл активів, підвищити ефективність існуючих ресурсів
18	1.3	2.1	3.1.2	Задовільно, важливо, Пасиви > Активів	Скоротити пасиви, інвестувати в ефективні активи
19	1.3	2.1	3.2.1	Задовільно, важливо, Пасиви < Активів	Підсилити контроль над пасивами, стабілізувати ресурсну базу
20	1.3	2.1	3.2.2	Задовільно, важливо, Пасиви > Активів	Реструктуризація боргів, пошук зовнішнього фінансування
21	1.3	2.2	3.1.1	Задовільно, неважливо, Активи > Пасивів	Мінімальне втручання, моніторинг
22	1.3	2.2	3.1.2	Задовільно, неважливо, Пасиви > Активів	Контроль витрат, уникнення росту пасивів
23	1.3	2.2	3.2.1	Задовільно, неважливо, Пасиви < Активів	Збереження балансу, уникнення розширення пасивів
24	1.3	2.2	3.2.2	Задовільно, неважливо, Пасиви > Активів	Відкласти інвестиції, уникати ризиків
25	1.4	2.1	3.1.1	Низько, важливо, Активи > Пасивів	Посилити активи, модернізувати ресурси
26	1.4	2.1	3.1.2	Низько, важливо, Пасиви > Активів	Зменшити пасиви, переорієнтувати фінансування
27	1.4	2.1	3.2.1	Низько, важливо, Пасиви < Активів (пасивна сфера)	Розширити резерви, підсилити базу
28	1.4	2.1	3.2.2	Низько, важливо, Пасиви > Активів (пасивна сфера)	Критична реструктуризація, зменшити залежність
29	1.4	2.2	3.1.1	Низько, неважливо, Активи > Пасивів	Підтримка статусу-кво, локальні вдосконалення
30	1.4	2.2	3.1.2	Низько, неважливо, Пасиви > Активів	Уникати надмірних витрат, пасивна підтримка
31	1.4	2.2	3.2.1	Низько, неважливо, Пасиви < Активів	Моніторинг ситуації, без нових вкладень
32	1.4	2.2	3.2.2	Низько, неважливо, Пасиви > Активів	Обмежити діяльність, тимчасова консервація
33	1.4	2.1	3.1.1	Низько, важливо, Активи > Пасивів	Технічне переоснащення, ефективне використання активів
34	1.4	2.1	3.1.2	Низько, важливо, Пасиви > Активів	Фінансова оптимізація, зменшення боргового навантаження
35	1.4	2.1	3.2.1	Низько, важливо, Пасиви < Активів	Підвищення готовності резервних структур
36	1.4	2.1	3.2.2	Низько, важливо, Пасиви > Активів	Кризовий менеджмент, екстрене управління
37	1.4	2.2	3.1.1	Низько, неважливо, Активи > Пасивів	Збереження поточних можливостей, низький пріоритет
38	1.4	2.2	3.1.2	Низько, неважливо, Пасиви > Активів	Обмежене фінансування, лише базові функції

Шлях	Стан	Важли- вість	Джерело	Інтерпретація	Загальні дії
39	1.4	2.2	3.2.1	Низько, неважливо, Пасиви < Активів	Фонове спостереження, обмежене залучення ресурсів
40	1.4	2.2	3.2.2	Низько, неважливо, Пасиви > Активів	Мінімізація активності, виведення з пріоритетів
41	1.5	2.1	3.1.1	Дуже низько, важливо, Активи > Пасивів	Негайна реформа, інвестування в активи, підсилення інституцій
42	1.5	2.1	3.1.2	Дуже низько, важливо, Пасиви > Активів	Фінансова санація, реструктуризація боргів, пошук грантів
43	1.5	2.1	3.2.1	Дуже низько, важливо, Пасиви < Активів	Оптимізувати структуру витрат, використати внутрішній резерв
44	1.5	2.1	3.2.2	Дуже низько, важливо, Пасиви > Активів	Фінансова підтримка ззовні, ліквідація надлишкових пасивів
45	1.5	2.2	3.1.1	Дуже низько, неважливо, Активи > Пасивів	Обмежене втручання, перегляд необхідності функції
46	1.5	2.2	3.1.2	Дуже низько, неважливо, Пасиви > Активів	Уникати інвестування, заморозка ініціатив, збереження ресурсів
47	1.5	2.2	3.2.1	Дуже низько, неважливо, Пасиви < Активів	Пасивний моніторинг, консервування наявного
48	1.5	2.2	3.2.2	Дуже низько, неважливо, Пасиви > Активів	Можлива ліквідація, оптимізація системи управління
49	1.5	2.1	3.1.1	Дуже низько, важливо, Активи > Пасивів	Негайна реформа, інвестування в активи, підсилення інституцій
50	1.5	2.1	3.1.2	Дуже низько, важливо, Пасиви > Активів	Фінансова санація, реструктуризація боргів, пошук грантів
51	1.5	2.1	3.2.1	Дуже низько, важливо, Пасиви < Активів	Оптимізувати структуру витрат, використати внутрішній резерв
52	1.5	2.1	3.2.2	Дуже низько, важливо, Пасиви > Активів	Фінансова підтримка ззовні, ліквідація надлишкових пасивів
53	1.5	2.2	3.1.1	Дуже низько, неважливо, Активи > Пасивів	Обмежене втручання, перегляд необхідності функції
54	1.5	2.2	3.1.2	Дуже низько, неважливо, Пасиви > Активів	Уникати інвестування, заморозка ініціатив, збереження ресурсів
55	1.5	2.2	3.2.1	Дуже низько, неважливо, Пасиви < Активів	Пасивний моніторинг, консервування наявного
56	1.5	2.2	3.2.2	Дуже низько, неважливо, Пасиви > Активів	Можлива ліквідація, оптимізація системи управління

Джерело: доробок авторів

Таблиця 2 – Матриця прийняття рішень щодо обґрунтування шляхів забезпечення необхідного рівня ОД

№ з/п	Напрямок	Стан оцінки	Важливість	Спів- відношення (А/П)	Рекомендований шлях
1	ВПТСР	Задовільно	Важливо	Активи = Пасиви	Шлях 17: оптимізувати розподіл активів
2	ПСПО	Добре	Важливо	Пасиви > Активів	Шлях 10: зниження навантаження пасивів
3	КВІ	Добре	Важливо	Пасиви < Активів	Шлях 11: модернізація активів
4	ТДІВТ	Відмінно	Важливо	Активи > Пасивів	Шлях 1: підтримка та розвиток
5	ПГОС	Дуже низько	Важливо	Пасиви > Активів	Шлях 42: фінансова санація
6	САМСР	Задовільно	Важливо	Пасиви > Активів	Шлях 20: реструктуризація боргів

№ з/п	Напрямок	Стан оцінки	Важливість	Спів-відношення (А/П)	Рекомендований шлях
7	БГРЗ	Відмінно	Важливо	Пасиви < Активів	Шлях 3: зміцнення активної частини
8	ІМО	Низько	Важливо	Пасиви > Активів	Шлях 26: переорієнтація фінансування
9	ЗРІВЗ	Дуже низько	Важливо	Пасиви > Активів	Шлях 42/50: фінансова реформа

Джерело: результати розрахунків автора.

Отже за результатами аналізу (на даний час) визначено наступні шляхи забезпечення необхідного рівня ОД:

1. ВПТСР – Шлях 17: оптимізація розподілу активів.

У напрямку ВПТСР наразі спостерігається баланс між активами і пасивами, що створює умови для підвищення ефективності без залучення додаткових ресурсів. Основним завданням є не розширення наявної бази, а оптимальний перерозподіл існуючих потужностей. Для цього необхідно провести всебічний аудит чинних інвестицій у сенсорні системи, безпілотні літальні апарати та аналітичне програмне забезпечення, після чого реалізувати передислокацію ресурсів – як технічних, так і кадрових – у найбільш критичні підрозділи. Водночас важливо вдосконалити програмні рішення для збору й обробки інформації, а також усунути дублювання функцій задля досягнення більшої точності й ефективності при менших витратах.

2. ПСПО – Шлях 10: зниження навантаження пасивів.

У сегменті ПСПО виявлено дисбаланс, за якого пасиви перевищують активи, що свідчить про надмірне фінансове навантаження або неефективну витрату ресурсів. Для виправлення цієї ситуації необхідно здійснити реструктуризацію застарілих або малоефективних систем, переглянувши їхню доцільність у сучасному контексті. Також доцільним є оптимізація витрат на технічне обслуговування, включно з можливістю списання або консервації застарілого обладнання. Варто зменшити адміністративне навантаження шляхом скорочення надлишкових структур і ліквідації дублюючих функцій, а також розширити пошук зовнішнього фінансування або міжнародної кооперації для полегшення внутрішнього тиску на бюджет.

3. КВІ – Шлях 11: модернізація активів.

У напрямку КВІ активи наразі мають домінуючу роль, однак їхній технічний стан вимагає оновлення відповідно до актуальних викликів. Необхідно спрямувати інвестиції у сучасні платформи кіберзахисту, зокрема у SIEM-системи та інструменти для моніторингу загроз. Паралельно з цим слід підвищити кваліфікацію персоналу через навчальні курси з кібервійни та криптографії, а також запровадити автоматизовані системи реагування на кіберінциденти. Важливою також є модернізація апаратної інфраструктури – зокрема, серверного обладнання в дата-центрах та центрах управління системами.

4. ТДІВТ – Шлях 1: підтримка та розвиток.

Напрямок ТДІВТ перебуває у стані найвищої ефективності, де обсяг активів перевищує потреби. У такій ситуації головне завдання полягає у підтриманні наявного рівня і масштабуванні найуспішніших рішень. Доцільно продовжити фінансування науково-дослідних інститутів та підприємств військово-промислового комплексу, які спеціалізуються на новітніх технологіях, одночасно розширюючи міжнародне партнерство з метою реалізації спільних дослідницько-інженерних проєктів. Також важливо створити умови для оперативного впровадження інновацій безпосередньо у військові структури, забезпечуючи при цьому технічне обслуговування та сервісну підтримку нових зразків озброєння.

5. ПГОС – Шлях 42: фінансова санація

У сфері ПГОС спостерігається критичний дисбаланс, що зумовлений надмірними пасивами й вимагає термінового фінансового втручання. Необхідно розпочати з комплексної оцінки наявного бюджету з подальшим скороченням усіх витрат, які не мають стратегічного значення. Кошти з неактуальних програм доцільно спрямувати на розвиток напрямків, пов'язаних зі стресостійкістю та медичною підготовкою військовослужбовців. Також слід розглянути можливість закриття застарілих полігонів і тренувальних центрів, а у кадровій структурі – здійснити звільнення, ротацію або перекваліфікацію персоналу з метою досягнення більшої ефективності.

6. САМСП – Шлях 20: реструктуризація боргів.

У напрямку САМСП накопичення зовнішніх зобов'язань почало перевантажувати систему, що створює необхідність у перегляді підходів до управління борговими пасивами. Пріоритетним кроком є ініціювання перемовин щодо відтермінування або перегляду поточних міжнародних зобов'язань. Крім того, слід оптимізувати існуючі проекти міжнародної підтримки, зосередившись лише на тих, які мають критичне значення, а частину систем – перевести на спільне фінансування у форматі кооперації або програм НАТО. Деякі партнерства доцільно трансформувати в модель обміну досвідом, що не потребує значних ресурсів.

7. БГРЗ – Шлях 3: зміцнення активної частини.

У напрямку БГРЗ вже наявна базова ресурсна платформа, яку необхідно посилити для підвищення практичної боєздатності. У цьому контексті доцільно активізувати розвиток бойової логістики, а також покращити координацію між штабами та передовими підрозділами. Варто організувати масштабні навчання з реагування на бойові загрози та здійснити інвестиції в технічні засоби – включно з системами зв'язку, ППО та розвідувальними БПЛА. Крім того, слід забезпечити постійне бойове чергування у районах підвищеного ризику.

8. ІМО – Шлях 26: переорієнтація фінансування.

Інформаційно-медійний операційний напрям (ІМО) страждає від хронічного недофінансування та неефективного розподілу ресурсів, що потребує кардинального перегляду фінансової стратегії. Необхідно скоротити фінансування другорядних напрямків, таких як ремонт застарілої техніки, натомість перенаправивши кошти на закупівлю сучасного обладнання, що дозволить здійснити модернізацію. Фінансування має бути переведено у проєктно-орієнтовану модель, де гроші надаються під конкретний результат, а не просто за факт існування напрямку. Також критично важливо забезпечити прозорість у витрачанні коштів через механізми звітування та аудиту.

9. ЗРІВЗ – Шлях 42/50: фінансова реформа.

У напрямку ЗРІВЗ спостерігається найгірший стан серед усіх секторів, що вимагає негайної фінансової та структурної реформи. Передусім слід провести повну ревізію бюджету, з подальшим переходом від фрагментарного до централізованого фінансування. Також потрібно створити єдиний координаційний орган, відповідальний за збір і обробку розвідувальної інформації, та активізувати залучення альтернативних джерел фінансування, таких як державне-приватне партнерство або міжнародні гранти.

Тому кожен зі шляхів, окреслених у цьому переліку, є конкретним управлінським кроком, адаптованим до специфіки відповідного напрямку та його слабких місць. Сукупність цих рішень формує цілісну стратегію з підвищення оборонної спроможності України, орієнтовану на досягнення балансу між ефективністю та доступністю ресурсів.

Висновки

Проведене дослідження розкриває результати чисельного експерименту за запропонованою методикою обґрунтування шляхів забезпечення необхідного рівня ОД держави, яка поєднує якісні та кількісні підходи та забезпечує комплексність оцінювання та формування стратегічно виважених управлінських рішень. Наукова новизна дослідження полягає у формалізації

процесу прийняття рішень за допомогою багатокритеріальної матриці, що дозволяє комплексно оцінити альтернативні напрямки розвитку оборонних спроможностей і обрати оптимальні управлінські рішення. Застосування такого підходу сприятиме більш об'єктивному та прозорому обґрунтуванню стратегічних пріоритетів зміцнення оборонного потенціалу України в умовах обмежених ресурсів та невизначеності безпекового середовища.

Подальші дослідження доцільно зосередити на удосконаленні методики шляхом інтеграції динамічних моделей прогнозування, розширенні критеріїв оцінювання, а також на її апробації в умовах міждержавної взаємодії, що дозволить підвищити ефективність управління оборонними ресурсами та адаптивність системи до можливих нових загроз.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Богданович, В. (2024). Концептуальна модель і система показників оцінювання рівнів оборонної достатності для забезпечення воєнної безпеки держави на основі визначення ризиків реалізації кризових сценаріїв. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки*, 92(3), 17–26. <https://doi.org/10.32453/3.v92i3.1472>
2. SIPRI. (2025, квітень). Trends in world military expenditure. London: SIPRI. URL : https://www.sipri.org/sites/default/files/2025-04/2504_fs_milex_2024.pdf
3. RAND Corporation. (2025, червень). Modernizing Department of Defense Civilian Human Resources: Harnessing AI for Transformative Change. RAND Corporation. URL : https://www.rand.org/pubs/research_reports/RR3462-1.html
4. European Defence Agency. (2025, березень). EDA Annual Report 2024. Brussels: EDA. URL : <https://eda.europa.eu/docs/default-source/brochures/eda-annual-report-2024.pdf>
5. Сироватко В. В. Трансформація оборонного потенціалу України в умовах збройної агресії : дис. ... д-ра філософії : 052 – політологія / Сироватко Віктор Володимирович ; наук. кер. Вовк С. О. ; Держ. закл. «Луганський національний університет імені Тараса Шевченка». – Полтава, 2025. – 306 с. URL : <http://dspace.luguniv.edu.ua/xmlui/handle/123456789/11183>
6. Семененко, О., Абрамова, М., Таран, О., Побережець, Т., Кравченко, Є., & Паламарчук, С. (2023). Аналіз теорії та практики визначення, обґрунтування та оцінювання оборонної достатності держави. *Social Development and Security*, 13(1), 38–51. <https://doi.org/10.33445/sds.2023.13.1.5>
7. Малишев, О. Оборонне планування на основі спроможностей в Україні: поточний стан і перспективи. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняхівського*. 2021. № 3-70. С. 54–61. URL: <https://doi.org/10.33099/2304-2745/2020-3-70/54-61>
8. Ткач, М. Проблеми оборонного менеджменту: теорія і практика: матеріали Науково-практичної конференції (Київ, 26 жовтня 2023 року). *Національний університет оборони України*. Київ, 2023. 213 с.

References

1. Bohdanovych, V. (2024). Kontseptualna model i systema pokaznykiv otsiniuvannia rivniv oboronnoi dostatnosti dlia zabezpechennia voiennoi bezpeky derzhavy na osnovi vyznachennia ryzykiv

- realizatsii kryzovykh stsensariiv. *Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Seriya: Viiskovi ta tekhnichni nauky*, 92(3), 17–26.
<https://doi.org/10.32453/3.v92i3.1472>
2. Stockholm International Peace Research Institute (SIPRI). (2025, April). *Trends in world military expenditure*. London: SIPRI. Available from : https://www.sipri.org/sites/default/files/2025-04/2504_fs_milex_2024.pdf
 3. RAND Corporation. (2025, June). *Modernizing Department of Defense civilian human resources: Harnessing AI for transformative change*. RAND Corporation. Available from : https://www.rand.org/pubs/research_reports/RRA3462-1.html
 4. European Defence Agency. (2025, March). *EDA annual report 2024*. Brussels: European Defence Agency. Available from : <https://eda.europa.eu/docs/default-source/brochures/eda-annual-report-2024.pdf>
 5. Syrovatko, V. V. (2025). *Transformation of Ukraine's defense potential under conditions of armed aggression* (Doctoral dissertation, Taras Shevchenko Luhansk National University, Poltava). 306 p. Available from : <http://dspace.luguniv.edu.ua/xmlui/handle/123456789/11183>
 6. Semenenko, O., Abramova, M., Taran, O., Poberezhets, T., Kravchenko, Y., & Palamarchuk, S. (2023). Analysis of the theory and practice of defining, justifying and evaluating the defense adequacy of the state. *Social Development and Security*, 13(1), 38-51.
<https://doi.org/10.33445/sds.2023.13.1.5>
 7. Malyshev, O. (2021). Capability-based defense planning in Ukraine: Current state and prospects. *Collection of Scientific Papers of the Center for Military-Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskyi*, (3-70), 54–61.
<https://doi.org/10.33099/2304-2745/2020-3-70/54-61>
 8. Tkach, M. (2023). Problems of defense management: Theory and practice. In *Proceedings of the Scientific and Practical Conference* (Kyiv, October 26, 2023). National Defence University of Ukraine. Kyiv. 213 p.

Методика оцінювання здатності національної економіки забезпечити її оборонний потенціал: структурно-логічна схема та алгоритм

Methodology for Assessing the Ability of a National Economy to Ensure Its Defense Potential: Structural and Logical Scheme and Algorithm

Igor Moskalenko

здобувач, e-mail: kidmos@bigmir.net, ORCID: 0000-0002-7822-6419

Національний університет оборони України, Київ, Україна

Ihor Moskalenko

PhD student, e-mail: kidmos@bigmir.net, ORCID: 0000-0002-7822-6419

National Defence University of Ukraine, Kyiv, Ukraine

Received: August 03, 2025 | Revised: August 28, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.23>

Мета роботи. Розробити структурно-логічну схему та алгоритм методики оцінювання здатності національної економіки забезпечити її оборонний потенціал.

Метод дослідження. Методи аналізу та синтезу, порівняння, стратегічного аналізу, експертного опитування, метод зважених показників.

Результати дослідження. Аналіз існуючих підходів щодо оцінювання здатності національної економіки держави забезпечити її оборонний потенціал; структурно-логічна схема та алгоритм методики оцінювання здатності національної економіки забезпечити її оборонний потенціал; практичний приклад оцінювання здатності національної економіки України забезпечити її оборонний потенціал за основними складовими; приклад діапазонів нечітких шкал оцінювання стану оборонного потенціалу та здатності національної економіки держави щодо забезпечення його достатнього рівня.

Теоретична цінність дослідження. Результати дослідження можуть використовуватися фахівцями органів військового управління вищого рівня, а також фахівцями державного управління та науковцями за напрямом воєнно-економічних досліджень.

Тип статті. Теоретичний.

Purpose. To develop a structural and logical scheme and algorithm for the methodology for assessing the ability of the national economy to ensure its defense potential.

Method. Methods of analysis and synthesis, comparison, strategic analysis, expert survey, weighted indicator method.

Findings. Analysis of existing approaches to assessing the ability of the national economy of a state to ensure its defense potential; structural and logical scheme and algorithm of the methodology for assessing the ability of the national economy to ensure its defense potential; a practical example of assessing the ability of the national economy of Ukraine to ensure its defense potential by main components; an example of ranges of fuzzy scales for assessing the state of the defense potential and the ability of the national economy of a state to ensure its sufficient level.

Theoretical implications. The results of the study can be used by specialists of higher-level military command bodies, as well as by public administration specialists and scientists in the field of military-economic research.

Paper type. Theoretical.

Ключові слова: воєнно-економічний потенціал, достовірність оцінювання, національна економіка, національна безпека, оборонний потенціал, макроекономічний ефект, оцінювання стану оборонного потенціалу.

Key words: military-economic potential, assessment reliability, national economy, national security, defense potential, macroeconomic effect, assessment of the state of defense potential.

Вступ

Проблематика оцінювання здатності національної економіки держави забезпечувати її оборонний потенціал набула особливої актуальності в умовах сучасних воєнно-економічних викликів [1–4]. Спроби математичного обґрунтування взаємозв'язку між воєнними витратами та економічним розвитком здійснювалися багатьма зарубіжними й вітчизняними дослідниками [1–20]. Проте в науковому доробку України досі відсутня цілісна методика, яка б дозволяла на основі формалізованих підходів визначати вплив оборонних витрат на зміну макроекономічних показників та стан національної економіки загалом. Це зумовлює необхідність розроблення спеціального методичного апарату, що забезпечував би можливість комплексного оцінювання здатності економіки держави формувати та підтримувати достатній рівень оборонного потенціалу. Такий апарат має не лише враховувати вплив воєнних витрат на економічну динаміку, а й дозволяти здійснювати оптимізацію фінансування потреб Збройних Сил з метою досягнення максимального макроекономічного ефекту при збереженні належного рівня обороноздатності.

Отже, забезпечення оборонного потенціалу (ОП) – це економіко-управлінська діяльність, яка дозволяє державі гарантувати готовність ЗС та інших складових сектору безпеки і оборони до виконання завдань за призначенням.

Під поняттям “достатнього рівня оборонного потенціалу” будемо розуміти такий стан воєнно-економічних і ресурсних можливостей держави, який: відповідає масштабу та характеру загроз національній безпеці; забезпечує стійкість функціонування військової організації держави у мирний час і в особливий період; дозволяє підтримувати стратегічну воєнну рівновагу на регіональному та глобальному рівнях; є економічно збалансованим, тобто не підриває стабільність розвитку держави в довгостроковій перспективі [1–20].

Інакше кажучи, “достатній рівень оборонного потенціалу” – це такий мінімально необхідний і водночас оптимальний рівень оборонних ресурсів та спроможностей, який дозволяє державі відвертати загрози, стримувати агресора та успішно вести оборонні дії.

Під процесом оцінювання здатності національної економіки держави до забезпечення її оборонного потенціалу будемо розуміти процес кількісного та якісного визначення можливостей національної економіки у формуванні та підтриманні оборонного потенціалу на необхідному рівні. Його сутність полягає у: виявленні ключових економічних факторів (ВВП, макроекономічна стабільність, енергетична безпека, розвиток ОПК, інвестиційний клімат, мобілізаційні ресурси тощо); визначенні їхнього впливу на обороноздатність держави; побудові системи критеріїв і показників, що відображають реальну здатність економіки забезпечувати сектор безпеки й оборони; застосуванні моделей, які дозволяють здійснювати прогнозування та оптимізацію розподілу ресурсів. Таким чином, оцінювання – це інструмент виявлення меж та резервів економіки у сфері оборонного будівництва.

Теоретичні основи дослідження

Питання оцінювання здатності національної економіки забезпечити оборонний потенціал набуло критично важливого значення у зв’язку з сучасною системною гібридною агресією, спрямованою проти суверенітету держав, у тому числі з урахуванням триваючої російсько-української війни. Розриви в логістиці, руйнування інфраструктури, демографічні втрати, шкоди промисловим і енергетичним активам, а також мультиплікаційні економічні ефекти потребують від держави не лише відновлення виробничих потужностей, але й наявності методики, яка забезпечує:

- кількісну та якісну оцінку ресурсів (фінансових, матеріальних, людських), які можуть бути мобілізовані на оборону;

- прогнозування здатності економіки підтримувати тривалий опір (за різних сценаріїв тривалості війни);

- ідентифікацію вразливих секторів і вузьких місць у ланцюгах постачання;

- обґрунтування стратегічних пріоритетів військово-економічної політики та заходів державно-приватної координації.

У воєнних умовах потреба такої методики – це питання не тільки економічної науки, а й національної безпеки.

Проведемо аналіз існуючих підходів іноземних та вітчизняних авторів (інституцій) щодо оцінювання здатності національної економіки держави забезпечити її оборонний потенціал (табл. 1.2). У табл. 1 розкрито результати досліджень авторів за напрямом оцінювання здатності національної економіки держави забезпечити її оборонний потенціал [1–20].

Таблиця 1 – Результати аналізу існуючих підходів щодо оцінювання здатності національної економіки держави забезпечити її оборонний потенціал

Автор / Інституція	Тема / предмет дослідження	Основні результати / підходи	Що залишилося недослідженим / обмеження
Keith Hartley (defence economics)	Економічні основи оборонних витрат, оцінка ефективності витрат на оборону	Розробка теоретичних рамок для оцінки оборонних витрат, аналіз взаємозв'язку оборонної політики та економіки	Менше уваги до оцінки стійкості ланцюгів постачання під масованими руйнуваннями; обмежена орієнтація на контекст пост-конфлікту
Todd Sandler (economics of conflict, public goods)	Моделі колективного дійства, витрати на безпеку як публічне благо	Теорії оптимального розподілу ресурсів на безпеку, макроекономічні моделі впливу конфлікту	Потреба у більш прикладних інструментах для оцінки мобілізаційної спроможності конкретних секторів
Paul Bracken / Barry Posen / інші стратеги	Взаємозв'язок стратегії, промисловості та мобілізації ресурсів	Аргументація важливості промислових баз та довгострокової стратегії мобілізації	Не завжди формалізовано економічні індикатори для національної “витривалості” у масштабі десятиліть
RAND Corporation (багато авторів)	Оцінки оборонної промисловості, сценарні аналізи, моделювання постачань	Прикладні моделі (сценарії, вразливості ланцюгів), рекомендації політикам	Результати часто контекстно-залежні; потребують адаптації до країн із руйнуванням об'єктів інфраструктури
NATO / EU resilience reports	Стійкість критичної інфраструктури; whole-of-government підхід	Концепти «resilience», індикатори готовності суспільства; рекомендації щодо інституцій	Не завжди містять кількісних економічних моделей для оцінки воєнного потенціалу ВВП-рівня
World Bank / UN / RDNA assessments	Rapid Damage & Needs Assessment; оцінки потреб відновлення	Методики оцінки руйнувань, інвестиційні потреби, пріоритезація секторів	Зазвичай орієнтовані на відновлення/реконструкцію, а не на довгострокову оборонну спроможність
Defense industrial policy researchers (economics of supply chains)	Аналіз оборонно-промислових кластерів і локальних ланцюгів	Індикатори здатності внутрішнього виробництва, залежності від імпорту	Менше уваги до демографічних та соціальних чинників, що впливають на мобілізаційний ресурс
Міжнародні економісти (макро-моделі війни)	Вплив війни на ВВП, інвестиції, інфляцію та бюджетні обмеження	Макроекономічні сценарні моделі, оцінки короткострокових шоків	Потреба в інтегруванні військово-стратегічних змін у моделі (оперативний вимір)
Семененко О.М. (Метод оцінювання рівня воєнно-економічного потенціалу держави, 2016)	Розробка методів оцінки воєнно-економічного потенціалу на основі статистичних підходів (головні компоненти, кореляційний аналіз)	Створено модель оцінювання воєнно-економічного потенціалу України (2013–2016), що враховує економічні, демографічні та військові чинники.	Обмеженість часових рамок; відсутність сценарного аналізу; не враховані секторні (енергетика, транспорт) та мобілізаційні складові.

Результати аналізу показують, що воєнно-економічний та оборонний потенціал повинні розглядатися як комплексна характеристика, яка поєднує економічну міцність держави з її мобілізаційними та військово-організаційними можливостями. Аналіз існуючих підходів до оцінювання здатності національної економіки забезпечувати оборонний потенціал показав, що питання є надзвичайно актуальним у сучасних умовах, особливо з

урахуванням триваючої російсько-української війни. Дослідження провідних іноземних та вітчизняних авторів демонструють багатство наукових напрацювань у сфері економіки оборони, макроекономічного моделювання, аналізу ланцюгів постачання та оцінки стійкості суспільства. Водночас наявні підходи залишаються фрагментарними: одні концентруються на бюджетних аспектах, інші – на теоретичних моделях конфлікту, ще інші – на оцінках збитків або відновлення.

Постановка проблеми

Ключові особливості цих досліджень свідчать про високу якість окремих напрацювань. Наявний науковий доробок закладає важливе підґрунтя, але водночас виявляє суттєву прогалину щодо відсутності єдиної, системної та адаптивної методики, яка дозволяла б уніфіковано оцінювати здатність економіки забезпечувати оборонний потенціал у різних сценаріях війни та відновлення. Отже, формування та впровадження такої методики є не лише науковим завданням, а й практичною вимогою національної безпеки, без реалізації якої Україна та інші країни, що перебувають у зоні воєнних ризиків, не зможуть ефективно забезпечувати стійкість та обороноздатність у XXI столітті.

Результати

Методика побудована на основі використання математичного апарату детермінованих та стохастичних моделей із використанням елементів методів факторного аналізу, експертного опитування та групування багатомірних спостережень. Стохастичні моделі застосовують під час оцінювання складових оборонного потенціалу держави, тому що детерміновані моделі факторних систем обмежені довжиною факторного поля прямих зв'язків та під час рішення поставленої задачі будуть виникати проблеми щодо недостатності інформаційної бази, яка описує прямі зв'язки до знання об'єктивної дійсності досліджуваного питання. Розмах кількісних змін економічних та воєнних показників можна з'ясувати тільки за допомогою використання стохастичного аналізу значної кількості емпіричних даних. Застосування стохастичного аналізу в методиці дозволить дослідити непрямі зв'язки опосередкованих факторів, якщо немає можливості визначити безперервний ланцюг прямого зв'язку між факторами та показниками, які досліджуються [6–20].

Стохастичний аналіз в цій задачі буде допоміжним інструментом детермінованого аналізу факторів, за якими неможливо буде побудувати детерміновану модель оцінки [15–18]. Специфікою додаткового застосування під час оцінювання здатності національної економіки забезпечити необхідний рівень оборонного потенціалу є виникнення та врахування невизначеностей під час формування конкретних значень як економічних, так і воєнних показників. Застосування детермінованих моделей разом із стохастичними дозволить вирішувати додатково такі завдання як: визначення наявності, напрямків та інтенсивності зв'язків між економічними та воєнними показниками; встановлення аналітичної форми зв'язку між показниками, що досліджуються; згладжування (виявлення трендів) динаміки досліджуваних показників; комплексна оцінка, ранжування та класифікація виробничих систем; виявлення та вибір найбільш інформативних показників (факторів) оцінки, формування нових синтетичних показників під час оцінювання; з'ясування внутрішньої структури зв'язків в системі як воєнних, так і економічних показників; порівняння структури зв'язків в різних сукупностях.

Головною метою методики є відображення показників-змінних – статистичних показників, які дають змогу чисельно оцінити складові ОП, які характеризують їх на момент оцінювання, через набір факторів (синтетичні фактори оцінювання оборонного потенціалу), що отримані з тих же самих змінних. У загальному вигляді розв'язання поставленої задачі можна розкласти на три стратегічних кроки (етапи).

Першим найбільш працемістким є формування вихідних даних щодо показників (кількість, ступінь взаємозв'язку тощо), які характеризують стан національної економіки держави та формування групи компетентних експертів у досліджуваному питанні. Процедура компетентності експертів має особливе та специфічне значення для цієї методики, бо від узгодженості думок експертів та їхнього фахового рівня за питаннями, які досліджуються, визначальним чином впливають на результати оцінювання.

Другим кроком є безпосереднє оцінювання групою відібраних компетентних експертів показників національної економіки за визначеною на попередньому етапі множиною показників, які характеризують тим чи іншим чином показник здатності національної економіки держави забезпечувати необхідний рівень її оборонного потенціалу. Сформовані оцінки будуть потребувати визначення їх ступеня взаємозв'язку та ступеня відповідності вимогам, що висувуються на час оцінювання до ОП, а також аналізу їх чутливості до змін вхідних даних.

Третім кроком необхідно провести оцінювання існуючого стану національної економіки держави щодо здатності забезпечення необхідного рівня її ОП, а далі здійснити оцінювання відповідності цього показника вимогам до нього щодо ефективного розвитку оборонної сфери в цілому.

Методика передбачає формування єдиної інтегральної оцінки здатності національної економіки держави забезпечити її ОП на основі оцінок синтетично створених факторів, які визначені на основі аналізу та оцінювання набору змінних оцінок показників (факторів), які характеризують здатність національної економіки щодо забезпечення необхідного рівня ОП, та, у свою чергу, розраховані фахівцями за їх напрямками. Кількість характеристик ОП має бути значно меншою за кількість початкових змінних його складових, що реалізується за допомогою використання методу групування багатовимірних спостережень [12–17]. Основними характеристиками здатності національної економіки держави забезпечити її ОП, які підлягають оцінюванню, обрано: достатність, економічність, перспективність, надійність, стабільність (так звані синтетичні фактори, які в собі групують воєнні та економічні показники оцінювання стану національної економіки та ОП). Для того, щоб оцінити рівень ОП держави за показниками національної економіки, необхідно за цими показниками на основі опрацювання значного масиву інформації сформулювати оцінки їх достатності за кожним із них, а також за показниками більш нижчого рівня ієрархії. Найближчими за змістом до показників, які характеризують достатність можливостей національної економіки країні щодо забезпечення необхідного рівня її ОП, є показники, що характеризують воєнно-економічну обстановку в країні, їх частково можна назвати складовими воєнно-економічного потенціалу держави або характеристиками оборонного потенціалу в рамках ресурсного забезпечення необхідного рівня оборонного потенціалу в цілому.

Загальна структура методики оцінювання здатності національної економіки забезпечити достатній рівень оборонного потенціалу наведена на рис. 1. На рис. 2 наведені основні процедури першого етапу методики, до яких належать: визначення множини показників національної економіки держави, які характеризують її ОП та проведення попереднього оцінювання їх важливості один за одним методом експертного опитування на основі попарних порівнянь [15]. Формування бази вхідних статистичних даних щодо стану та динаміки кожного показника національної економіки мають проводити фахівці за відповідними напрямками залежно від галузі, яку характеризує кожен показник. Тобто набір необхідної статистичної інформації надає кожне міністерство (відомство), яке безпосередньо відповідає за такий напрям в державі. Далі формуються анкети опитування для відібраних для оцінювання експертів.

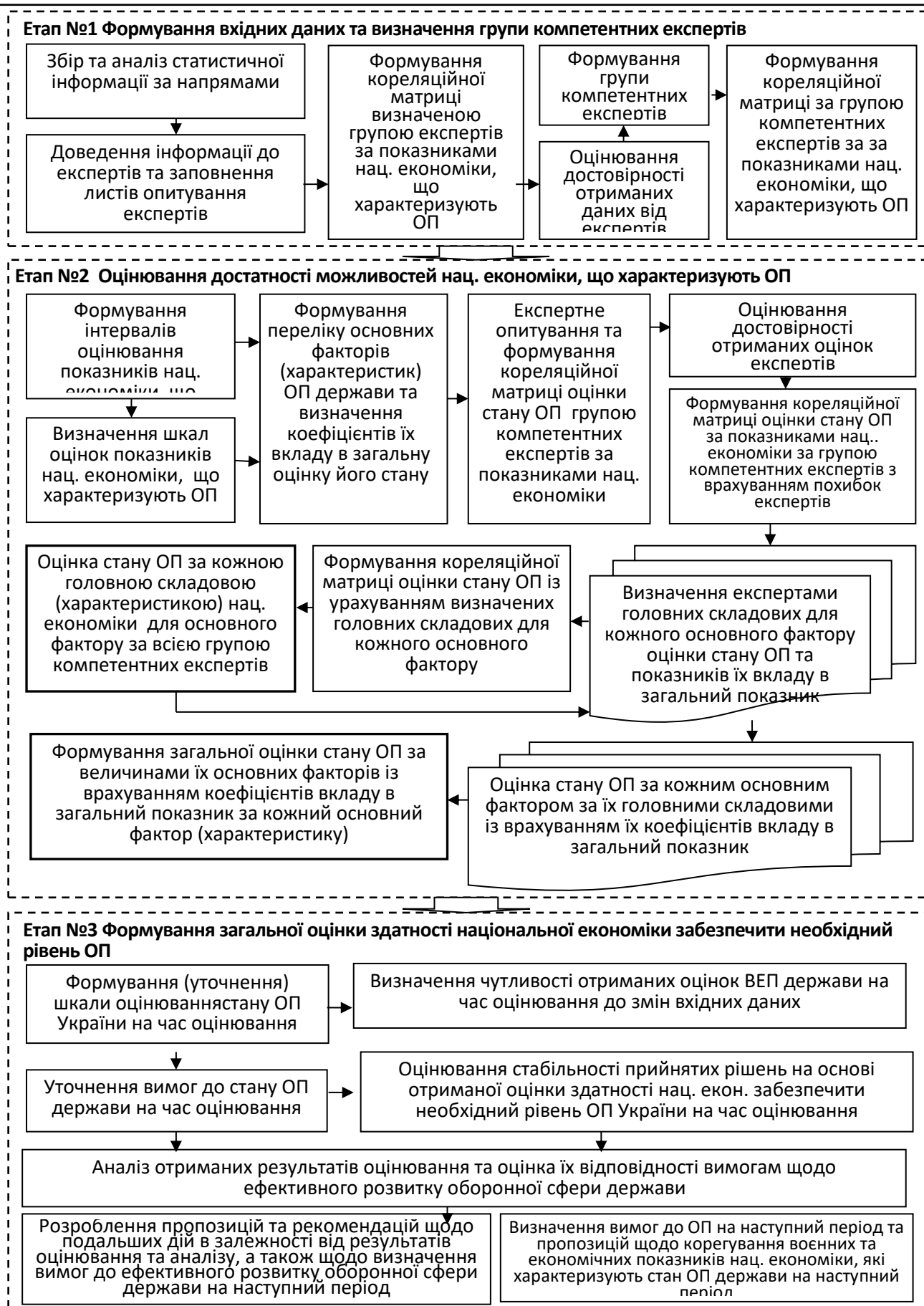


Рисунок 1 – Загальна структура методики оцінювання здатності національної економіки держави забезпечити її оборонний потенціал

Відповідно до анкет експерти заповнюють кореляційні матриці залежності за кожним із визначених двадцяти показників оцінювання методом попарного порівняння. Для проведення практичного дослідження за запропонованим методом було відібрано 7 експертів.

Кореляційна матриця кожного із експертів має такий вигляд:

$$|X_z| = \begin{vmatrix} x_1 & \dots & x_m \\ x_1 & 1 & a_{12} & a_{1m} \\ \dots & a_{21} & 1 & \dots \\ x_n & a_{2n} & a_{mn} & 1 \end{vmatrix}, \quad (1)$$

де $a_{mn} = f(x_1, x_2)$, $(0 \leq a_{mn} \leq 1)$ – коефіцієнт порівняльної (кореляційної) залежності (вплив) показників один на одного.

За всіма експертами групи (7 експертів) формується середньоарифметична кореляційна матриця:

$$|\bar{X}_z| = \begin{vmatrix} x_1 & \dots & x_m \\ x_1 & 1 & \bar{a}_{12} & \bar{a}_{1m} \\ \dots & \bar{a}_{21} & 1 & \dots \\ x_n & \bar{a}_{2n} & \bar{a}_{mn} & 1 \end{vmatrix}, \quad (2)$$

де $\bar{a}_{mn}$ – середньоарифметичне значення кореляційного коефіцієнта за Z експертами.

На основі аналізу даних експертного опитування оцінюють достовірність отриманих результатів шляхом використання підходу щодо аналізу оцінок експертів за середньоквадратичним відхиленням S_{mn} :

$$\bar{a}_{mn} = 1/Z \cdot \sum_{z=1}^Z a_{mn}^z; \quad S_{mn} = 1/Z-1 \cdot \sum_{z=1}^Z (a_{mn}^z - \bar{a}_{mn})^2, \quad (3)$$

Етап 1 Формування вихідних даних щодо оцінювання здатності національної економіки в рамках забезпечення необхідного рівня оборонного потенціалу та визначення групи R компетентних експертів

Визначення показників національної економіки, які характеризують достатність оборонного потенціалу держави

x_1 – стан фінансової системи держави; x_2 – стан природних ресурсів; x_3 – рівень економічних зв'язків; x_4 – стан рівень організованості та плановості розвитку економіки; x_5 – наявний бойовий потенціал держави; x_6 – реальний бойовий потенціал; x_7 – відносний рівень бойового потенціалу до бойового потенціалу ймовірного противника; x_8 – рівень виробництва продукції військового призначення; x_9 – можливі потужності виробництва; x_{10} – інфраструктурний потенціал держави; x_{11} – рівень морально-політичної підготовленості та дисциплінованості населення; x_{12} – рівень необхідних запасів та резервів матеріально-технічних засобів; x_{13} – рівень розвитку системи сполучень в країні; x_{14} – рівень забезпеченості транспортними засобами; x_{15} – рівень забезпеченості господарчими товарами військових потреб; x_{16} – можливі потужності господарства; x_{17} – рівень забезпеченості товарами сільськогосподарства військових потреб; x_{18} – можливі потужності сільськогосподарства держави; x_{19} – рівень розвитку організаційно-управлінської системи забезпечення військових потреб; x_{20} – рівень впровадження науково-технічного потенціалу в воєнному секторі економіки держави.

Формування кореляційної матриці кожним z-м експертом за визначеною множиною показників

$$|X_z| = \begin{vmatrix} x_1 & \dots & x_m \\ x_1 & 1 & a_{12} & a_{1m} \\ \dots & a_{21} & 1 & \dots \\ x_n & a_{2n} & a_{mn} & 1 \end{vmatrix}$$

$a_{mn} = f(x_1, x_2)$ ($0 \leq a_{mn} \leq 1$) – коефіцієнт порівняльної залежності (вплив) визначених показників один від одного (визначається експертами)

Оцінювання достовірності

отриманих результатів коефіцієнтів порівняльної залежності a_{mn} щодо сформованої матриці $|X|$

за $Z = \overline{1, Z}$ експертів:

$$\bar{a}_{mn} = 1/Z \cdot \sum_{z=1}^Z a_{mn}^z;$$

$$S_{mn} = 1/Z-1 \cdot \sum_{z=1}^Z (a_{mn}^z - \bar{a}_{mn})^2$$

$V_n = \frac{|\bar{a}_{mn} - a_{mn}|}{S}$, якщо $V_n > V_{зад}$, то результат оцінки даного експерта не враховується

НІ
ТАК
V_n > V_{зад} для

z-ий експерт не входить до групи компетентних експертів ($r = \overline{1, R}$) - його оцінка не враховується

z-ий експерт входить до групи компетентних експертів ($r = \overline{1, R}$)

Формування загальної кореляційної матриці за R експертів за визначеною базою показників

$$|X| = \begin{vmatrix} x_1 & \dots & x_m \\ x_1 & 1 & \bar{a}_{12} & \bar{a}_{1m} \\ \dots & \bar{a}_{21} & 1 & \dots \\ x_n & \bar{a}_{2n} & \bar{a}_{mn} & 1 \end{vmatrix}$$

$\bar{a}_{mn} = f(x_1, x_2)$ – середньоарифметичне за R експертів

Рисунок 2 – Перший етап методики оцінювання здатності національної економіки забезпечити її оборонний потенціал

Відбір групи компетентних експертів здійснюється за показником:

$$V_n = \frac{|\bar{a}_{mn} - a_{mn}|}{S_{mn}}, \quad (4)$$

якщо $V_n > V_{зад}$, то результат оцінки даного експерта вважається хибним.

Відповідно до отриманих оцінок формуються матриці оцінювання достовірності отриманих експертних даних. Таблиця результатів достовірності оцінок експертів (табл. 2.3) дає відповідь щодо рівня компетентності експерта під час проведення оцінювання за проблему, що розглядається.

Під компетентністю експерта будемо розуміти ступінь узгодженості його думки із середнім значенням думок усієї групи експертів. Кореляційні матриці, які містять кількість помилок понад вказаний поріг, не враховуються під час оцінювання та даний експерт не буде входити до групи компетентних експертів (r). Результати оцінювання показали, що 2-й та 4-й експерти мали найбільшу кількість помилок (неузгодженостей із думкою більшості групи), тому до групи компетентних експертів увійде лише п'ять експертів (табл. 2, рис. 3).

Таблиця 2 – Результати достовірності оцінок експертів

№ з/п	Експерт / показники	Кількість вірних оцінок	Кількість невірних оцінок	Допустима межа помилок ($V_{зад}$)	Ступінь компетентності експертів (ТАК чи НІ)
1	1-й експерт	264	136	201	ТАК
2	2-й експерт	158	242	201	НІ
3	3-й експерт	270	130	201	ТАК
4	4-й експерт	174	226	201	НІ
5	5-й експерт	254	146	201	ТАК
6	6-й експерт	248	152	201	ТАК
7	7-й експерт	242	158	201	ТАК
8	Загальна оцінка (компетентні)	1610	1190		5

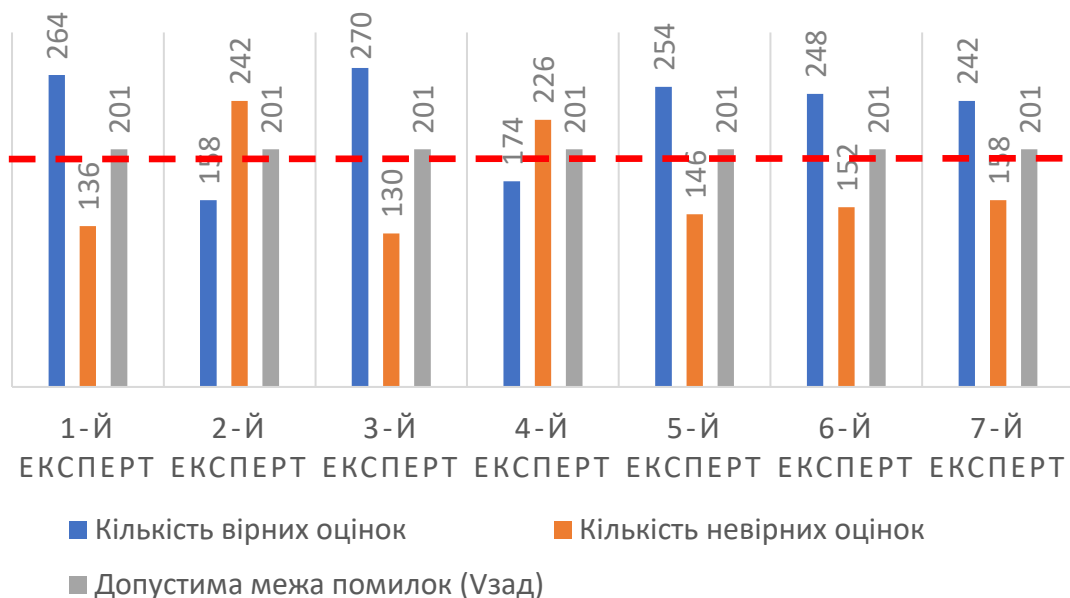


Рисунок 3 – Результати оцінювання достовірності оцінок експертів

На рис. 4 наведено основні процедури другого етапу методики, а саме: оцінювання стану ОП через оцінки змінних показників національної економіки станом на час оцінювання. Цей крок передбачає найбільшу кількість математичних операцій.

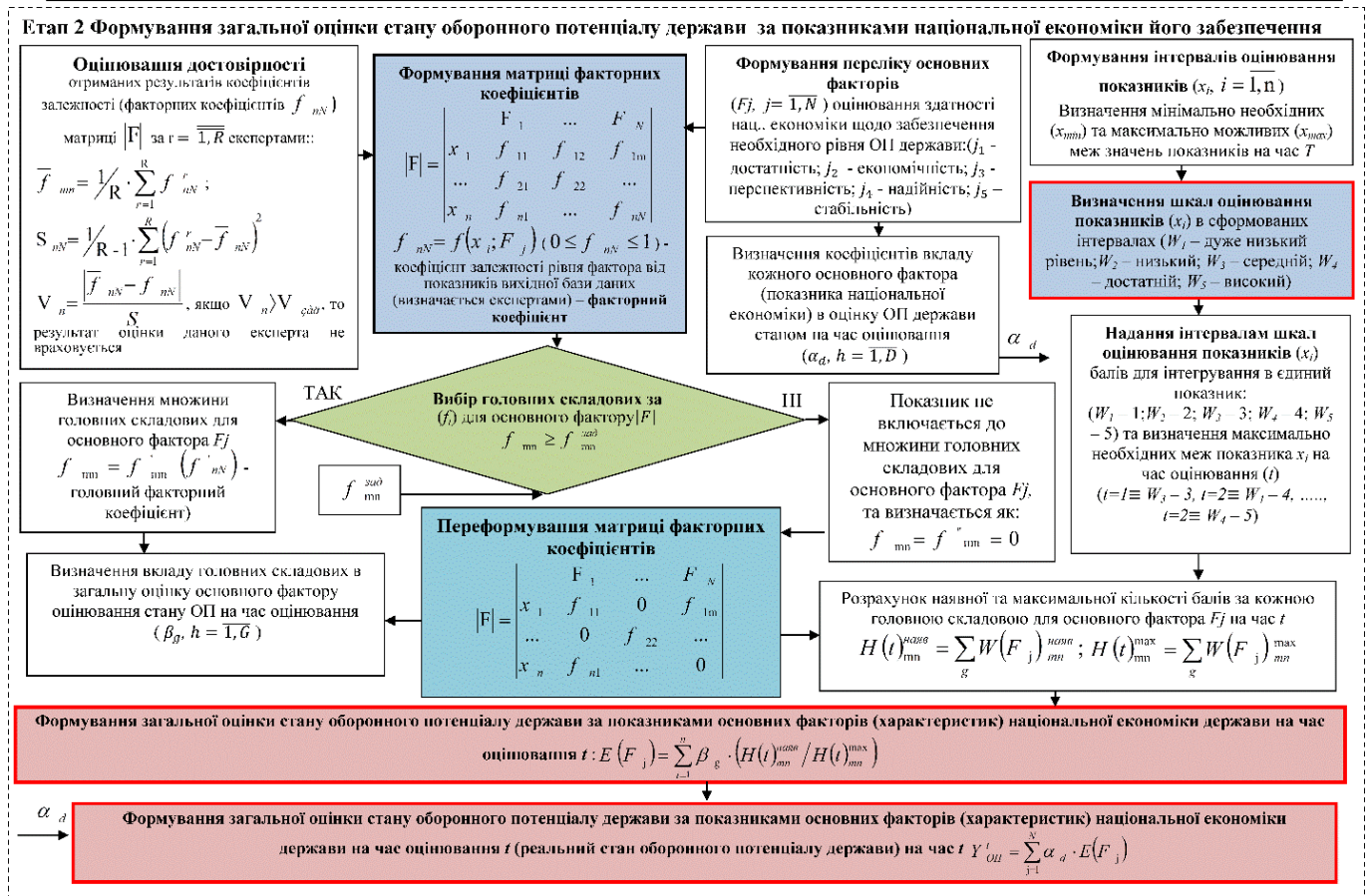


Рисунок 4 – Другий етап методики оцінювання здатності національної економіки держави забезпечити її оборонний потенціал

По-перше, визначена група компетентних експертів формує інтервали оцінювання для кожного із визначених двадцяти показників національної економіки, які характеризують стан ОП (визначаються мінімально необхідні ($x_{\min}$) та максимально можливі ($x_{\max}$) межі значень показників на час (t) T . Далі визначаються шкали оцінювання кожного з показників ($x_i, i = \overline{1, n}$) у сформованих інтервалах значень від мінімуму до максимуму (W_1 – дуже низький рівень; W_2 – низький; W_3 – середній; W_4 – достатній; W_5 – високий) та надаються інтервалам шкал оцінювання показників (x_i) бали оцінки для інтегрування даних оцінок у єдиний показник. Наприклад, візьмемо таку відповідність балів та інтервалів ($W_1 - 1; W_2 - 2; W_3 - 3; W_4 - 4; W_5 - 5$). Під час переходу до бальної шкали оцінювання можна для підвищення реальності оцінки здійснити ранжування показників або просто визначити максимально можливий результат на час оцінювання. Наприклад, для показника $x_5 \rightarrow W_3 = W_{\max} = 3, x_{16} \rightarrow W_4 = W_{\max} = 4$ тощо. У загальному вигляді цей етап розрахунків є етапом оцінювання стану національної економіки держави за складовими оборонного потенціалу держави на t -й час оцінювання. Група компетентних експертів залучається для визначення основних факторів (характеристик) оцінювання стану ОП за визначеною множиною показників (F_j, j) національної економіки, які характеризують стан ОП держави. До таких факторів (характеристик) згідно з запропонованим підходом оцінювання експерти визначили: j_1 – достатність показників національної економіки для необхідного стану ОП; j_2 – економічність використання ресурсів для досягнення необхідного стану ОП; j_3 – перспективність планів щодо досягнення необхідного ОП; j_4 – надійність прийнятих рішень щодо забезпечення необхідного ОП; j_5 – стабільність ситуації щодо розвитку національної економіки держави та стану ОП залежно від ситуації що складається навколо країни та всередині неї. Для кожного із визначених факторів

(характеристик) експерти визначають коефіцієнти вкладу кожного основного фактора в оцінювання реального стану ОП та оцінювання здатності національної економіки забезпечити необхідний рівень ОП ($\alpha_d, h=\overline{1, D}$). Після таких математичних процедур експерти здійснюють вибірку автокореляції, тобто будують кореляційні матриці факторних навантажень групою R компетентних експертів (залежності основного фактора (характеристики) стану ОП від стану кожного показника стану національної економіки):

$$|F_R| = \begin{vmatrix} F_1 & \dots & F_N \\ x_1 & f_{11} & f_{12} & f_{1m} \\ \dots & f_{21} & f_{22} & \dots \\ x_n & f_{n1} & \dots & f_{nN} \end{vmatrix}, \quad (6)$$

де f_{mn} – кореляційний коефіцієнт факторного навантаження за j -м основним фактором (характеристикою) відносно i -го показника національної економіки.

Далі за всіма експертами групи компетентних експертів (5 експертів) формується середньоарифметична кореляційна матриця

$$|\overline{F}_R| = \begin{vmatrix} \overline{F}_1 & \dots & \overline{F}_N \\ x_1 & \overline{f}_{11} & \overline{f}_{12} & \overline{f}_{1m} \\ \dots & \overline{f}_{21} & \overline{f}_{22} & \dots \\ x_n & \overline{f}_{n1} & \dots & \overline{f}_{nN} \end{vmatrix}, \quad (7)$$

де $\overline{f}_{nN}$ – середньоарифметичне значення факторного навантаження.

З формальної точки зору запропонована процедура оцінювання взаємозв'язків основних факторів та показників національної економіки, які характеризують стан ОП, являє собою застосування процедур факторного аналізу, яка має забезпечити виявлення сили та напрямку різних внутрішніх зв'язків між змінними (показниками національної економіки та ОП) та визначеними основними факторами – синтетичними показниками, що характеризують стан ОП через достатність можливостей національної економіки України. Опис цих взаємозв'язків і являє собою значення факторних навантажень, які будуть описуватися в інтервалі від 0 до 1. Може використовуватися й інша шкала, яка включатиме від'ємні значення. Для нашого випадку щодо опису визначених показників та факторів практично немає навіть нульових залежностей між змінними і факторами, тому обрана шкала від 0 до 1. У процесі оцінювання рівня ОП треба створити так звану воєнно-економічну модель розуміння залежностей між ОП та показниками національної економіки держави. Тобто в процесі інтерпретації визначених основних синтетичних факторів під час такого воєнно-економічного оцінювання здійснюється смислове агрегування змінних (показників стану (достатності) національної економіки), частка яких найбільш суттєва під час формування оцінок ОП за оцінками основних факторів, що його характеризують.

За допомогою розрахованих показників матриці (7) оцінюють достовірності оцінок за кожним R-м експертом шляхом застосування середньоквадратичних відхилень:

$$\overline{f}_{mn} = 1/R \cdot \sum_{r=1}^R f_{r,nN}, \quad S_{nN} = 1/R-1 \cdot \sum_{r=1}^R (f_{r,nN} - \overline{f}_{nN})^2. \quad (8)$$

Потім формуються матриці оцінювання достовірності оцінок експертів, якщо

$$V_n \geq V_{зад}, \quad \text{де } V_n = \frac{|\overline{f}_{nN} - f_{nN}|}{S}, \quad (9)$$

тоді результат оцінки даного експерта не враховується в оціночних матрицях, замість оцінки даного експерта виставляється значення "0".

Наступним кроком практичного застосування методу є вибір головних компонент (показників національної економіки, які безпосередньо характеризують стан ОП) для кожного

із факторів, що описують стан ОП держави. Вибір головних компонент здійснюється на основі оцінок середньоарифметичної кореляційної матриці. Результати вибору являють собою порівняння отриманого середньоарифметичного значення показників матриці f_i (факторних коефіцієнтів) за кожним із основних факторів F .

Якщо $f_{mn} \geq f_{mn}^{\text{зад}}$, тоді ця складова ОП включається до множини головних складових для основного фактора F_j , тобто $f_{mn} = f'_{mn}$ та f'_{nN} – головний факторний коефіцієнт, який буде враховуватися під час формування загальної оцінки ОП за даним j -м основним фактором – показником національної економіки. Навпаки, результати оцінювання за такою складовою ОП не враховуються в загальну оцінку і місце в матриці заповнюється значенням “0”. Слід зауважити, що значення заданого факторного коефіцієнта $f_{mn}^{\text{зад}}$, відносно якого здійснюється порівняння, може задаватися як одразу для всієї матриці, так і окремо для кожного основного фактора. Найпрактичнішим є задавання його за кожним основним фактором (показником) окремо, бо тоді враховуються усі особливості взаємозв’язків самого фактора із змінними складовими.

Аналіз такої матриці показує, що за першим основним фактором F_1 визначено 9 головних складових, за другим F_2 – 5, F_3 – 8, F_4 – 6, F_5 – 9. Наступним кроком даного етапу є визначення вкладу головних складових (показників національної економіки) у загальну оцінку основного фактора оцінювання стану ОП (β_g , $h = \overline{1, G}$). Далі експерти на основі аналізу попередньої статистичної інформації щодо показників за напрямками складових ОП, яка надається відповідальними за напрям відомствами, оцінюють стан ОП за показниками стану національної економіки на час оцінювання за бальною шкалою. Отже, відбувається формування оціночних матриць за R експертів без урахування їх недостовірних результатів за відповідними складовими, які були визначені під час оцінювання достовірності оцінок групи обраних компетентних експертів:

$$|F_r^W| = \begin{vmatrix} R_1 & \dots & R_N \\ x_1 & W_3 & \dots & W_4 \\ \dots & W_5 & W_2 & \dots \\ x_n & W_3 & \dots & W_1 \end{vmatrix}. \quad (10)$$

Оціночні матриці являють собою остаточну матрицю оцінювання стану ОП за показниками оцінок стану національної економіки України за думкою кожного із компетентних експертів. Отримані результати оцінювання у вигляді такої оціночної матриці, яка дає змогу оцінити стан ОП за існуючими оцінками стану можливостей національної економіки, яка сформована експертами як похідна від воєнно-політичної та соціально-економічної обстановки всередині країни станом на наступний період. Зведення показників оціночної матриці у загальні оцінки:

$$H(t)_{mn}^{\text{наяв}} = \sum_r W(F_j)_{mn}^{\text{наяв}} / R; H(t)_{mn}^{\text{max}} = \sum_r W(F_j)_{mn}^{\text{max}} / R. \quad (11)$$

Вже під час аналізу інформації щодо вимог до стану ОП треба переходити до оцінювання достатності можливостей національної економіки забезпечити необхідний рівень ОП держави з урахуванням існуючих загроз та викликів.

Далі необхідно сформулювати загальну оцінку за кожний основний фактор F_j – синтетичний показник (характеристика ОП держави) на час t

$$E(F_j) = \sum_{i=1}^n \beta_g \cdot (H(t)_{mn}^{\text{наяв}} / H(t)_{mn}^{\text{max}}). \quad (12)$$

На рис. 5 та рис. 6 наведено приклад кінцевих результатів оцінювання стану ОП держави за оцінками стану показників національної економіки у період 2020-2021 років. Отримані кінцеві результати розрахунків дають можливість за розрахованими показниками перейти до оцінювання здатності (достатності можливостей) національної економіки щодо забезпечення необхідного рівня ОП у разі наявності вимог до його величини. Вимоги до його

величини повинні визначатися на основі оцінок стану загроз національній безпеці України або, наприклад, на основі оцінок стану воєнно-економічної безпеки тощо.

Результати оцінювання, наведені на рис. 5, ілюструють стан множини показників національної економіки, які відібрані для характеристики ОП держави, а на рис. 6 наведені результати оцінювання здатності національної економіки України забезпечити її ОП за основними синтетичними (штучно створеними) показниками (факторами), які характеризують здатність національної економіки забезпечувати необхідний стан ОП, тобто зроблено перехід від більшого масиву оцінок до менших обсягів, з метою підвищення достовірності оцінок та зменшення їх чутливості до змін вхідних даних.

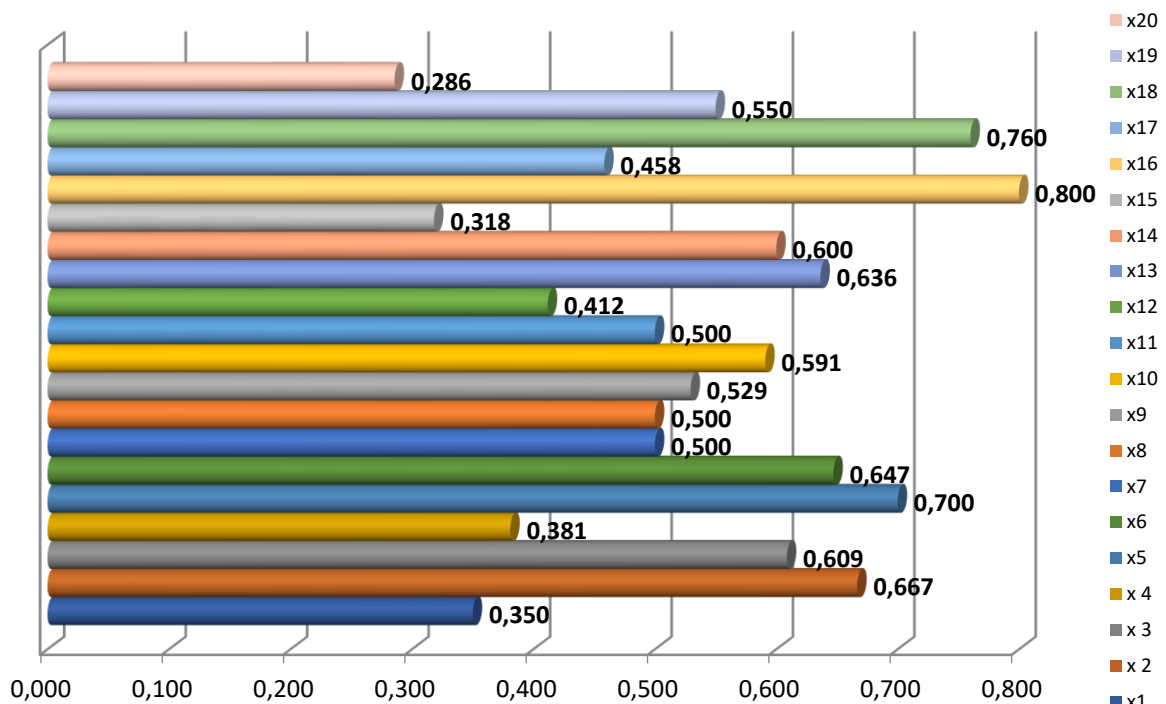


Рисунок 5 – Оцінки здатності національної економіки держави забезпечити її ОП за відповідними показниками національної економіки, що характеризують стан ОП держави

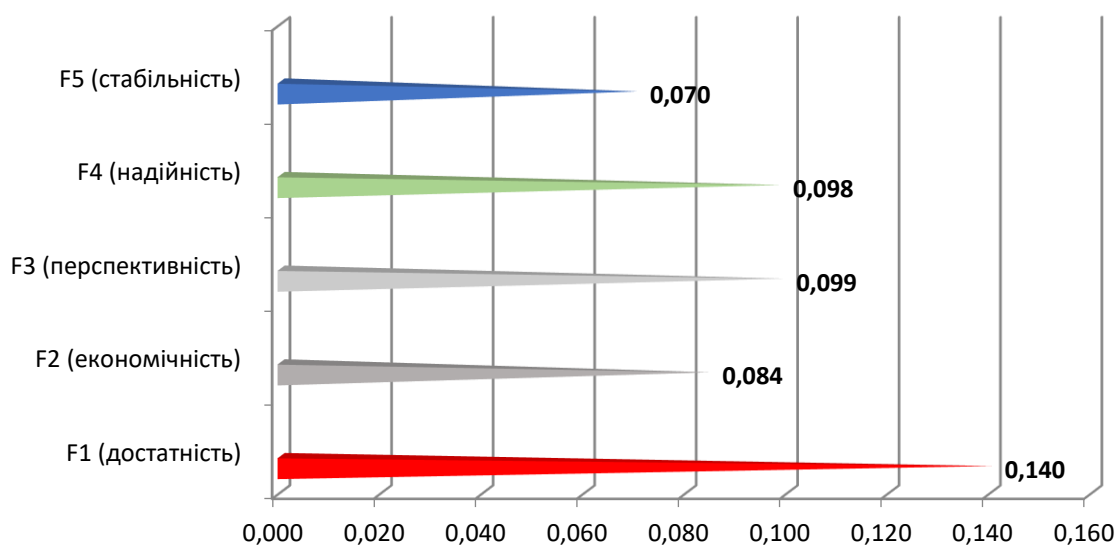


Рисунок 6 – Оцінки здатності національної економіки України забезпечити її оборонний потенціал за основними складовими (синтетичними показниками, факторами), що визначені на основі оцінок стану національної економіки України та взаємозв'язку з показниками ОП

Останньою процедурою цього етапу є формування загальної оцінки здатності національної економіки забезпечувати необхідний рівень оборонного потенціалу, в принципі це є характеристика стану ОП на основі оцінок стану показників національної економіки на час оцінювання (t):

$$Y_{BEY}^t = \sum_{j=1}^N \alpha_d \cdot E(F_j). \quad (13)$$

Для того щоб оцінити відповідність оцінювання стану ОП існуючим вимогам до нього, необхідно перейти до третього етапу методики (рис. 7), який передбачає оцінювання стану ОП відповідно до вимог, що висувуються на час оцінювання до нього, з подальшим переходом до оцінювання вже достатності можливостей національної економіки щодо забезпечення необхідного (потрібного) рівня ОП.

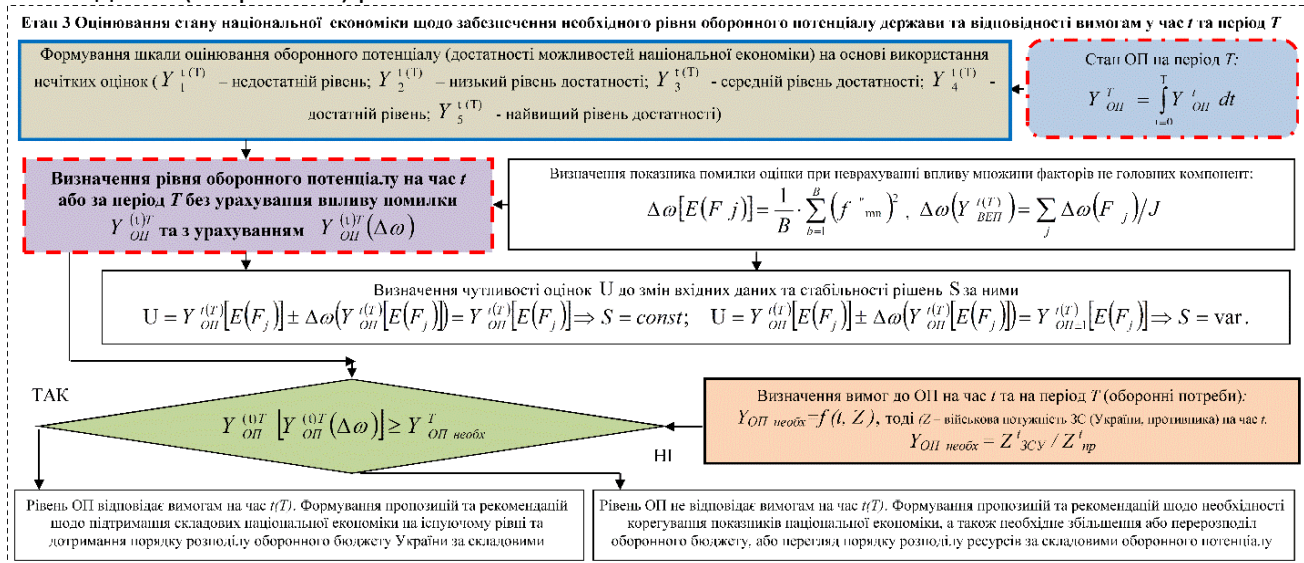


Рисунок 7 – Третій етап методики оцінювання здатності національної економіки держави забезпечити її оборонний потенціал

Отже, третій етап є етапом підготовки інформації для прийняття рішень щодо подальшого розвитку оборонної сфери держави, формування реальних вимог до рівня ОП країни, визначення раціональних шляхів пошуку додаткових можливостей національної економіки України для забезпечення необхідного рівня її ОП. Це етап оцінювання стану національної економіки держави щодо забезпечення рівня необхідного рівня оборонного потенціалу на t -й час. У табл. 3 наведено приклад кінцевих результатів оцінювання за другим етапом методики, а також вже наведена якісна оцінка існуючого стану ОП держави за попередньо розрахованими даними до відповідно сформованих шкал оцінювання, які є елементом третього етапу. Для цього необхідно на третьому етапі здійснити проаналізувати отримані результати відповідно до чутливості їх до змін або неточностей вихідних даних та дослідити ступінь стабільності рішень, які будуть прийматися на основі цих оцінок. Кінцевим результатом третього етапу методики оцінювання здатності національної економіки держави забезпечити її ОП мають стати пропозиції та рекомендації, щодо:

по-перше, щодо можливих способів підвищення оборонного потенціалу держави шляхом коригування розподілу державного бюджету за основними показниками національної економіки, які визначають його стан;

по-друге, щодо формування вимог до рівня оборонного потенціалу на наступний плановий період, у тому числі шляхом оптимізації (зниження) надмірних вимог до нього;

по-третє, щодо визначення наступних термінів проведення оцінювання здатності національної економіки забезпечувати необхідний рівень оборонного потенціалу країни;

Таблиця 4 – Оціночна матриця стану головних складових оцінювання здатності національної економіки забезпечити її ОП (ВЕП)

№	Показники ВЕП / Головні фактори	F_1 (достатність)	F_2 (економічність)	F_3 (перспективність)	F_4 (надійність)	F_5 (стабільність)
1	Результати оцінювання здатності національної економіки держави забезпечити її ОП України (стан ОП)	0,140	0,084	0,099	0,098	0,070
2	Загальна оцінка здатності національної економіки забезпечити її ОП (стан ОП України на час t ($Y_{OP}(t)$))	0,492				
3	Якісна оцінка стану ОП України за шкалою оцінювання (низька здатність національної економіки забезпечити необхідний рівень ОП держави на час оцінювання)	Низький рівень здатності національної економіки України забезпечити її ОП (низький рівень ОП)				

по-четверте, щодо заходів з поліпшення стану основних складових національної економіки, які мають вирішальний вплив на оборонний потенціал держави, або ж визначення компромісів у взаємозалежності цих показників.

Першим кроком третього етапу є розроблення або уточнення шкал оцінювання здатності національної економіки щодо забезпечення необхідного рівня ОП. Ця шкала може визначатися завчасно та бути вихідними даними, а може визначатися (уточнюватися) експертами визначеної компетентної групи.

Інтервали цієї шкали мають бути функціонально залежними від багатьох як зовнішніх, так і внутрішніх факторів, що будуть впливати на розмір інтервалів.

Для формування можливостей щодо визначення чутливості отриманих оцінок до змін вхідних даних та стабільності прийнятих на їх основі рішень пропонується інтервали цієї шкали формувати за допомогою логічних висновків використанням нечітко-множинної математичної моделі, де в основі оцінок лежать нечіткі числа з відповідними функціями належності.

Наприклад, $Y_1^{(T)}$ – недостатній рівень ОП або здатності національної економіки забезпечити його необхідний рівень; $Y_2^{(T)}$ – низький рівень здатності національної економіки держави забезпечити її оборонний потенціал (тобто стан ОП); $Y_3^{(T)}$ – середній рівень здатності національної економіки держави (стан ОП); $Y_4^{(T)}$ – достатній здатності національної економіки держави; $Y_5^{(T)}$ – найвищий здатності національної економіки держави (стану ОП) (рис. 12).

Шкала оцінювання стану ОП розбивається на п'ять нечітких підмножин $Y, y = \overline{1,5}$, кожна з яких задається своєю функцією належності $\mu_y(X_\Sigma)$, $y = \overline{1,5}$, $X_\Sigma \in [0,1]$. Для оцінки формується шкала, в якій також кожен з показників займає відповідну частину (підмножину) від загального показника (рис. 13). Задані проміжки, на які розбивається шкала кожного із показників, що оцінюються аналогічним способом нечітко-множинної логіки, визначено нечіткими числами (рис. 13), які можуть формуватися на основі узагальненої функції Харінгтона [13–18] або експертного опитування як з урахуванням компетентності експертів, так і без.

У методиці для задавання відповідних функцій належності для показника стану ОП або здатності національної економіки щодо забезпечення його необхідного рівня пропонується використовувати процедуру проведення експертного опитування групи компетентних експертів. Приклад такої шкали для одного з показників наведено в табл. 5. Відповідна шкала

може формуватися за окремими оцінками, а також може бути використана і для загальної оцінки з метою переходу від кількісної оцінки до якісної оцінки отриманих результатів оцінювання.

Таблиця 5 – Експертні оцінки діапазонів нечітких шкал оцінювання стану ОП на час t (приклад)

Якісні характеристики / Границі функцій приналежності	Границі трапецієдальних функцій приналежності			
	a	b	c	d
недостатній рівень ОП	0	0,08	0,11	0,23
низький рівень достатності ОП	0,19	0,29	0,42	0,54
середній достатності рівень ОП	0,45	0,58	0,64	0,69
достатній рівень ОП	0,63	0,72	0,82	0,89
найвищий (бажаний) рівень ОП	0,84	0,95	1	1

Також на цьому етапі необхідно провести такі процедури: уточнення вимог до необхідного рівня ОП країни на час оцінювання; уточнення вимог до ОП на час t та на період T (оборонні потреби) щодо рівня ОП $Y_{\text{ОПнеобх}} = f(t, Z)$ (Z – військова потужність ЗС (України, противника) на час t ; оцінювання $Y_{\text{ОПнеобх}} = Z \cdot t^{\text{ЗСУ}} / Z \cdot t^{\text{пр}}$ відповідно до вимог на час t ; оцінювання здатності національної економіки щодо забезпечення необхідного рівня ОП на час t або за період T без урахування впливу помилки $Y_{\text{ОП}}^{(t)T}$ та з урахуванням $Y_{\text{ОП}}^{(t)T}(\Delta\omega)$.

Проведення розрахунків щодо практичної оцінки рівня ОП України станом на період 2020-2021 років показали такі результати: $Y_{\text{ОП}} = 0,492$ – це відповідає якісному оцінюванню щодо середнього рівня здатності національної економіки забезпечити необхідний рівень ОП. Але об'єктивним є те, що оцінка наближена до нижньої межі інтервалу середнього рівня достатності, а це означає, що отриманий результат має пройти перевірку на чутливість його до змін вхідних даних. На основі цієї оцінки слід зробити висновки щодо стабільності прийнятих рішень на основі даного результату оцінювання. Тобто отримані результати стану ОП та здатності національної економіки забезпечити необхідний рівень на рівні 0,492 спричиняє неоднозначність оцінювання за різних вхідних даних.

Показник відхилень оцінювання стану ОП або здатності національної економіки забезпечити його достатній рівень у разі неврахування впливу множини факторів неголовних компонент може розраховуватися так:

$$\Delta\omega[E(Fj)] = \frac{1}{B} \cdot \sum_{b=1}^B (f''_{mn})^2, \quad \Delta\omega(Y_{\text{ОП}}^{(t)T}) = \sum_j \Delta\omega(F_j) / J. \quad (14)$$

Аналіз формули (14) показує, що відхилення в методиці пропонується розраховувати як середнє значення за основними факторами від середньоквадратичної помилки (відхилення) за коефіцієнтами кожного з основних факторів, які не увійшли до головних складових основного фактора, що розглядається.

Оцінка чутливості U отриманих результатів до змін вхідних даних та стабільності рішень S за ними визначається так:

$$\begin{cases} U = Y_{БЕП}^{t(T)}[E(F_j)] \pm \Delta\omega(Y_{БЕП}^{t(T)}[E(F_j)]) = Y_{БЕП}^{t(T)}[E(F_j)] \Rightarrow S = const; \\ U = Y_{БЕП}^{t(T)}[E(F_j)] \pm \Delta\omega(Y_{БЕП}^{t(T)}[E(F_j)]) = Y_{БЕП\pm 1}^{t(T)}[E(F_j)] \Rightarrow S = var. \end{cases} \quad (15)$$

Відповідно до формули (14), якщо врахування визначеного за формулою (15) відхилення у бік додавання або віднімання змінює рівень достатності стану ОП, або здатності національної економіки щодо його забезпечення на необхідному рівні, то отримана оцінка вважається чутливою до змін вхідних параметрів, та рішення, прийняті за ними, є нестабільними і будуть підлягати більш ретельному аналізу та обґрунтуванню. Якщо рівень не змінюється, тоді оцінка вважається стабільною і рішення на основі даної оцінки також є стабільними.

Якщо оцінювання стану ОП або здатності національної економіки щодо забезпечення його необхідного рівня здійснюється за період T , тоді отримані результати оцінок за інтервали цього періоду інтегруються в загальний показник

$$Y_{ОП}^T = \int_{t=0}^T Y_{ОП}^t dt. \quad (2.21)$$

Останньою процедурою цього етапу методики є порівняння отриманої оцінки із вимогами до стану ОП $Y_{ОП}^{(t)T} [Y_{ОП}^{(t)T}(\Delta\omega)] \geq Y_{ОП}^T_{необх}$, які були визначені на час або період оцінювання. Визначення вимог до ОП на час або період оцінювання є своєрідними вимогами до держави щодо розмірів забезпечення оборонних потреб для ефективного розвитку сектору оборони. Тобто ці вимоги є багатофункціональною залежністю від значення багатьох параметрів як економіки держави, так і стану розвитку сектору оборони.

Останнім кроком методики є прогнозування оцінок динаміки показників національної економіки держави щодо розрахунку динаміки її оборонного потенціалу та відповідності вимогам до нього, які визначаються на основі існуючих та прогнозованих загроз національній безпеці.

Висновки

У статті запропонована методика оцінювання здатності національної економіки забезпечити її оборонний потенціал ґрунтується на системному підході та поєднанні інструментів структурно-логічного аналізу й алгоритмічного моделювання. Вона дозволяє: ідентифікувати ключові елементи економічної системи, що безпосередньо впливають на оборонний потенціал держави; визначати взаємозв'язки між економічними, воєнними та соціальними чинниками у формуванні ресурсної бази для національної оборони; здійснювати багаторівневе оцінювання – від окремих показників до інтегрального індексу здатності економіки підтримувати оборону; забезпечувати можливість прогнозування наслідків перерозподілу ресурсів і розроблення варіантів управлінських рішень у сфері оборонно-економічної політики.

Методика у вигляді структурно-логічної схеми та алгоритму робить процес оцінювання прозорим і відтворюваним, що сприяє підвищенню обґрунтованості державних рішень у сфері оборонного планування. Її практичне застосування створює передумови для підвищення стійкості національної економіки, оптимізації використання ресурсів і забезпечення воєнної безпеки держави в умовах сучасних загроз.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Горбулін, В. П., Качинський, А. Б. Стратегічне планування: вирішення проблем національної безпеки. Київ: НІСД, 2010. 288 с.
2. Абрамов, А. П. Воєнно-економічні дослідження: методологія та практика. Київ: НАОУ, 2015. 312 с.
3. Семененко, О. М. Методологічні засади оцінювання воєнно-економічного потенціалу держави. Київ: ІС НАН України, 2018. 256 с.
4. Про Стратегію розвитку системи воєнної безпеки України: Рішення РНБО України № 121/2021 від 25.03.2021 [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/121/2021> (дата звернення: 08.08.2025).
5. Про Стратегію розвитку оборонно-промислового комплексу України: Указ Президента України № 372/2021 від 20.08.2021 [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/372/2021> (дата звернення: 08.08.2025).
6. Про схвалення Концепції Державної цільової програми реформування та розвитку оборонно-промислового комплексу до 2020 року: Розпорядження Кабінету Міністрів України від 20.01.2016 № 19-р [Електронний ресурс]. Режим доступу: <https://www.kmu.gov.ua/npas/248779815> (дата звернення: 08.08.2025).
7. Воробйов, Г. П. Воєнна економіка: навч. посіб. Москва: ВА Генерального штабу, 1985. 340 с.
8. Бажал, Ю. М. Економічний розвиток і економічна теорія: дослідження трансформаційних процесів. Київ: Основи, 2001. 272 с.
9. Семиноженко, В. П. Інноваційна стратегія України: наука, освіта, виробництво. Київ: Либідь, 2003. 320 с.
10. Nye, J. S. Soft Power: The Means to Success in World Politics. New York: PublicAffairs, 2004. 208 p.
11. Skliar, N. M. The Concept of the State Complex Power in Assessing the Military-Economic Component of the Security and Defence Sector. Економіка і суспільство, 2021, № 27. DOI: <https://doi.org/10.32782/2524-0072/2021-27-19>
12. Методичні рекомендації з фінансово-економічного обґрунтування вартості повного життєвого циклу спроможностей з урахуванням принципів та стандартів НАТО: затв. Міністром оборони України 02.06.2020 [Електронний ресурс]. Режим доступу: https://www.mil.gov.ua/content/oboron_plans/metod_recom_z_fin_ekon_life_ciklu_nato (дата звернення: 08.08.2025).
13. Потенціали співробітництва України з ЄС у сфері безпеки. Центр досліджень армії, конверсії та роззброєння для Фонду Конрада Аденауера [Електронний ресурс]. Режим доступу: https://www.kas.de/c/document_library/get_file?uuid=3c38095e-4b0b-26e6 (дата звернення: 08.08.2025).
14. Леоненков, А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH: функция принадлежности и методы ее построения. Санкт-Петербург: БХВ-Петербург, 2005. 736 с.
15. Шахов, А. Н. Политический потенциал оборонной мощи государства. Москва: ГАС, 1992. 148 с.
16. Смолянук, В. Ф. Військова могутність України: теоретико-методологічні засади формування та розвитку (політологічний аналіз досвіду 1990-х років): монографія. Київ; Ірпінь: ВТФ «Перун», 2000. 448 с.
17. Семененко, О. М., Водчиць, О. Г., Добровольський, Ю. Б., Бойко, Р. В., Кремешний, О. І. Метод оцінювання воєнно-економічних умов розвитку Збройних Сил України. Наука і техніка Повітряних Сил Збройних Сил України, 2015, № 2 (19), с. 16–23.

18. Семененко, О. М., Водчиць, О. Г., Бойко, Р. В., Іванов, В. Л. Щодо оцінювання ефективності виконання основних бюджетних програм Міністерства оборони України на період 2006–2014 рр. Збірник наукових праць ХНУПС, 2016, № 1 (46), с. 41–45.
19. Жуков, Г. П., Викулов, С. Ф. Военно-экономический анализ и исследование операций. Ч. 3: Количественные методы обоснования военно-экономических решений: уч. пособ. Москва: Кафедра экономики Вооружённых Сил МФИ, 1981. 252 с.
20. Экономико-математические методы и модели планирования и управления. Кн. 4 / під заг. ред. проф. В. Г. Шорина. Москва: Знание, 1973. 240 с.

References

1. Ghorbulin, V. P., & Kachynskiy, A. B. (2010). *Stratehichne planuvannia: vyrishennia problem natsionalnoi bezpeky* [Strategic planning: Solving national security problems]. NISD. 288 p.
2. Abramov, A. P. (2015). *Voienno-ekonomichni doslidzhennia: metodolohiia ta praktyka* [Military-economic studies: Methodology and practice]. NAOU. 312 p.
3. Semenenko, O. M. (2018). *Metodolohichni zasady otsiniuvannia voienno-ekonomichnoho potentsialu derzhavy* [Methodological foundations for assessing a state's military-economic potential]. Institute for Systems Research of the NAS of Ukraine. 256 p.
4. National Security and Defense Council of Ukraine. (2021, March 25). *Pro Stratehiiu rozvytku systemy voiennoi bezpeky Ukrainy* [On the Strategy for the Development of Ukraine's Military Security System] (Decision No. 121/2021). <https://zakon.rada.gov.ua/laws/show/121/2021>
5. President of Ukraine. (2021, August 20). *Pro Stratehiiu rozvytku oboronno-promyslovoho kompleksu Ukrainy* [On the Strategy for the Development of Ukraine's Defense-Industrial Complex] (Decree No. 372/2021). <https://zakon.rada.gov.ua/laws/show/372/2021>
6. Cabinet of Ministers of Ukraine. (2016, January 20). *Pro skhvalennia Kontseptsii Derzhavnoi tsilovoi prohramy reformuvannia ta rozvytku oboronno-promyslovoho kompleksu do 2020 roku* [On approval of the Concept of the State Target Program for reforming and developing the defense-industrial complex until 2020] (Order No. 19-r). <https://www.kmu.gov.ua/npas/248779815>
7. Vorobyov, G. P. (1985). *Voennaia ekonomika* [Military economics] (Textbook). Military Academy of the General Staff. 340 p.
8. Bazhal, Yu. M. (2001). *Ekonomichni rozvytok i ekonomichna teoriia: doslidzhennia transformatsiinykh protsesiv* [Economic development and economic theory: Studies of transformational processes]. Osnovy. 272 p.
9. Semynozhenko, V. P. (2003). *Innovatsiina stratehiia Ukrainy: nauka, osvita, vyrobnytstvo* [Innovation strategy of Ukraine: Science, education, production]. Lybid. 320 p.
10. Nye, J. S. (2004). *Soft power: The means to success in world politics*. PublicAffairs. 208 p.
11. Skliar, N. M. (2021). The concept of the state complex power in assessing the military-economic component of the security and defence sector. *Economy and Society*, (27). <https://doi.org/10.32782/2524-0072/2021-27-19>
12. Ministry of Defence of Ukraine. (2020, June 2). *Metodychni rekomendatsii z finansovo-ekonomichnoho obgruntuvannia vartosti povnoho zhyttievoho tsykladu spromozhnosti z urakhuvanniam pryntsyviv ta standartiv NATO* [Guidelines on life-cycle costing of capabilities in line with NATO principles and standards]. https://www.mil.gov.ua/content/oboron_plans/metod_recom_z_fin_ekon_life_ciklu_nato
13. Centre for Army, Conversion and Disarmament Studies. (n.d.). *Potentsialy spivrobitnytstva Ukrainy z YeS u sferi bezpeky* [Potential for Ukraine–EU cooperation in the field of security]. Konrad Adenauer Foundation. https://www.kas.de/c/document_library/get_file?uuid=3c38095e-4b0b-26e6

14. Leonenkov, A. V. (2005). **Nechetkoe modelirovanie v srede MATLAB i fuzzyTECH: Funktsiia prinadlezhnosti i metody ee postroeniia** [Fuzzy modeling in MATLAB and fuzzyTECH]. BHV-Petersburg. 736 p.
15. Shakhov, A. N. (1992). **Politicheskii potentsial oboronnoi moshchi gosudarstva** [The political potential of a state's defense power]. GAS. 148 p.
16. Smolianiuk, V. F. (2000). **Viiskova mohutnist Ukrainy: teoretyko-metodolohichni zasady formuvannia ta rozvytku (politolohichniy analiz dosvidu 1990-kh rokiv)** [Ukraine's military power: Theoretical and methodological foundations]. Perun. 448 p.
17. Semenenko, O. M., Vodchyts, O. H., Dobrovolskyi, Yu. B., Boiko, R. V., & Kremeshnyi, O. I. (2015). *Metod otsiniuvannia voienno-ekonomichnykh umov rozvytku Zbroinykh Syl Ukrainy* [A method for assessing the military-economic conditions for the development of the Armed Forces of Ukraine]. **Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy**, (2[19]), 16–23.
18. Semenenko, O. M., Vodchyts, O. H., Boiko, R. V., & Ivanov, V. L. (2016). *Shchodo otsiniuvannia efektyvnosti vykonannia osnovnykh biudzhetnykh prohram Ministerstva oborony Ukrainy na period 2006–2014 rr.* [On evaluating the effectiveness of key MoD budget programs for 2006–2014]. **Zbirnyk naukovykh prats KhNUPS**, (1[46]), 41–45.
19. Zhukov, G. P., & Vikulov, S. F. (1981). **Voenno-ekonomicheskii analiz i issledovanie operatsii. Chast' 3: Kolichestvennye metody obosnovaniia voenno-ekonomicheskikh reshenii** [Military-economic analysis and operations research. Part 3]. Department of Economics of the Armed Forces (MFI). 252 p.
20. Shorin, V. G. (Ed.). (1973). **Ekonomiko-matematicheskie metody i modeli planirovaniia i upravleniia** [Economic-mathematical methods and models of planning and management] (Book 4). Znanie. 240 p.

Погляди щодо формування основних завдань та функцій системи органів управління оперативного угруповання військ в Збройних Силах України

Views on the Formation of the Main Tasks and Functions of the System of Command Bodies of the Operational Group of Troops in the Armed Forces of Ukraine

Тимур Куртсеітов ^A

Corresponding author: д.т.н., професор, заступник начальника науково-методичного центру організації наукової та науково-технічної діяльності, e-mail: kurttimur@ukr.net, ORCID: 0000-0001-6478-6469

Сергій Баранов ^A

здобувач Національного університету оборони України, e-mail: sharada3699@gmail.com, ORCID: 0000-0002-3306-943X

Володимир Ремез ^A

доктор філософії, доцент кафедри територіальної оборони, e-mail: remezv93145@gmail.com, ORCID: 0000-0002-2561-1081

Дмитро Рибак ^A

старший викладач кафедри територіальної оборони, e-mail: rybak.dima@ukr.net, ORCID: 0009-0005-4239-2131

Максим Самсоненко ^A

викладач кафедри управління військами, e-mail: samson8115@ukr.net, ORCID: 0009-0001-6264-6582

Ярослав Янковий ^A

ад'юнкт кафедри інформаційної боротьби, e-mail: ya.yankovyi@gmail.com, ORCID: 0009-0007-1718-3607

Tymur Kurtseitov ^A

Corresponding author: Dr of Technical Sciences, Professor, Deputy Head of the Scientific and Methodological Center for the Organization of Scientific and Scientific and Technical Activities, e-mail: kurttimur@ukr.net, ORCID: 0000-0001-6478-6469

Serhiy Baranov ^A

Postgraduate Military Student of the National Defense University of Ukraine, e-mail: sharada3699@gmail.com, ORCID: 0000-0002-3306-943X

Volodymyr Remez ^A

PhD, Associate Professor of the Department of Territorial Defense, e-mail: remezv93145@gmail.com, ORCID: 0000-0002-2561-1081

Dmytro Rybak ^A

Senior Teacher of the Department of Territorial Defense, e-mail: rybak.dima@ukr.net, ORCID: 0009-0005-4239-2131

Maksym Samsonenko ^A

Lecturer, Department of Command and Control of Troops, e-mail: samson8115@ukr.net, ORCID: 0009-0001-6264-6582

Yaroslav Yankovyi ^A

PhD student Department of Information Warfare, e-mail: ya.yankovyi@gmail.com, ORCID: 0009-0007-1718-3607

^AНаціональний університет оборони України, Київ, Україна

^ANational Defence University of Ukraine, Kyiv, Ukraine

Received: August 1, 2025 | Revised: August 11, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.24>

Мета роботи. Формування поглядів щодо визначення раціональної системи завдань та функцій системи органів управління оперативного угруповання військ в Збройних Силах України в операціях (бойових діях).

Метод дослідження. Аналіз; синтез; абстрагування та кон'юнктурного аналізу (мислення).

Результати дослідження. Проведено аналіз наявної наукової і аналітичної літератури, а також бойового досвіду та доктринально-нормативного підґрунтя з питання розподілу завдань та функцій системи органів управління оперативного угруповання військ в Збройних Силах України; визначено основні завдання та функції системи органів управління оперативного угруповання військ в Збройних Силах України відповідно до J-структур.

Теоретична цінність дослідження. Результати дослідження можуть бути використані під час удосконалення функціональних структур органів військового управління оперативно-стратегічної ланки управління в Збройних Силах України.

Тип статті. Теоретичний.

Ключові слова: ефективність управління, завдання та функції органів військового управління, оперативне угруповання військ (сил), операції (бойові дії), органи військового управління, стійкість управління військ (сил), ефективність.

Purpose. Formation of views on determining a rational system of tasks and functions of the system of command bodies of the operational group of troops in the Armed Forces of Ukraine in operations (combat actions).

Method. Analysis; synthesis; abstraction and situational analysis (thinking).

Findings. An analysis of the available scientific and analytical literature, as well as combat experience and doctrinal and normative basis on the issue of the distribution of tasks and functions of the system of command bodies of the operational group of troops in the Armed Forces of Ukraine was conducted; the main tasks and functions of the system of command bodies of the operational group of troops in the Armed Forces of Ukraine were determined in accordance with J-structures.

Theoretical implications. The results of the study can be used to improve the functional structures of the military command bodies of the operational-strategic level of command in the Armed Forces of Ukraine.

Paper type. Theoretical.

Key words: effectiveness management, tasks and functions of military command bodies, operational grouping of troops (forces), operations (combat actions), military command bodies, stability of the command system of troops (forces), effectiveness.

Вступ

У сучасних умовах повномасштабної збройної агресії російської федерації проти України питання ефективної організації управління силами оборони набуває вирішального значення. Досвід бойових дій засвідчує [1–3], що результативність застосування угруповань військ безпосередньо залежить від здатності системи органів управління (ОУ) забезпечувати безперервне, стійке, гнучке й адаптивне керівництво підпорядкованими силами. В умовах високої динаміки та невизначеності оперативного середовища, широкого використання противником високотехнологічних засобів ураження, засобів РЕБ, кібератак і розвідки, традиційні підходи до побудови органів управління оперативних угруповань військ виявляються недостатніми.

Необхідність своєчасного прийняття обґрунтованих рішень, координації спільних дій різномірних компонентів сил оборони, ефективного застосування сучасних систем озброєння та забезпечення сталої взаємодії вимагає переосмислення поглядів на структуру, завдання та функції органів управління оперативних угруповань військ (ОУВ) [1–19].

Особливої актуальності набуває наукове обґрунтування їх складу та функціонального наповнення з урахуванням сучасних стандартів НАТО, передового бойового досвіду та умов ведення війни високої інтенсивності на власній території.

Таким чином, формування оновленої системи органів управління оперативного угруповання військ у Збройних Силах (ЗС) України є одним із ключових чинників забезпечення ефективності стратегічного та оперативного управління під час триваючої війни, що й зумовлює актуальність обраної теми дослідження.

Теоретичні основи дослідження

Питання формування основних завдань і функцій системи органів управління ОУВ у сучасних ЗС України потребує врахування як реального бойового досвіду, так і доктринально-нормативного підґрунтя. У наявній науковій і аналітичній літературі можна виокремити три основні групи джерел: дослідження, засновані на аналізі російсько-української війни; іноземні доктрини та концепції управління; а також вітчизняні наукові розробки та нормативні документи [1–19].

Джерела першої групи – це аналітичні звіти та дослідження щодо російсько-української війни, які надають практично орієнтовані висновки про стан, проблеми та тенденції розвитку органів управління військами (силами) у бойових умовах. Регулярні оперативні зведення Russian Offensive Campaign Assessment Інституту вивчення війни (ISW) відзначають, що російські угруповання часто стикаються з розривами у системі командування та управління (C2), надмірною централізацією рішень і слабкою взаємодією між родами військ [1]. Ці висновки важливі, оскільки демонструють критичність гнучкості та узгодженості штабних структур. Дослідження RUSI Preliminary Lessons from Ukraine's Offensive Operations (2022–23) (Watling, Reynolds, Heidenkamp) підкреслює, що ефективність українських наступальних дій значною мірою залежала від здатності штабів оперативного рівня координувати дії різномірних підрозділів, швидко перерозподіляти ресурси та делегувати повноваження нижчим ланкам [2]. Аналогічні висновки містяться у вітчизняних збірниках ЦНДІ ЗС України, де узагальнено досвід застосування Сухопутних військ і наведено пропозиції щодо автоматизації та децентралізації управління на оперативному рівні [3]. Таким чином, аналіз практичного досвіду ведення війни підтверджує ключову роль органів управління оперативного угруповання у забезпеченні стійкості управлінського циклу, координації бойових дій і своєчасного прийняття рішень.

Друга група джерел охоплює іноземні доктрини і стандарти, що задають методологічні засади для визначення завдань та функцій штабів. У Allied Joint Doctrine for the Conduct of

Operations (AJP-3) НАТО визначено рамкову структуру планування і виконання операцій, описано ключові функції (управління, розвідка, вогневе ураження, логістика, C4ISR) та вимоги до узгодженості дій багатонаціональних компонентів [4]. Доктрина закладає принцип «mission command», який передбачає делегування повноважень і автономність дій підлеглих командирів. Американська доктрина FM 3-0 Operations (U.S. Army) доповнює цей підхід концепцією багатодомених операцій, у якій наголошується на інтеграції різномірних сил і постійній адаптивності командування [5]. Такі доктрини надають структурований підхід до визначення функцій органів управління, від планування і розподілу ресурсів до забезпечення управлінської стійкості, інформаційної переваги і логістичної підтримки. Їхні положення доцільно використовувати як концептуальну основу при формуванні української системи управління оперативними угрупованнями.

Третю групу становлять вітчизняні нормативно-правові та методичні документи, які визначають загальні принципи функціонування системи військового управління. Закон України “Про оборону України” встановлює правові основи організації та функціонування органів військового управління, їхні повноваження та завдання [6]. Воєнна доктрина України (Указ Президента № 555/2015) визначає базові підходи до планування і застосування ЗС України у воєнних конфліктах, задаючи стратегічну рамку для нижчих рівнів управління [7]. Операційно-тактичні документи Генерального штабу, такі як Інструкція з діловодства у Збройних Силах України (2023) та Настанова з бойової підготовки (2024), регламентують процеси роботи штабів, планування операцій, документообігу та координації з органами забезпечення [8; 9]. Окрему важливу групу джерел становлять наукові публікації ЦНДІ ЗСУ, які містять методичні підходи до побудови та оцінювання ефективності систем управління. Зокрема, Баталюк В. І. пропонує методику обґрунтування раціональної структури командування Сухопутних військ, спрямовану на оптимізацію розподілу функцій та підвищення оперативності управління [10]. Гусак Ю. А. досліджував моделі оцінювання оперативності управління та імітаційне моделювання ієрархічних систем управління [11; 12], Кірсанов С. О. розробив метод визначення вимог до живучості перспективних автоматизованих систем управління військами (АСУВ) [13], Волощенко О. – концептуальний підхід до оцінки внеску забезпечення в боєздатність військ [14]. Усі ці праці закладають науково-методичне підґрунтя для розроблення системи завдань і функцій органів управління ОУВ, враховуючи як структурно-організаційні, так і функціональні аспекти їх діяльності.

Узагальнюючи наведений аналіз, можна стверджувати, що сучасна система органів управління ОУВ має поєднувати практичний досвід, здобутий під час російсько-української війни, з найкращими зразками доктринального забезпечення країн НАТО та вимогами вітчизняної нормативної бази. Лише синтез цих джерел дозволить сформувати функціонально стійку, адаптивну та ефективну систему управління, спроможну забезпечити перевагу в умовах високодинамічної сучасної війни.

Постановка проблеми

Сучасні збройні конфлікти, зокрема війна в Україні, демонструють високий рівень динамічності та складності застосування військ на оперативному рівні. Органи управління ОУВ опиняються в умовах постійної необхідності швидкого прийняття рішень, координації дій різномірних підрозділів і адаптації до непередбачуваних змін у ситуації. Разом із тим існуючі підходи до формування завдань та функцій системи органів управління часто залишаються недостатньо узгодженими з реаліями сучасної війни, що може призводити до зниження ефективності управлінських процесів та втрати ініціативи на полі бою. В умовах постійної трансформації форм і способів застосування угруповань військ виникає необхідність системного аналізу та перегляду завдань і функцій органів управління з метою забезпечення

їхньої оперативної гнучкості та боєздатності, а також сучасної адаптації до стандартів НАТО за принципом J-структур.

Результати

У сучасних умовах ведення збройної боротьби, що характеризуються високою динамікою змін у бойовій обстановці, зростанням ролі інформаційного забезпечення та необхідністю комплексної взаємодії різнорідних сил і засобів, особливого значення набуває ефективна система управління ОУВ (об'єднаними тактичними угрупованнями). Для забезпечення безперервного, стійкого та гнучкого управління, кожне оперативне угруповання потребує чітко визначеної структури органів військового управління, здатної забезпечити планування, організацію, координацію та контроль виконання бойових завдань. З цією метою формується типовий склад органів керівництва та управління ОУВ та ОТУВ (оперативно-тактичного), який охоплює командування, центри, відділи та групи, що відповідають за всі ключові напрями діяльності угруповання — від розвідки, планування та логістики до морально-психологічного забезпечення й взаємодії з громадськістю.

Далі наведено приклад типового складу органів управління та управління оперативного угруповання військ (ОУВ, ОТУ): командування; центр персоналу (G1); центр розвідки (G2); центр управління поточними операціями (G3); відділ логістики (G4); центр планування застосування військ (G5); відділ зв'язку та інформаційних систем (G6); відділ підготовки (G7); відділ планування оборонних ресурсів (G8); відділення ЦВС (G9); відділ бойового застосування РВіА; відділ ППО; відділ армійської авіації; відділ сил підтримки; відділ морально-психологічного забезпечення; відділ ОДТ та захисту інформації; центр відновлення боєздатності та підготовки резервів; центр логістичного забезпечення; група транспортного забезпечення; група БпС; група медичного забезпечення; група фінансового забезпечення; центр моніторингу інформаційного простору та протидії; група міжнародного військового співробітництва; група внутрішнього контролю; група юридичного радника; адміністративна група; група зв'язків з громадськістю; оперативні групи ВСП та ІССО.

Командування призначено для безпосереднього управління військами, організації оперативного планування застосування військ (сил), у тому числі інших складових сил оборони, їх органів управління, переданих у підпорядкування відповідним органам військового управління. До складу командування входять командувач та його заступники або особи, які виконують їх обов'язки, за рішенням командувача можуть входити окремі підрозділи (інші посадові особи).

Об'єднаний штаб у складі центрів (відділів) J-структур, які формуються за рахунок штатних підрозділів органів військового управління, виконує завдання згідно свого бойового призначення.

Центр персоналу J 1 призначений для ведення оперативного обліку стану укомплектованості особовим складом частин (підрозділів), управління і контролю за виконанням заходів мобілізаційного розгортання підпорядкованих військ (частин, підрозділів) та органів (частин, підрозділів) інших складових сил оборони, доукомплектування та покриття втрат особового складу у ході їх застосування. До складу J 1, як правило, входять: відділ комплектування персоналом; відділ обліку втрат особового складу та стану укомплектованості військ (частин, підрозділів) та інші підрозділи за необхідністю.

Основними завданнями J 1 є: збір, аналіз та узагальнення оперативної інформації щодо стану укомплектованості частин (підрозділів) особовим складом; збір оперативної інформації щодо санітарних та безповоротних втрат особового складу, підготовка зведених донесень про втрати особового складу та стану укомплектованості частин (підрозділів); здійснення контролю за відправкою військово-навченого людського ресурсу та прибуттям їх для поповнення частин (підрозділів); підтримання взаємодії із структурними підрозділами КП,

взаємодіючими органами військового управління, органами управління інших складових сил оборони.

Центр розвідки J 2 призначений для забезпечення розвідувальною інформацією в інтересах планування застосування сил і засобів у ході підготовки та ведення операцій (бойових дій) та управління силами і засобами розвідки. До складу J 2, як правило, входять: відділ планування; відділ координації застосування сил і засобів розвідки та інші підрозділи за необхідністю.

Основними завданнями J 2 є: організація збору (добування) розвідувальних даних; оцінювання противника та підготовка висновків командувачу; збір та узагальнення даних щодо стану та положення сил і засобів розвідки; забезпечення командувача вихідними даними для вироблення замислу та формулювання (уточнення) рішення на операцію (бойові дії); безпосереднє (детальне) планування застосування сил і засобів розвідки у ході підготовки та ведення операції (бойових дій); управління визначеними силами і засобами розвідки; організація та здійснення взаємодії між органами військового управління, частинами (підрозділами) розвідки усіх видів (у тому числі родів військ), інших складових сил оборони; організація інформування заінтересованих структурних підрозділів КП, підпорядкованих, взаємодіючих органів військового управління, військ, інших складових сил оборони.

Центр управління операціями J 3 призначений для управління військами під час підготовки та в ході ведення операції (бойових дій). На J 3 здійснюється збір та узагальнення даних обстановки, робота щодо формулювання рішення у ході ведення поточних операцій, постановка завдань військам та безпосереднє управління військами. Центр управління операціями (далі – ЦУО) (J 3) за рахунок своїх структурних підрозділів формує (створює) основну функціональну складову ОКП (ПКП). ЦУО розгортається в спеціально обладнаних захищених спорудах, а в польових умовах – на базі спеціального комплексу командно-штабних (штабних) машин. Для роботи кожного структурного підрозділу J-3 обладнується окреме приміщення. У робочі приміщення J 3 допускаються особи, які мають безпосереднє відношення до завдань, за спеціальними перепустками (шифрам на перепустках) або списками. Перелік зазначених осіб затверджується командувачем (начальником штабу). Приміщення ЦУО оснащуються комплексами засобів автоматизації та зв'язку, які включають: командні пульти для передачі оперативних (бойових) документів, сигналів бойового управління та оповіщення; екрани (прилади) для відображення обстановки; інформаційні табло різних видів, апаратуру прийому та передачі графічних та текстових документів, дисплеї та інші засоби дистанційного введення та виведення інформації з ЕОМ, апаратуру документування, запису переговорів, друку та розмноження. ЦУО J 3 складається з оперативного складу штатного підрозділу, оперативних груп родів військ (сил) та інших складових сил оборони.

Структурними підрозділами J 3 можуть бути: відділ напрямків (оперативно-чергової служби); відділ поточних операцій; інформаційно-аналітичний відділ; відділ забезпечення та координації роботи штабу; відділ (група) узагальнення обстановки.

Основними завданнями J 3 є: розробка планувальних (поточних операцій) та директивних документів застосування військ в операції; доведення завдань до військ та контроль за їх виконанням; організація моніторингу стану військ, рівня їх навченості, стану ОБТ, забезпечення матеріально-технічними та іншими засобами; відстеження змін в оперативній обстановці (стан, положення, хід виконання завдань); підготовка доповідей, інформаційно-аналітичних та довідкових документів командувачу про стан та хід виконання визначених завдань військами; контроль за виконанням заходів, спрямованих на підтримання військ у готовності до виконання завдань за призначенням; управління військами в ході їх застосування, збір, узагальнення, аналіз обстановки в ході ведення поточних операцій (бойових дій), підготовка пропозицій командувачу щодо подальших дій; координація

діяльності інших структурних підрозділів КП; збір, обробка (аналіз, оцінка і узагальнення) відомостей, які містяться у доповідях, донесеннях та зведеннях, що надходять з вищих органів військового управління та підпорядкованих частин, ведення їх обліку; контроль за проходженням інформації; розподіл поточної інформації за змістом та призначенням, оперативна передача її всередині КП; аналіз, оцінка поточної інформації від підпорядкованих та взаємодіючих органів військового управління (органів), ІССО; інформування структурних підрозділів ПУ щодо розвитку оперативної обстановки; організація та несення оперативно-чергової служби; підготовка (ведення) звітно-інформаційних документів щодо складу, стану і положення військ, ходу (результатів) виконання ними завдань та дій військ противника.

Центр логістики J4 призначений для планування логістичного забезпечення відмобілізування, оперативного розгортання, підготовки та ведення операції (бойових дій) військ (сил).

Основними завданнями J4 є: планування логістичного забезпечення; планування мобілізаційної потреби у техніці та інших МТЗ; планування забезпечення матеріальних засобів, ведення їх оперативного обліку та контроль за їх отриманням; планування (створення, оновлення) оперативних запасів МТЗ; визначення потреб у військовому майні, послугах, земельних і водних ділянках, фондах та комунікаціях, необхідних для належного виконання завдань за призначенням; підготовка пропозицій командувачу щодо логістичного забезпечення подальших дій.

Підрозділ озброєння призначений для управління та організації технічного забезпечення підпорядкованих військ (частин, підрозділів) та органів (частин, підрозділів) інших складових сил оборони.

Основними завданнями підрозділу озброєння є: планування та управління технічним забезпеченням військ; добування, збір, вивчення, аналіз і оцінювання даних про якісний стан та рівень технічного забезпечення у ході підготовки і ведення операції (бойових дій), стану і можливостей сил і засобів технічного забезпечення; проведення оперативно-тактичних розрахунків та підготовка даних для вироблення замислу (формування рішення) на технічне забезпечення; визначення потреб в ОВТ, ракетах і боєприпасах, ВТМ, необхідних для забезпечення виконання військами визначених завдань; управління силами та засобами технічного забезпечення; уточнення (розроблення) і ведення оперативних (бойових) документів; організація і підтримання взаємодії зі структурними підрозділами КП та іншими органами державного і військового управління з питань технічного забезпечення військ.

Підрозділ тилу призначений для управління та організації тилового забезпеченням військ (частин, підрозділів) та органів (частин, підрозділів) інших складових сил оборони.

Основними завданнями підрозділу тилу є: планування та управління тиловим забезпеченням військ; добування (збір), вивчення, відображення, аналіз і оцінювання даних щодо забезпеченості військ ПММ, продовольством, речовим та технічним майном та іншими матеріальними засобами, стану і можливостей сил та засобів тилового забезпечення; проведення оперативних (тактичних) розрахунків за видами тилового забезпечення та підготовка даних для вироблення замислу (формулювання рішення) на тилове забезпечення військ; визначення потреб в ПММ, продовольстві, речовому і технічному майні, інших матеріальних засобів, необхідних для забезпечення виконання військами визначених завдань; уточнення (розроблення) та ведення оперативних (бойових) документів; організація і підтримання взаємодії з питань тилового забезпечення військ; організація військових сполучень на залізничному, морському, річковому, повітряному та автомобільному транспорті; проведення оперативно-тактичних розрахунків щодо військових перевезень; планування, управління та контроль за виконанням військових перевезень залізничним, автомобільним, морським, річковим та повітряним транспортом; розроблення оперативних (бойових) документів в частині, що стосується військових перевезень, та доведення їх до

транспортних органів; планування та управління підвезенням органам військового управління, частинам (підрозділам) усіх видів матеріальних засобів автомобільним транспортом підпорядкованих частин автотранспортного забезпечення.

Група транспортного забезпечення (військових перевезень) призначена для організації транспортного забезпечення підпорядкованих військ (сил), виконання та контролю автомобільних, залізничних перевезень, підготовки донесень, зведень, інформаційних, довідкових документів з питань військових перевезень.

Основними завданнями групи є: планування військових перевезень підпорядкованих військових частин в зоні відповідальності, контроль за підготовкою підрозділів до виконання завдань за призначенням; координація та організація узгодженої роботи по підготовці єдиної мережі шляхів сполучення, організація та керування здійсненням перевезень військ і вантажів різними видами транспорту; організація підвезення матеріальних засобів автомобільним транспортом військовим частинам; організація військових перевезень залізничним транспортом; збір, аналіз, узагальнення та надання необхідної інформації щодо стану мережі шляхів сполучень; участь у розробленні проектів наказів командира, інших нормативно-правових актів з питань військових перевезень військ (сил); підготовка звітно-інформаційних документів; збір, обробка (аналіз, оцінка і узагальнення) відомостей, які містяться у доповідях, донесеннях та зведеннях щодо військових перевезень, що надходять з вищих штабів та підпорядкованих частин, ведення їх обліку.

Група транспортного забезпечення відповідно до покладених на неї основних завдань: проводить збір, аналіз, оцінювання і відображення даних щодо стану транспортного забезпечення військових частин, положення та дії підпорядкованих частин (підрозділів, установ) логістичного забезпечення; приймає участь в оперативному плануванні застосування підпорядкованих частин і підрозділів логістичного забезпечення та управління ними під час виконання завдань за призначенням; організовує перевезення матеріальних засобів військових частин і контроль за їх виконанням; відпрацьовує та надає до органів військового управління донесень (звітів, відомостей) щодо виконання військових перевезень; здійснює організацію та керівництво автомобільних та залізничних перевезень по забезпеченню підпорядкованих військ (сил); організовує взаємодію з начальниками родів військ, управлінь, служб, відділів та груп КП з питань перевезення військових частин та матеріальних засобів; організовує взаємодію між командуванням військових частин та посадових осіб органів військових сполучень, підприємств, установ та організацій транспорту щодо своєчасного надання військовими частинами заявок на навантаження ешелонів (транспортів); веде облік виконання військових перевезень.

Центр планування застосування J5 призначений для організації та здійснення планування застосування військ, планування, організації, координації та контролю заходів безпеки застосування, вогневого ураження противника в інтересах застосування угруповання військ. До складу J5, як правило, входять: відділ (група) планування застосування (операції); відділ (група) безпеки операцій; відділ (група) планування управління та взаємодії. J5 складається з оперативного складу штатного підрозділу, в тому числі фахівців РВіА, авіації ПС та СВ, ВМС на постійній основі. За необхідності залучаються фахівці з РЕБ та інженерного забезпечення.

Основними завданнями J5 є: планування застосування (операції) військ (сил); планування і організація проведення заходів оперативного розгортання військ; збір, вивчення, аналіз і оцінювання даних обстановки; визначення переліку критичних об'єктів у складі угруповання військ противника та об'єктів військової інфраструктури для планування їх вогневого ураження; розробка варіантів застосування (способів дій) військ в операції; розробка плану рекогносцировки району операції (бойових дій); розробка плану організації управління; проведення оперативно-тактичних розрахунків, моделювання розроблених

варіантів дій військ та їх оцінка; підготовка пропозицій до замислу операції (бойових дій); забезпечення своєчасного формулювання рішення та його оформлення; планування та організація взаємодії, її підтримка в ході проведення операції; планування, координація та організація заходів безпеки застосування; координація та контроль за виконанням плану операції (бойових дій); координація діяльності інших центрів (відділів, груп) КП.

Центр (управління) об'єднаної вогневої підтримки призначений для планування та координації вогневого ураження.

До складу Центру (управління), як правило, входять: 1) відділ планування та координації ОВГП; 2) група планування ОВГП; 3) відділення (група) координації ОВГП; 4) група авіації; 5) група БпЛА; 6) група розвідки.

Основними завданнями Центру (управління) є: планування об'єднаної вогневої підтримки; управління (координація) силами і засобами, що залучаються до вогневої підтримки; взаємодія зі структурними підрозділами ОКП в інтересах реалізації завдань об'єднаної вогневої підтримки; організація артилерійської розвідки, повітряної розвідки противника в інтересах об'єднаної вогневої підтримки; оцінювання результатів (ефектів) об'єднаної вогневої підтримки; розподіл і контроль ресурсів (озброєння та військової техніки, боєприпасів) у підрозділах, які залучені до об'єднаної вогневої підтримки; координація дій засобів ОВГП (наземного, повітряного, морського компонентів) з метою запобігання ведення вогню по своїх підрозділах та мінімізації супутніх збитків; організація комплексного та ефективного застосування засобів об'єднаної вогневої підтримки (летальних і нелетальних, найбільш відповідних засобів для досягнення необхідних ефектів).

Центр зв'язку J 6 призначений для планування зв'язку, безпосереднього керівництва системами зв'язку, управління використанням радіочастотного ресурсу, організації виконання заходів щодо захисту систем зв'язку та інформаційних систем, у тому числі від кібернетичних загроз, організація технічного забезпечення зв'язку і автоматизації.

Основними завданнями J 6 є: збір та аналіз даних про стан системи зв'язку й обстановку зі зв'язку, прогнозування її розвитку; участь у виробленні замислу та розробленні (уточненні) плану застосування військ, розробленні оперативних (бойових) документів в частині, що стосується зв'язку; безпосереднє планування зв'язку; визначення та доведення завдань зі зв'язку підпорядкованим органам військового управління та бойових (спеціальних) завдань підпорядкованим частинам (підрозділам) зв'язку; підготовка та надання до вищого органу військового управління донесень із зв'язку; організація та керівництво розгортанням, нарощуванням та функціонуванням систем зв'язку, оперативне управління підпорядкованими частинами (підрозділами) зв'язку; організація зв'язку з підпорядкованими та взаємодіючими органами військового управління, частинами (підрозділами), у т.ч. інших складових сил оборони; організація контролю за проходженням оперативної інформації та оперативних документів через вузли зв'язку; організація оперативно-технічної служби та бойового чергування на вузлах, лініях, та об'єктах зв'язку; організація роботи служби єдиного часу і частотно-диспетчерської служби на вузлах зв'язку КП, участь в організації та проведенні заходів забезпечення електромагнітної сумісності радіоелектронних засобів; організація, керівництво та забезпечення захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах, перешкоджання роботі засобам технічних розвідок під час роботи засобів зв'язку; організація всебічного забезпечення системи зв'язку та частин (підрозділів) зв'язку; організація технічного забезпечення зв'язку і автоматизації військ; організація розгортання та переміщення КП.

Центр оперативної підготовки J 7 призначений для забезпечення планування та проведення заходів оперативної підготовки структурних підрозділів, перевірки та оцінки спроможностей підпорядкованих військ (сил), а також організації та здійснення вивчення,

узагальнення і впровадження досвіду застосування частин (підрозділів) в ході планування та ведення операції.

Основними завданнями J 7 є: збір, узагальнення та аналіз даних про стан готовності підпорядкованих військ (частин, підрозділів) та органів (частин, підрозділів) інших складових сил оборони; аналіз оперативних (бойових) можливостей та оцінка боездатності військ (частин, підрозділів); організація оперативної (бойової) підготовки, контроль повноти проведення заходів; взаємодія з органами інших складових сил оборони щодо підготовки їх сил та засобів до бойового застосування; збір та первинне оброблення інформації про застосування військ у ході ведення операції (бойових дій); розробка плану узагальнення досвіду ведення бойових дій; доведення до військ досвіду ведення операцій (бойових дій), нових способів застосування військ, результатів застосування противником нових видів зброї.

Центр цивільно-військового співробітництва J9 призначений для планування, організації та підтримання відносин між командуванням та цивільним населенням, місцевими органами виконавчої влади і органами місцевого самоврядування, міжнародними та неурядовими організаціями в зоні (районі) ведення операції (бойових дій), у районах проведення міжнародних миротворчих операцій та у районах проведення антитерористичних заходів, ліквідації наслідків НС техногенного та природного характеру.

Основними завданнями J 9 є: формування основних напрямів цивільно-військового співробітництва в ході ведення операції (бойових дій); розробка оперативних (бойових) документів у частині, що стосується цивільно-військового співробітництва; вивчення можливостей цивільної інфраструктури, що може бути використана в інтересах частин (підрозділів); визначення негативних чинників та настрою місцевого населення, оцінка його впливу на умови виконання завдань; участь у всіх етапах планування військової операції, планування завдань під час її проведення, а також після її закінчення.

Група міжнародного військового співробітництва призначена для здійснення загального планування заходів військового співробітництва за участю командувача та його заступників, координації заходів військового та військово-технічного співробітництва за участю представників військових частин.

Основними завдання: участь у координації діяльності під час планування та застосування підрозділів країн-партнерів під час виконання спільних дій у складі (за умови створення відповідних багатонаціональних угруповань, або прийняття відповідних рішень про спільні дії) угруповань військ (сил), сил і засобів інших складових сил оборони, та управління (координацію взаємодії) ними під час виконання завдань за призначенням; здійснення загального планування заходів військового співробітництва за участю командувача та його заступників; розроблення плану заходів військового співробітництва; координація заходів військового співробітництва за участю представників військових частин; відпрацювання звітних (інформаційно-аналітичних, довідкових) матеріалів щодо проведених заходів військового співробітництва та надання їх командиру (командувачу), контроль за своєчасністю та якістю звітування; прийняття участі у визначенні переліку осіб, які потребують оформлення сертифікатів перевірки персоналу на допуск до роботи з інформацією НАТО за відповідною категорією, та надсилання до Служби безпеки відповідних запитів для оформлення таких сертифікатів (за потреби); ведення ділового листування з питань військового співробітництва зі структурними підрозділами міжнародного співробітництва Міністерства оборони, Генерального штабу Збройних Сил, військових частин і установ; організація взаємодії військ з іншими військовими формуваннями та правоохоронними органами щодо миротворчої діяльності с залученням військ.

На КП з урахуванням їх функціонального призначення можуть не створюватися деякі структурні підрозділи типової структури або додатково (рішенням відповідних посадових осіб) створюватися інші.

Висновки

Аналіз сучасного стану органів управління ОУВ показав, що ефективність їх діяльності значною мірою залежить від чіткої структури, розподілу завдань між штабами та підрозділами, а також від впровадження уніфікованих процедур планування та взаємодії. Типовий склад ОКП ОУВ (ОТУ) забезпечує функціонування ключових компонентів управління таких як: планування, розвідки, вогневого ураження, логістики, інформаційного та технологічного забезпечення, що створює умови для оперативної гнучкості угруповання. Завдання органів управління на оперативному рівні включають координацію бойових дій, розподіл ресурсів, забезпечення управлінської стійкості та безперервності управління, адаптацію планів відповідно до зміни обстановки та контроль за виконанням рішень. Чітке визначення функцій і повноважень дозволяє уникнути дублювання роботи та скоротити час прийняття рішень у динамічних бойових умовах.

Розробка та впровадження Типового складу ОКП ОУВ (ОТУ) у ЗС України слугує основою для стандартизації процедур, уніфікації командних взаємодій та підвищення ефективності оперативного управління угрупованням військ. Це також дозволяє швидко інтегрувати нові технології, автоматизовані системи управління та засоби розвідки, що забезпечує інформаційну перевагу та підвищує боєздатність угруповання. Науково-методичні підходи до визначення завдань і функцій органів управління, розроблені ЦНДІ ЗСУ, підтверджують необхідність комплексного підходу, який враховує як організаційні, так і функціональні аспекти діяльності штабів, і створюють основу для подальшого вдосконалення управлінських структур, що є критично важливим у контексті сучасної війни та розвитку асиметричних і багатодомених операцій.

Узагальнення досвіду ведення бойових дій, аналіз сучасних іноземних доктрин та вітчизняних нормативних документів дозволяють зробити висновок, що ефективна система органів управління ОУВ має поєднувати структурованість, гнучкість та технологічну підтримку, що забезпечує перевагу у прийнятті рішень та координованому застосуванні військ у складних умовах сучасного бою.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Institute for the Study of War. Russian Offensive Campaign Assessment. Вашингтон, 2022–2025. URL: <https://www.understandingwar.org>
2. Watling J., Reynolds N., Heidenkamp H. Preliminary Lessons from Ukraine's Offensive Operations (2022–23). London: RUSI, 2023. 64 p.
3. Ніколаєнко М. В., Сірченко Р. С., Кузнєцов О. А. Рекомендації щодо удосконалення організації об'єднаних операцій Сил оборони України Центральний науково-дослідний інститут Збройних Сил України. Збірник наукових праць ЦНДІ ЗС України №1(112). Київ: ЦНДІ ЗС України, 2025. ISSN 2414-0651. С.111-119.
4. NATO Standardization Office. Allied Joint Doctrine for the Conduct of Operations (AJP-3). Brussels: NATO, 2022. 168 p.
5. U.S. Department of the Army. Field Manual FM 3-0 Operations. Washington, D.C.: Headquarters, Department of the Army, 2022. 336 p.

6. Закон України “Про оборону України” від 06.12.1991 №1932-XII. URL: <https://zakon.rada.gov.ua/laws/show/1932-12>
7. Президент України. Воєнна доктрина України: Указ Президента України від 24.09.2015 №555/2015. URL: <https://zakon.rada.gov.ua/laws/show/555/2015>
8. Генеральний штаб Збройних Сил України. Інструкція з діловодства у Збройних Силах України (наказ ГШ ЗСУ від 15.08.2023 №250). Київ: МО України, 2023.
9. Генеральний штаб Збройних Сил України. Настанова з бойової підготовки Збройних Сил України (ред. 2024). Київ: МО України, 2024.
10. Баталюк В. І. Методичний підхід до обґрунтування раціональної структури командування Сухопутних військ Збройних Сил України. Зб. наук. пр. ЦНДІ ЗСУ, 2024.
11. Гусак Ю. А. Спосіб оцінювання оперативності управління під час виконання оперативних (бойових) завдань. Зб. наук. пр. ЦНДІ ЗСУ, 2024.
12. Гусак Ю. А. Імітаційна модель для дослідження ієрархічних систем управління військами. ЦНДІ ЗСУ, 2025.
17. Кірсанов С. О. Метод обґрунтування вимог до живучості перспективної автоматизованої системи управління військами (АСУВ). Зб. наук. пр. ЦНДІ ЗСУ / ДНДІВСВТ, 2022.
18. Семененко О. М., Митченко С. І., Добровольський Ю. В., Твердохліб Є. О. Еволюція форм і способів застосування угруповань військ (сил): тенденції збройної боротьби. *Збірник наукових праць Центрального науково-дослідного інституту Збройних Сил України*. Київ: ЦНДІ ЗСУ, 2024. № 2(108). С. 45–56. URL: <https://znpcvds.nuou.org.ua/article/view/XXXXX>
19. Волощенко О. Концептуальний підхід до визначення необхідного внеску інженерних видів забезпечення у забезпеченні боєздатності військ (сил). Зб. наук. пр. ЦНДІ ЗСУ, 2024.

References

1. Institute for the Study of War. (2022–2025). *Russian offensive campaign assessment*. Washington, DC. <https://www.understandingwar.org>
2. Watling, J., Reynolds, N., & Heidenkamp, H. (2023). *Preliminary lessons from Ukraine’s offensive operations (2022–23)*. London: Royal United Services Institute (RUSI).
3. Nikolaenko, M. V., Sirchenko, R. S., & Kuznetsov, O. A. (2025). Recommendations for improving the organization of joint operations of the Defense Forces of Ukraine. *Collection of Scientific Papers of the Central Research Institute of the Armed Forces of Ukraine*, 1(112), 111–119. Central Research Institute of the Armed Forces of Ukraine. ISSN 2414-0651.
4. NATO Standardization Office. (2022). *Allied joint doctrine for the conduct of operations (AJP-3)*. Brussels: NATO.
5. U.S. Department of the Army. (2022). *Field manual FM 3-0: Operations*. Washington, DC: Headquarters, Department of the Army.
6. Verkhovna Rada of Ukraine. (1991, December 6). *On the defense of Ukraine* (Law of Ukraine No. 1932-XII). <https://zakon.rada.gov.ua/laws/show/1932-12>
7. President of Ukraine. (2015, September 24). *Military doctrine of Ukraine* (Presidential Decree No. 555/2015). <https://zakon.rada.gov.ua/laws/show/555/2015>
8. General Staff of the Armed Forces of Ukraine. (2023). *Instruction on office work in the Armed Forces of Ukraine* (Order No. 250 of 15 August 2023). Kyiv: Ministry of Defense of Ukraine.
9. General Staff of the Armed Forces of Ukraine. (2024). *Manual on combat training of the Armed Forces of Ukraine* (2024 ed.). Kyiv: Ministry of Defense of Ukraine.
10. Bataliuk, V. I. (2024). Methodological approach to substantiating the rational command structure of the Ukrainian Ground Forces. *Collection of Scientific Papers of the Central Research Institute of the Armed Forces of Ukraine*.
11. Husak, Yu. A. (2024). Method for assessing the efficiency of command during the execution of

- operational (combat) tasks. *Collection of Scientific Papers of the Central Research Institute of the Armed Forces of Ukraine*.
12. Husak, Yu. A. (2025). *Simulation model for the study of hierarchical command and control systems*. Central Research Institute of the Armed Forces of Ukraine.
13. Kirsanov, S. O. (2022). Method for substantiating requirements for survivability of a prospective automated command and control system (ACYB). *Collection of Scientific Papers of the Central Research Institute of the Armed Forces of Ukraine / State Research Institute of Armament and Military Equipment Testing*.
14. Semenenko, O. M., Mytchenko, S. I., Dobrovolskyi, Yu. V., & Tverdokhlib, Ye. O. (2024). Evolution of the forms and methods of employing troop groupings: Trends in armed struggle. *Collection of Scientific Papers of the Central Research Institute of the Armed Forces of Ukraine*, 2(108), 45–56. <https://znp-cvsvd.nuou.org.ua/article/view/XXXXX>
15. Voloshchenko, O. (2024). Conceptual approach to determining the necessary contribution of engineering support to ensuring the combat readiness of troops (forces). *Collection of Scientific Papers of the Central Research Institute of the Armed Forces of Ukraine*.

Модернізація оборонно-промислового комплексу України в умовах воєнних викликів: проблеми, перспективи та стратегічні пріоритети

Modernization of Ukraine's Defense-Industrial Complex under Wartime Challenges: Problems, Prospects, and Strategic Priorities

Віталій Половенко

Vitalii Polovenko

кандидат військових наук, докторант,
polovenko469@gmail.com, ORCID: 0000-0002-1753-395X

e-mail: Candidate of Military Sciences, Doctoral Candidate, e-mail:
polovenko469@gmail.com, ORCID: 0000-0002-1753-395X

Національний університет оборони України, м. Київ, Україна

National Defense University of Ukraine, Kyiv, Ukraine

Received: August 11, 2025 | Revised: August 25, 2025 | Accepted: August 31, 2025

УДК 351.864

DOI: <https://doi.org/10.33445/sds.2025.15.4.25>

Мета роботи: Аналіз сучасного стану та ключових проблем модернізації оборонно-промислового комплексу України в умовах триваючої воєнної агресії, а також обґрунтування стратегічних пріоритетів його розвитку з метою зміцнення національної безпеки та обороноздатності держави.

Метод дослідження: Дослідження ґрунтується на комплексному методологічному підході, що включає аналіз і синтез наукової літератури, порівняльний аналіз, системний аналіз, логико-структурний аналіз, а також вивчення нормативно-правових актів, що регламентують функціонування сектору безпеки і оборони України.

Результати дослідження: У ході дослідження виявлено системні проблеми функціонування оборонно-промислового комплексу України, зокрема застарілість виробничої інфраструктури, недостатній рівень фінансування, технологічну залежність та обмежену конкурентоспроможність на світових ринках. Проведений аналіз засвідчує наявність позитивної динаміки у виробництві бронетехніки, високоточної зброї та безпілотних літальних апаратів, водночас підкреслюючи збереження значної частки застарілого озброєння і військової техніки. Обґрунтовано стратегічні пріоритети модернізації, зокрема нарощування інвестицій у науково-дослідні та дослідно-конструкторські роботи, розвиток державно-приватного партнерства, розширення міжнародної співпраці та вдосконалення механізмів управління і фінансування.

Теоретична цінність дослідження: Дослідження робить внесок у теоретичне осмислення модернізації оборонно-промислового комплексу шляхом систематизації підходів до розвитку оборонного сектору в умовах воєнного часу та розширення концептуальних засад щодо ролі оборонної промисловості у забезпеченні національної безпеки й економічної стійкості держави.

Практична цінність дослідження: Отримані результати можуть бути використані органами державної влади, суб'єктами оборонного планування та стейкхолдерами оборонно-промислового комплексу під час формування й коригування державної політики, оборонних стратегій і програм модернізації оборонно-промислового комплексу. Результати дослідження також можуть застосовуватися в освітній та науково-аналітичній діяльності у сферах безпекових досліджень і оборонної економіки.

Тип статті: теоретична.

Purpose: To analyze the current state and key challenges of the modernization of Ukraine's defense-industrial complex under conditions of ongoing military aggression and to substantiate strategic priorities for its development aimed at strengthening national security and defense capabilities.

Method: The study is based on a comprehensive methodological approach that includes analysis and synthesis of scientific literature, comparative analysis, system analysis, logical-structural analysis, and examination of regulatory and legal documents governing the security and defense sector of Ukraine.

Findings: The study identifies systemic problems in the functioning of Ukraine's defense-industrial complex, including outdated production infrastructure, insufficient financing, technological dependence, and limited competitiveness in global markets. The analysis demonstrates positive dynamics in the production of armored vehicles, high-precision weapons, and unmanned aerial systems, while highlighting the persistence of a high share of obsolete weapons and equipment. Strategic priorities for modernization are substantiated, including increased investment in R&D, development of public-private partnerships, expansion of international cooperation, and improvement of management and financing mechanisms.

Theoretical implications: The study contributes to the theoretical understanding of defense-industrial modernization by systematizing approaches to the development of the defense sector under wartime conditions and by expanding conceptual frameworks related to the role of the defense industry in ensuring national security and economic resilience.

Practical implications: The findings may be used by public authorities, defense planners, and defense-industry stakeholders in the formulation and adjustment of state policies, defense strategies, and programs for the modernization of the defense-industrial complex. The results are also applicable in educational and analytical activities in the fields of security studies and defense economics.

Paper type: Theoretical.

Ключові слова: оборонно-промисловий комплекс, модернізація, національна безпека, власне виробництво, фінансування, інновації, військові виклики, стратегічні пріоритети, державно-приватне партнерство.

Key words: Defense-industrial complex, modernization, national security, domestic production, financing, innovation, military challenges, strategic priorities, public-private partnership.

Вступ

Сучасний оборонно-промисловий комплекс (ОПК) України стикається з низкою критичних викликів, які вимагають негайного та системного вирішення. Насамперед, значною перешкодою є застаріла структура промисловості, що успадкована з радянських часів і не повною мірою відповідає потребам сучасної війни. Ця проблема посилюється недостатньою адаптацією до динамічних військово-політичних завдань, що постійно еволюціонують, а також відсутністю глибокого та всебічного аналізу ринкових закономірностей, що гальмує розвиток конкурентоспроможної та інноваційної продукції.

В умовах повномасштабного вторгнення та триваючої агресії, ці проблеми набувають особливої гостроти, адже ефективність функціонування ОПК безпосередньо впливає на обороноздатність країни та її здатність протистояти зовнішнім загрозам. Застарілі виробничі потужності, брак сучасних технологій та кваліфікованих кадрів, а також відсутність чіткої стратегії розвитку стримують потенціал України у виробництві високотехнологічного озброєння та військової техніки.

Проте, ці виклики водночас є каталізатором для трансформаційних змін та відкривають унікальні можливості для реформування та розвитку ОПК. Необхідність швидкої модернізації, інтеграції інноваційних підходів та налагодження ефективної взаємодії між державою, наукою та промисловістю стає ключовим фактором успіху.

Таким чином, проблема полягає у критичній потребі розробки та впровадження комплексної стратегії модернізації ОПК України, що дозволить не лише подолати існуючі структурні та технологічні недоліки, але й забезпечить його перетворення на потужний, інноваційний та конкурентоспроможний сектор економіки, здатний ефективно забезпечувати національну безпеку та сприяти економічному розвитку країни в умовах сучасних геополітичних викликів.

Теоретичні основи дослідження

Останні наукові розвідки про український оборонно-промисловий комплекс висвітлюють широкий спектр питань: від стратегічного планування до фінансового забезпечення та взаємодії з іншими секторами економіки. Ці дослідження допомагають глибше зрозуміти як виклики, так і можливості, що стоять перед вітчизняним ОПК.

Ефективність державного регулювання є одним з ключових аспектів, що розглядається науковцями. Наприклад, В. Рижих та П. Богуцький [1] пропонують механізми, які можуть значно підвищити ефективність управління оборонним сектором економіки через кращу координацію економічної, фінансової, організаційно-правової участі держави.

Питання фінансування галузі також привертає значну увагу. У. Ватаманюк-Зелінська [2] наголошує, що недостатній обсяг капітальних вкладень в інноваційні розробки може суттєво уповільнювати прогрес ОПК. Це підкреслює критичну потребу в адекватному інвестуванні для стимулювання інновацій.

Позитивні зрушення у створенні умов для розвитку оборонної промисловості та продукції подвійного призначення відзначає С. Кулицький [3]. Це особливо актуально в контексті постійно зростаючих потреб національної оборони.

Дослідження також акцентують увагу на важливості міжнародної співпраці та партнерства. К. Слободяник [4] вказує, що співпраця оборонної промисловості з транснаціональними компаніями може стати потужним стимулом для розвитку новітніх технологій та розширення експорту оборонної продукції.

Сучасні наукові розвідки також розглядають питання інноваційного розвитку та реформування системи управління ОПК. Так, О. Тимошенко [6] зосереджується на механізмах

стимулювання технологічного прогресу та інтеграції у світові інноваційні мережі, підкреслюючи важливість державно-приватного партнерства та венчурного фінансування.

Однак, існують і перешкоди. А. Савицький [5] звертає увагу на проблему взаємодії ОПК з іншими галузями економіки, яка може гальмувати повний розвиток сектора. Подібні дослідження, як у П. Толоки [7], підкреслюють важливість взаємодії оборонної промисловості із зовнішнім середовищем через партнерства та співробітництво для зміцнення фінансової безпеки підприємств.

Всі ці наукові роботи роблять вагомий внесок у розуміння поточного стану та перспектив українського ОПК. Проте, зважаючи на агресію з боку РФ та необхідність забезпечення подальшого економічного зростання, потрібне додаткове наукове обґрунтування конкретних шляхів розвитку оборонної промисловості (ОП) в умовах воєнного часу, аби розробити ефективні рішення та стратегії для її подальшого зміцнення та інтеграції у світовий ринок.

Постановка проблеми

Метою статті є формування чіткого бачення шляхів розвитку ОП України, що має вирішальне значення для національної безпеки в умовах триваючої воєнної агресії. У центрі уваги стоїть трансформаційний перехід від переважного імпорту до власного повноцінного виробництва озброєння та військової техніки (ОВТ). Цей стратегічний крок є безальтернативним, адже лише він забезпечить Україні справжній стратегічний контроль над власною обороноздатною сферою, зменшуючи критичну залежність від зовнішніх поставачань.

Для досягнення цієї мети стаття зосередиться на комплексному аналізі фінансування та оцінці економічної ефективності. Ми дослідимо поточні механізми фінансування оборонного виробництва та проаналізуємо дохідність підприємств ОПК. Це дозволить не лише оцінити поточну ефективність, а й виявити резерви для підвищення стабільності та самодостатності галузі.

Також важливо глибоко вивчити проблеми, що гальмують розвиток оборонної промисловості. До них належать критичні питання логістики, забезпечення кадрового потенціалу, доступу до сировини та критично важливих технологій. Розуміння цих викликів є першочерговим для розробки дієвих стратегій їх подолання.

Представлене наукове дослідження покликане стати надійним фундаментом для прийняття обґрунтованих рішень на рівні державної політики та формування ефективних стратегій розвитку ОП. Воно дозволить не тільки всебічно оцінити наявні проблеми оборонної галузі, а й чітко визначити пріоритетні напрямки фінансування. Це, у свою чергу, відіграє ключову роль у забезпеченні стабільного та динамічного розвитку цієї стратегічно важливої сфери, що є запорукою стійкості та обороноздатності України.

Результати

Цільова спрямованість оборонно-промислового комплексу дійсно визначається його тісною взаємодією з військовими структурами та виробництвом продукції військового призначення. Важливо розрізняти ОПК та оборонну промисловість. ОПК є ширшим поняттям, що охоплює комплекс функцій та партнерств, тоді як оборонна промисловість зосереджена безпосередньо на виробництві військової техніки та обладнання.

Постійне зростання вартості інноваційних товарів та послуг є суттєвим фактором, що впливає на ОП. Новітні технології та розробки відіграють ключову роль у підтримці оборонної потужності країни, що, своєю чергою, значно впливає на фінансові рішення щодо розвитку та підтримки ОПК. З огляду на ці фактори, критично важливо продовжувати розвивати та модернізувати оборонну промисловість, забезпечуючи не лише ефективність виробництва, а й його відповідність найсучаснішим стандартам та технологіям. Такий підхід допоможе

зберегти й посилити оборонну потужність країни в умовах мінливого геополітичного середовища.

Державний концерн “Українська оборонна промисловість” відіграє ключову роль у розвитку ОПК України. Об’єднання у своєму складі представників різних оборонних галузей забезпечує комплексний підхід до виробництва, модернізації та ремонту ОВТ. Наявність наукових установ і промислових підприємств у концерні дозволяє поєднувати наукові дослідження з практичною реалізацією проєктів у сфері оборонної техніки. Зокрема, співпраця з авіаційною, радіоелектронною, суднобудівною та іншими галузями дає змогу створювати інтегровані та високоякісні оборонні системи [8].

Такий підхід до організації оборонної промисловості сприяє ефективному використанню ресурсів, підвищенню якості виробів та забезпеченню відповідності міжнародним стандартам. Це також стимулює розвиток інноваційних технологій та надає Україні можливість бути конкурентоспроможною на світовому ринку оборонної продукції.

Для повноцінного розуміння поточного стану та перспектив розвитку ОПК України необхідно проаналізувати обсяги виробництва продукції ключовими галузями оборонної промисловості. Цей аналіз дозволяє оцінити внесок окремих секторів у загальну обороноздатність країни, виявити сильні та слабкі сторони, а також визначити пріоритетні напрямки для інвестицій і модернізації.

Основними галузями оборонної промисловості України є авіабудування, суднобудування, виробництво бронетехніки, ракетно-артилерійського озброєння, радіоелектроніки та високоточної зброї. Кожна з цих галузей має свої особливості, виклики та потенціал для розвитку. Наприклад, авіабудівна галузь, представлена підприємствами державного концерну “Українська оборонна промисловість”, такими як ДП “Антонов”, зосереджена на модернізації літаків і розробці нових моделей, які відповідають сучасним вимогам. Суднобудування, попри значний потенціал, стикається з обмеженнями через брак інвестицій та застарілі виробничі потужності. Виробництво бронетехніки, зокрема танків і бронетранспортерів, демонструє позитивну динаміку завдяки підвищеному попиту в умовах війни, але потребує оновлення технологій та розширення виробничих ліній.

За даними відкритих джерел, у 2023–2024 роках обсяги виробництва в окремих сегментах ОПК України показали зростання, зокрема у сфері виробництва безпілотних літальних апаратів (БПЛА) та високоточної зброї. Це зумовлено як внутрішніми потребами Збройних Сил (ЗС) України, так і зростанням експортного потенціалу. Наприклад, за оцінками експертів, виробництво БПЛА зросло в кілька разів порівняно з довоєнним періодом, що стало відповіддю на сучасні виклики гібридної війни. Водночас, у таких галузях, як суднобудування, обсяги виробництва залишаються обмеженими через логістичні проблеми та недостатнє фінансування.

Аналіз кількісних показників обсягів виробництва дещо ускладнено через обмежену доступність відкритої інформації в умовах воєнного часу. Проте, за оцінками аналітиків, підприємства ОПК України у 2024 році змогли забезпечити значну частину потреб армії у боєприпасах, легкій бронетехніці та засобах радіоелектронної боротьби. Наприклад, виробництво 155-мм артилерійських снарядів, яке раніше було критично залежним від імпорту, почало поступово налагоджуватися завдяки створенню нових виробничих ліній за підтримки міжнародних партнерів.

Аналіз обсягів виробництва також вказує на необхідність диверсифікації та інтеграції сучасних технологій. Наприклад, впровадження автоматизованих систем управління виробництвом та використання штучного інтелекту у розробці озброєння може значно підвищити продуктивність і якість продукції. Крім того, співпраця з міжнародними партнерами, зокрема через спільні підприємства та трансфер технологій, відкриває можливості для нарощування виробництва та виходу на нові ринки.

Таким чином, аналіз обсягів виробництва галузями ОП України підкреслює як досягнення, так і виклики, що потребують негайного вирішення. Подальше зростання виробництва можливе за умови реалізації комплексної стратегії модернізації, яка включатиме інвестування в нові технології, підготовку кадрів, оптимізацію логістики та розширення міжнародного співробітництва. Це дозволить не лише задовольнити внутрішні потреби, але й зміцнити позиції України на глобальному ринку оборонної продукції.

Збільшення обсягів виробництва озброєння та військової техніки є важливим успіхом української ОБ, що підкреслює зростання її ефективності та потенціалу. Проте, 80 % застарілого озброєння та військової техніки залишаються значним викликом, що вимагає невідкладного вирішення.

Розташування підприємств оборонної промисловості в межах науково-промислових кластерів сприяє оптимізації взаємодії та координації між ними, що є важливим фактором для досягнення успіху у сфері виробництва оборонної техніки. Така концентрація дозволяє ефективніше використовувати ресурси, обмінюватися технологіями та спільно вирішувати складні завдання, пов'язані з розробкою і виготовленням високотехнологічної продукції.

Для забезпечення конкурентоспроможності вітчизняної ОП необхідна системна трансформація та оновлення її інфраструктури. Це передбачає не лише створення сучасної техніки, але й впровадження новітніх технологічних рішень у виробничі процеси та вдосконалення системи управління. Модернізація має охоплювати всі аспекти діяльності – від розробки інноваційних продуктів до оптимізації управлінських процедур, що дозволить відповідати міжнародним стандартам якості та технологій.

Збільшення обсягів виробництва є важливим кроком, але для гарантування національної безпеки необхідно також забезпечити постійне оновлення та вдосконалення ОВТ. Окрім цього, ключовим аспектом є підвищення ефективності управлінських і контрольних механізмів, які забезпечують стабільність і якість роботи оборонного сектору.

Завдяки рішенням Ради національної безпеки і оборони України, затверджені Указом Президента України від 16 лютого 2022 року №56/2022 “Про Стратегію забезпечення державної безпеки”, визначено необхідність формування ефективної бюджетної політики в секторі безпеки та оборони. Цей документ підкреслює критичну важливість адекватного фінансового забезпечення для підтримки обороноздатності країни. Згідно з нормативною базою, зокрема Законом України “Про національну безпеку України” [10] та законами про Державний бюджет України на 2019-2023 роки [11-15], мінімальний рівень фінансування сектору безпеки та оборони встановлено на рівні не менше 5% ВВП, з яких щонайменше 3% мають бути спрямовані на потреби сил оборони.

Проте, незважаючи на ці законодавчі норми, фактичне фінансування Міністерства оборони України у період з 2019 по 2023 роки становило лише 2,1–2,4% ВВП. Такий рівень фінансування створює серйозні виклики для розвитку оборонного сектору, особливо в умовах сучасних геополітичних та безпекових загроз. Недостатнє фінансування обмежує можливості для модернізації техніки, закупівлі нового обладнання та впровадження інноваційних технологій.

Станом на 2024 рік та у перспективі 2025 року, ситуація з фінансуванням зазнала суттєвих змін внаслідок повномасштабного вторгнення. Хоча точні відсотки від ВВП можуть коливатися, абсолютні обсяги видатків на оборону значно зросли, відображаючи пріоритетність забезпечення потреб ЗС України. Фінансування оборонного сектору здійснюється як за рахунок внутрішніх ресурсів (державний бюджет, військові облігації, внутрішні запозичення), так і завдяки значній міжнародній фінансовій та воєнній допомозі. Уряд України продовжує працювати над формуванням ефективної бюджетної політики, спрямованої на стабільне та достатнє фінансування оборонного потенціалу, що відповідатиме реальним потребам армії та дозволить інвестувати в оновлення техніки, розвиток інноваційних технологій та підготовку кваліфікованих кадрів [16-17].

Для зміцнення оборонного потенціалу України необхідно забезпечити стабільне та достатнє фінансування, яке відповідатиме реальним потребам Збройних Сил України. Це включає інвестиції в оновлення техніки, розвиток інноваційних технологій і підготовку кваліфікованих кадрів. Такий підхід є критично важливим для підвищення ефективності оборонної промисловості та забезпечення національної безпеки в умовах сучасних викликів.

Нинішній стан фінансування сектору безпеки й оборони України характеризується недостатнім обсягом коштів, що ускладнює повноцінну модернізацію та оновлення оборонного потенціалу. Обмеженість оборонного бюджету та нерівномірний розподіл ресурсів створюють значні перешкоди для забезпечення національної безпеки. Зокрема, повільне оновлення основних видів озброєння та недостатнє фінансування сил оборони ускладнюють постачання сучасних військових систем, що є критично важливим в умовах сучасних викликів.

Зростаюча потреба в переозброєнні та модернізації вимагає пошуку нових джерел фінансування та інноваційних підходів до розвитку ОП. Одним із перспективних рішень є активізація державно-приватного партнерства. Залучення приватних компаній до виробництва оборонної техніки може не лише розвантажити державні підприємства, але й сприяти впровадженню новітніх технологій і гнучких підходів до розробки та виготовлення озброєння. Приватний сектор здатен забезпечити швидшу адаптацію до сучасних вимог і підвищити ефективність виробництва.

Такий формат співпраці сприятиме прискоренню оновлення військової техніки та забезпечить відповідність оборонних систем міжнародним стандартам. Державно-приватне партнерство може стати основою для трансформації оборонного сектору, дозволяючи Україні зміцнити свою обороноздатність у відповідь на сучасні геополітичні виклики.

Незважаючи на спроби агресора послабити українську ОП, Україна продемонструвала значний прогрес у нарощуванні виробництва зброї та підтримці власної обороноздатності. Це стало можливим завдяки ефективним заходам, вжитим урядом для підтримки оборонного сектору та забезпечення потреб ЗС України. Зростання обсягів виробництва ОВТ є важливим фактором, що зміцнює оборонний потенціал країни та сприяє її стійкості в умовах триваючої агресії з боку рф.

Україна володіє значними виробничими можливостями та технологічними досягненнями в ОП, які дозволяють їй ефективно відновлювати та розвивати власний потенціал у сфері виробництва ОВТ. Ці успіхи підкреслюють рішучість України у зміцненні своєї обороноздатності та здатність країни відстоювати власну незалежність і суверенітет у складних геополітичних умовах.

Розвиток оборонної промисловості України є стратегічно важливим для зміцнення обороноздатності країни в умовах геополітичних викликів та триваючого конфлікту з рф. Посилення виробництва озброєння та боєприпасів дозволяє Україні не лише забезпечувати власні ЗС, але й підвищувати свою стійкість у сучасному воєнному середовищі.

Серед основних напрямків розвитку виділяють: активізацію виробництва артилерійських снарядів, зокрема стандартів НАТО, і бронетехніки, що сприяє підвищенню бойової ефективності ЗС України та дозволяє українським військам ефективніше діяти в умовах сучасних бойових операцій. Нарощування виробництва бронетранспортерів та інших видів броньованої техніки забезпечує більшу мобільність і захист для військ на полі бою.

Особливе значення має розвиток БПЛА, включаючи розвідувальні та ударні моделі, а також боєприпасів до них, що значно посилює можливості ЗС України у розвідці, моніторингу та високоточному ураженні цілей. Крім того, виробництво систем радіоелектронної боротьби відіграє ключову роль у протидії сучасним технологічним загрозам, зокрема ворожим безпілотникам, забезпечуючи захист військ (сил). Ці напрямки підкреслюють критичну роль ОП у зміцненні національної безпеки України в умовах сучасних викликів.

Ці напрямки підкреслюють критичну роль ОП у зміцненні національної безпеки України в умовах сучасних викликів.

Інвестиції в оборонне виробництво є необхідною умовою для оновлення та модернізації техніки й технологій. За оцінками експертів, фізичний і моральний знос основного капіталу оборонного комплексу становить 30–40%, що вказує на потребу у значних капіталовкладеннях. ОП не лише сприяє зміцненню безпеки, але й має суттєвий вплив на економіку країни, створюючи робочі місця та стимулюючи суміжні галузі.

Однак низька конкурентоспроможність української оборонної продукції на світовому ринку залишається серйозною проблемою. Для її подолання необхідно залучати молодих фахівців, які можуть привнести свіжі ідеї та інноваційні рішення. Крім того, проблеми у сфері науково-дослідних і дослідно-конструкторських робіт гальмують технологічний прогрес галузі.

Для вирішення цих викликів необхідно розробити та впровадити стратегії, спрямовані на посилення інноваційного потенціалу оборонної промисловості. Це включає підтримку науково-дослідних і дослідно-конструкторських робіт, модернізацію виробничих потужностей і розширення співпраці з міжнародними партнерами. Такий підхід дозволить не лише підвищити конкурентоспроможність української оборонної продукції, але й зміцнити позиції України на глобальному ринку, забезпечуючи стійкість і безпеку країни в умовах сучасних геополітичних реалій.

Для зміцнення науково-технічного потенціалу ОП України та забезпечення її конкурентоспроможності на глобальному рівні пропонується впровадження наступних заходів:

посилення фінансування науково-дослідних і дослідно-конструкторських робіт: забезпечення стабільного та достатнього фінансування науково-дослідних і дослідно-конструкторських робіт з розробки інноваційних оборонних технологій, що сприятиме створенню сучасного озброєння та зменшенню залежності від іноземних постачальників;

поглиблення співпраці з академічними та промисловими партнерами: створення науково-технічних хабів і дослідницьких центрів у співпраці з університетами та промисловими підприємствами для спільної розробки передових технологій і прискорення їх впровадження у виробництво;

розвиток адаптивних виробничих систем: впровадження гнучких виробничих потужностей, які дозволяють оперативно реагувати на зміни ринкових потреб і швидко перебудовувати виробничі процеси для виготовлення актуальної продукції;

підтримка молодих фахівців: створення умов для залучення молодих інженерів і дослідників через грантові програми, стажування та підтримку стартапів у сфері оборонних технологій, що сприятиме появі нових інноваційних рішень;

розширення міжнародного співробітництва: активізація науково-технічного обміну з іноземними партнерами, участь у міжнародних проєктах і залучення передового досвіду для підвищення якості та конкурентоспроможності української оборонної продукції.

Ці ініціативи сприятимуть розвитку незалежної та інноваційної оборонної промисловості, зменшуючи залежність України від зарубіжних технологій. Інвестиції в технічну освіту та наукові дослідження є критично важливими для забезпечення сталого прогресу галузі та підвищення якості продукції.

Розвиток оборонної промисловості також матиме позитивний вплив на економіку, стимулюючи суміжні галузі та створюючи нові робочі місця. Збільшення витрат на оборону демонструє серйозне ставлення до національної безпеки, однак ключовим є забезпечення ефективного використання цих ресурсів. Розробка стратегій, орієнтованих на довгострокове зміцнення оборонного потенціалу, дозволить Україні впевнено протистояти потенційним загрозам і відстоювати свої національні інтереси.

Висновки

Розвиток ОПК України є критично важливим для забезпечення національної безпеки та стійкості країни в умовах триваючої агресії та геополітичних викликів. Аналіз сучасного стану ОПК виявив низку системних проблем, зокрема застарілу інфраструктуру, недостатнє фінансування, дефіцит кваліфікованих кадрів і обмежену конкурентоспроможність продукції на світовому ринку. Водночас ці виклики відкривають можливості для трансформаційних змін, спрямованих на модернізацію та інноваційний розвиток галузі.

Ключовими напрямками розвитку ОПК є нарощування виробництва артилерійських систем, бронетехніки, безпілотних літальних апаратів і засобів радіоелектронної боротьби, що відповідають сучасним стандартам і потребам Збройних Сил України. Успіхи в цих сферах, зокрема зростання виробництва БПЛА та налагодження випуску 155-мм снарядів, демонструють потенціал України для зміцнення власної обороноздатності. Проте значний рівень фізичного та морального зносу обладнання (30–40%) і недостатнє фінансування (2,1–2,4% ВВП замість передбачених 5%) залишаються серйозними перешкодами.

Для подолання викликів, що стоять перед ОПК України, необхідна комплексна стратегія, яка охоплює кілька ключових напрямків. Вона передбачає збільшення інвестицій у НДДКР з метою створення інноваційних технологій. Важливим елементом є розвиток державно-приватного партнерства для активного залучення приватного сектору до виробництва та впровадження гнучких виробничих систем. Не менш суттєвим є поглиблення співпраці з академічними установами та міжнародними партнерами, що сприятиме ефективному обміну технологіями та досвідом. Стратегія також передбачає підтримку молодих фахівців через освітні програми та гранти для стимулювання інновацій. Нарешті, ключовим є забезпечення стабільного фінансування, яке відповідатиме реальним потребам сектору безпеки й оборони.

Реалізація цих заходів сприятиме трансформації ОПК України в потужний, інноваційний і конкурентоспроможний сектор економіки. Це не лише забезпечить незалежність від імпорту озброєння, але й зміцнить економічний потенціал країни через створення робочих місць і розвиток суміжних галузей. Успішна модернізація ОПК стане запорукою стійкості України, її здатності протистояти зовнішнім загрозам і відстоювати національні інтереси в умовах складного геополітичного середовища.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Рижих В. М., Богущкий П. П. Щодо першочергових заходів удосконалення організації державного управління оборонним сектором економіки України // Наука і оборона. 2021. № 1. С. 40–47. URL : <https://nio.nuou.org.ua/article/view/230823>.
2. Ватаманюк-Зелінська У. З., Беднарчук В. В., Млінцова А. О. Фінансування потреб оборонного сектору в Україні // Інноваційна економіка. 2020. № 7–8. С. 22–27. URL : <https://financial.lnu.edu.ua/wp-content/uploads/2015/11/670-1412-1-SM.pdf>
3. Кулицький С. П. Сучасний етап розвитку оборонно-промислового комплексу та виробництва продукції подвійного призначення в Україні // Україна: події, факти, коментарі. 2018. № 5. С. 54–69.

4. Слободяник К. П. Український оборонно-промисловий комплекс у системі міжнародних економічних зв'язків // Проблеми підвищення ефективності інфраструктури. 2014. № 38. С. 95–101. URL : <https://jrnل.nau.edu.ua/index.php/PPEI/article/view/7253>
5. Савицький А. В. Концептуальні засади розвитку потенціалу підприємств оборонно-промислового комплексу в економічному зростанні України // Збірник наукових праць ТДАТУ імені Дмитра Моторного (економічні науки). 2023. № 1 (47). С. 116–128.
6. Тимошенко О. В. Виклики та загрози четвертої промислової революції: наслідки для України // Бізнес Інформ. 2019. № 2. С. 21–29.
7. Толок П. О. Взаємодія оборонних підприємств України із зовнішнім середовищем: контекст фінансової безпеки // Інфраструктура ринку. 2019. № 30. С. 235–240.
8. Стратегічний партнер у виробництві озброєння та військової техніки в Україні [Електронний ресурс] // Укроборонпром : офіц. веб-сайт. URL: <https://ukroboronprom.com.ua/> (дата звернення: 20.06.2025).
9. Про Стратегію забезпечення державної безпеки : Указ Президента України від 16 лют. 2022 р. № 56/2022. URL: <https://zakon.rada.gov.ua/laws/show/56/2022#Text> (дата звернення: 19.06.2025).
10. Про національну безпеку України : Закон України від 21 серп. 2018 р. № 2469-VIII // Відомості Верховної Ради України. 2018. № 31. Ст. 24.
11. Про Державний бюджет України на 2019 рік : Закон України від 23 листоп. 2018 р. № 2629-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2629-19#Text> (дата звернення: 19.06.2025).
12. Про Державний бюджет України на 2020 рік : Закон України від 14 листоп. 2019 р. № 294-IX. URL: <https://zakon.rada.gov.ua/laws/show/294-20#Text> (дата звернення: 19.06.2025).
13. Про Державний бюджет України на 2021 рік : Закон України від 15 груд. 2020 р. № 1082-IX. URL: <https://zakon.rada.gov.ua/laws/show/1082-20#Text> (дата звернення: 19.06.2025).
14. Про Державний бюджет України на 2022 рік : Закон України від 02 груд. 2021 р. № 1928-IX. URL: <https://zakon.rada.gov.ua/laws/show/1928-20#Text> (дата звернення: 19.06.2025).
15. Про Державний бюджет України на 2023 рік : Закон України від 03 листоп. 2022 р. № 2710-IX. URL: <https://zakon.rada.gov.ua/laws/show/2710-20#Text> (дата звернення: 20.06.2025).
16. Про Державний бюджет України на 2024 рік : Закон України від 09 листоп. 2023 р. № 3460-IX. URL: <https://zakon.rada.gov.ua/go/3460-20> (дата звернення: 20.06.2025).
17. Про Державний бюджет України на 2025 рік : Закон України від 19 листоп. 2024 р. № 4059-IX. URL: <https://zakon.rada.gov.ua/go/4059-20> (дата звернення: 20.06.2025).

References

1. Ryzhykh, V. M., & Bohutskyi, P. P. (2021). Priority measures for improving the organization of public administration of Ukraine's defense sector of the economy. *Science and Defense*, (1), 40–47. <https://nio.nuou.org.ua/article/view/230823>
2. Vatamaniuk-Zelinska, U. Z., Bednarchuk, V. V., & Mlintsova, A. O. (2020). Financing the needs of the defense sector in Ukraine. *Innovative Economy*, (7–8), 22–27. <https://financial.lnu.edu.ua/wp-content/uploads/2015/11/670-1412-1-SM.pdf>
3. Kulytskyi, S. P. (2018). The current stage of development of the defense-industrial complex and dual-use production in Ukraine. *Ukraine: Events, Facts, Comments*, (5), 54–69.
4. Slobodianiuk, K. P. (2014). The Ukrainian defense-industrial complex in the system of international economic relations. *Problems of Improving Infrastructure Efficiency*, (38), 95–101. <https://jrnл.nau.edu.ua/index.php/PPEI/article/view/7253>
5. Savytskyi, A. V. (2023). Conceptual principles for developing the potential of defense-industrial enterprises in Ukraine's economic growth. *Proceedings of Dmytro Motornyi Tavria State Agrotechnological University (Economic Sciences)*, 1(47), 116–128.

6. Tymoshenko, O. V. (2019). Challenges and threats of the Fourth Industrial Revolution: Implications for Ukraine. *Business Inform*, (2), 21–29.
7. Tolok, P. O. (2019). Interaction of Ukraine's defense enterprises with the external environment: The financial security context. *Market Infrastructure*, (30), 235–240.
8. Ukroboronprom State Concern. (2025). *Strategic partner in the production of weapons and military equipment in Ukraine*. <https://ukroboronprom.com.ua/>
9. President of Ukraine. (2022). *On the National Security Strategy of Ukraine* (Decree No. 56/2022). <https://zakon.rada.gov.ua/laws/show/56/2022#Text>
10. Verkhovna Rada of Ukraine. (2018). *On National Security of Ukraine* (Law No. 2469-VIII). *Bulletin of the Verkhovna Rada of Ukraine*, (31), Article 24.
11. Verkhovna Rada of Ukraine. (2018). *On the State Budget of Ukraine for 2019* (Law No. 2629-VIII). <https://zakon.rada.gov.ua/laws/show/2629-19#Text>
12. Verkhovna Rada of Ukraine. (2019). *On the State Budget of Ukraine for 2020* (Law No. 294-IX). <https://zakon.rada.gov.ua/laws/show/294-20#Text>
13. Verkhovna Rada of Ukraine. (2020). *On the State Budget of Ukraine for 2021* (Law No. 1082-IX). <https://zakon.rada.gov.ua/laws/show/1082-20#Text>
14. Verkhovna Rada of Ukraine. (2021). *On the State Budget of Ukraine for 2022* (Law No. 1928-IX). <https://zakon.rada.gov.ua/laws/show/1928-20#Text>
15. Verkhovna Rada of Ukraine. (2022). *On the State Budget of Ukraine for 2023* (Law No. 2710-IX). <https://zakon.rada.gov.ua/laws/show/2710-20#Text>
16. Verkhovna Rada of Ukraine. (2023). *On the State Budget of Ukraine for 2024* (Law No. 3460-IX). <https://zakon.rada.gov.ua/go/3460-20>
17. Verkhovna Rada of Ukraine. (2024). *On the State Budget of Ukraine for 2025* (Law No. 4059-IX). <https://zakon.rada.gov.ua/go/4059-20>

Стратегічний аналіз трансформації ОПК України під впливом воєнних загроз та глобальних технологічних змін

Strategic Analysis of the Transformation of Ukraine's Defense Industry Under the Influence of Military Threats and Global Technological Changes

Володимир Коваль

Volodymyr Koval

кандидат військових наук, старший науковий співробітник, e-mail: Candidate of Military Sciences, Senior Researcher, e-mail: vladimerkoval69@gmail.com, ORCID: 0000-0002-6209-6779 vladimerkoval69@gmail.com, ORCID: 0000-0002-6209-6779

Міністерство оборони України, м. Київ, Україна

Ministry of Defense of Ukraine, Kyiv, Ukraine

Received: August 11, 2025 | Revised: August 25, 2025 | Accepted: August 31, 2025

DOI: <https://doi.org/10.33445/sds.2025.15.4.26>

Мета роботи. Наукове обґрунтування та систематизація факторів зовнішнього і внутрішнього середовища функціонування підприємств оборонно-промислового комплексу України для розробки адаптивної системи стратегічного планування на основі когнітивного підходу та інтелектуальних технологій.

Метод дослідження. Застосовано комплекс інструментів стратегічного аналізу: адаптовану модель «п'яти сил» М. Портера для аналізу мікросередовища, SWOT-аналіз для визначення можливостей і загроз ОПК, а також методи когнітивного та логіко-лінгвістичного моделювання для формалізації процесів прийняття рішень суб'єктом управління.

Результати дослідження. Проведено детальну класифікацію факторів зовнішнього середовища ОПК в умовах воєнного стану; ідентифіковано атрибутивні та реляційні параметри мікросередовища підприємств; систематизовано загрози функціонуванню галузі. Обґрунтовано доцільність впровадження систем підтримки прийняття рішень (DSS), що базуються на технологіях Індустрії 4.0 (ERP, MES, AI), та використання зворотного логічного виводу для проектування «моделі майбутнього» підприємства.

Теоретична цінність дослідження. Робота поглиблює теорію адаптивного управління через впровадження когнітивного підходу до аналізу концептосфери та онтології знань у сфері ОПК. Уточнено сутність «атрибутивних» та «реляційних» концептів як основи для створення цифрових двійників складних промислових систем.

Практична цінність дослідження. Отримані результати дозволяють підприємствам ОПК перейти від директивного до адаптивного планування, забезпечуючи стійкість (resilience) виробничих циклів до зовнішніх шоків. Запропоновані алгоритми сприяють автоматизації взаємодії із замовником, оптимізації собівартості та ефективній диверсифікації діяльності.

Цінність дослідження. Уперше проведено авторську систематизацію параметрів мікросередовища ОПК України з урахуванням специфіки воєнного стану та DefenseTech-кластерів, що дозволило поєднати методи класичного стратегічного менеджменту з наскрізними цифровими технологіями (AI, Big Data, когнітивне моделювання).

Обмеження дослідження. Обмеження стосуються високої динамічності змін у нормативно-правовому регулюванні оборонних закупівель та складності формалізації суб'єктивних ментальних моделей осіб, що приймають рішення (ОПР).

Тип статті: Дослідницький.

Purpose. To provide a scientific substantiation and systematization of external and internal environmental factors of the Ukrainian defense-industrial complex (DIC) to develop an adaptive strategic planning system based on a cognitive approach and intelligent technologies.

Method. A complex of strategic analysis tools was applied: an adapted M. Porter's "Five Forces" model for microenvironment analysis, SWOT analysis to identify DIC opportunities and threats, and methods of cognitive and logical-linguistic modeling to formalize decision-making processes of the management subject.

Findings. A detailed classification of external DIC environmental factors under martial law was conducted; attributive and relational parameters of enterprise microenvironments were identified; threats to industry functioning were systematized. The feasibility of implementing Decision Support Systems (DSS) based on Industry 4.0 technologies (ERP, MES, AI) and using backward logical inference for designing the "future model" of the enterprise was justified.

Theoretical implications. The work deepens the theory of adaptive management through the introduction of a cognitive approach to the analysis of the conceptosphere and knowledge ontology in the DIC sphere. The essence of "attributive" and "relational" concepts is clarified as the basis for creating digital twins of complex industrial systems.

Practical implications. The results allow DIC enterprises to transition from directive to adaptive planning, ensuring the resilience of production cycles to external shocks. The proposed algorithms facilitate automated interaction with customers, cost optimization, and effective diversification of activities.

Originality. For the first time, an original systematization of microenvironment parameters of the Ukrainian DIC was conducted, considering the specifics of martial law and DefenseTech clusters, which allowed for combining classical strategic management methods with end-to-end digital technologies (AI, Big Data, cognitive modeling).

Research limitations. Limitations relate to the high dynamics of changes in the regulatory environment for defense procurement and the difficulty of formalizing the subjective mental models of decision-makers.

Paper type. Research.

Ключові слова: ОПК України, стратегічний аналіз, когнітивне управління, цифровий двійник, модель М. Портера, адаптивне планування, штучний інтелект, логіко-лінгвістичне моделювання, національна стійкість.

Key words: Ukrainian Defense Industry, Strategic Analysis, Cognitive Management, Digital Twin, Porter's Five Forces, Adaptive Planning, Artificial Intelligence, Logical-Linguistic Modeling, National Resilience.

Вступ

Трансформація оборонно-промислового комплексу (ОПК) України в умовах повномасштабної агресії вимагає перегляду класичних підходів до стратегічного аналізу. В умовах воєнного стану підприємства ОПК стикаються з безпрецедентною динамікою зовнішнього середовища, що робить традиційні методи планування “від досягнутого” малоефективними. Сучасний етап розвитку національної економіки вимагає впровадження інтелектуальних систем, здатних обробляти великі масиви даних та здійснювати антиципацію (випереджальне реагування) на загрози.

Актуальність дослідження зумовлена необхідністю переходу від жорсткого директивного управління до гнучких адаптивних стратегій. Це передбачає використання когнітивних технологій та цифрових двійників, які дозволяють синхронізувати виробничі можливості підприємств із мінливими потребами сектору безпеки та оборони. ОПК сьогодні розглядається не лише як засіб забезпечення армії, а й як локомотив технологічного розвитку країни, що базується на принципі “безпека через розвиток”.

Теоретичні основи дослідження

Теоретичний фундамент роботи базується на поєднанні класичного стратегічного менеджменту та новітніх кібернетичних підходів:

- Параметрична теорія систем: розгляд ОПК через призму атрибутивних (властивості об'єкта) та реляційних (відносини суб'єкта) концептів, що формують основу для створення цифрових моделей.
- Концепція адаптивного управління: використання зворотного логічного виводу для проектування траєкторії досягнення стратегічних цілей в умовах високої невизначеності.
- Теорія когнітивного моделювання: застосування логіко-лінгвістичного апарату для формалізації мисленнєвої діяльності особи, що приймає рішення (ОПР), та перетворення знань у керований вплив.
- Модель “п'яти сил” М. Портера: адаптована до специфіки моносонічного ринку озброєнь, де держава виступає головним замовником.

Постановка проблеми

Незважаючи на активну цифровізацію та зростання DefenseTech-сектору, залишається низка невирішених проблем:

1. Брак інструментів антиципації: відсутність на підприємствах систем, здатних автоматично розпізнавати класи проблемних ситуацій до моменту їх критичного впливу на виробництво.
2. Інформаційний розрив: низька якість взаємодії між управляючим контуром (державні органи) та виробничим контуром через відсутність єдиної онтології знань та терміносистеми.
3. Складність формалізації: управлінські рішення в ОПК часто базуються на суб'єктивному досвіді ОПР, який важко інтегрувати в сучасні ERP-системи без використання когнітивних методів.

Ресурсні обмеження: жорстке регулювання цін та дефіцит компонентів вимагають математично точного, але гнучкого планування, яке не забезпечується застарілими методами.

Методологія дослідження

Для комплексного дослідження архітектури ОПК та розробки системи планування застосовано такі методи:

- SWOT-аналіз: для ідентифікації стратегічних можливостей (експортний потенціал, технологічний прорив) та систематизації загроз (технологічна залежність, волатильність попиту).
- Логіко-лінгвістичне моделювання (ЛЛМ): розробка дискретно-ситуаційних мереж для формалізації сценаріїв розв'язання стратегічних завдань.
- Фреймовий підхід: структурування знань про ресурси (метали, ЕКБ, фінанси) у вигляді стандартних одиниць знань (CO3) для систем підтримки прийняття рішень (DSS).
- Метод цифрових двійників: моделювання промислової системи через потоки ресурсів для виявлення розривів між потребами замовника та можливостями виробництва.

Використана методологія дозволяє інтегрувати когнітивний аналіз у цифрову архітектуру підприємства, створюючи надійне підґрунтя для забезпечення національної стійкості.

Результати

Трансформація оборонно-промислового комплексу (ОПК) України в умовах повномасштабної агресії вимагає перегляду класичних підходів до стратегічного аналізу. Склад факторів зовнішнього та внутрішнього середовища підприємств ОПК безпосередньо зумовлює архітектуру об'єкта та суб'єкта управління, а їх вивчення в сучасних умовах нерозривно пов'язане з можливостями інтелектуальної обробки великих масивів даних та антиципації ризиків.

Розглянемо основні чинники зовнішнього середовища через призму функціонування українського ОПК у період воєнного стану (табл. 1).

Таблиця 1 – Фактори зовнішнього середовища функціонування підприємств ОПК України

Категорія факторів	Склад та галузева специфіка	Вплив на систему планування
Замовники	Міноборони України, Генштаб ЗСУ, ДП “Агенція оборонних закупівель”, іноземні партнери (в межах міжурядових угод).	Визначають пріоритетність НДДКР та обсяги серійного виробництва.
Постачальники ресурсів та кооперація	Постачальники ЕКБ, металопродукату, західні виробники комплектуючих, учасники кластеру Brave1, фінансові інституції.	Формують ланцюги створення вартості та визначають технологічну незалежність.
Контролюючі органи	Держаудитслужба, НАЗК, АМКУ, Міноборони (військові представництва), СБУ (контроль режиму секретності).	Регулюють ціноутворення, дотримання антикорупційних норм та якість продукції.
Конкуренти	Приватні оборонні компанії України, глобальні гравці (Lockheed Martin, Rheinmetall), виробники товарів-субститутів (FPV-дрони vs артилерія).	Стимулюють інновації та боротьбу за кадровий ресурс.
Державне регулювання	Закони про оборонні закупівлі, бюджетна політика, військово-технічне співробітництво, інтеграція до стандартів НАТО.	Встановлює правові межі та обсяги фінансового забезпечення.

Для поглибленого пізнання міжелементних зв'язків та обставин мікросередовища доцільно використовувати інструментарій стратегічного аналізу на основі адаптованої моделі “п'яти сил” М. Портера [1]. Це дозволяє виділити специфіку аналізованої області в частині вдосконалення аналітичного забезпечення стратегічного планування (табл. 2).

Детальний аналіз мікросередовища слугує основою для антиципації ризиків та загроз утворення проблемних ситуацій. Він дозволяє сформулювати емпіричну логіко-лінгвістичну

модель дискретно-ситуаційної мережі, що допомагає визначити граничні умови для фреймового представлення знань про шляхи розв'язання стратегічних завдань.

Таблиця 2 – Аналіз мікросередовища підприємства ОПК (адаптація моделі М. Портера з урахуванням атрибутивних та реляційних параметрів)

Сила конкуренції	Атрибутивні параметри (властивості)	Реляційні параметри (відносини)
Ринкова влада постачальників	Унікальність ЕКБ, залежність від імпорту, дефіцит спецсталей.	Ступінь вертикальної інтеграції, контракція на 1–3 роки.
Ринкова влада замовників	Монопсонія (державна як єдиний покупець), жорсткі вимоги до ТТХ.	Залежність від державного оборонного замовлення, процедури приймання ВП МОУ.
Загроза появи нових гравців	Високий бар'єр входу (ліцензії), потреба в капіталі.	Динамічне зростання сегменту DefenseTech, залучення стартапів.
Загроза товарів-субститутів	Глобальні технологічні зміни (роботизація), зміна тактики ведення бою.	Конкуренція між традиційним озброєнням та новими високотехнологічними зразками.
Суперництво між діючими фірмами	Спеціалізація (авіація, бронетехніка), державна vs приватна власність.	Боротьба за державні кошти та дефіцитні інженерні кадри.

Джерело: розроблено автором на основі [1]

Слід зазначити, що конкуренція в ОПК України має нерівномірний та специфічний характер:

1. Монопольне становище: Окремі державні підприємства залишаються єдиними постачальниками унікальних технологій (наприклад, ракетне озброєння, авіаремонт), що забезпечує їм стабільність, але знижує мотивацію до зниження витрат.

2. Загроза субститутів: В умовах сучасної війни дрони-камікадзе стають ефективним заміном дорогої високоточної зброї, що змушує традиційні заводи ОПК до швидкої диверсифікації.

3. Залежність від замовника: Високий ступінь впливу Міністерства оборони через можливість передачі конструкторської документації від одного розробника до іншого виробника (нового конкурента), що радикально змінює ситуацію на ринку.

Аналіз внутрішнього середовища та зовнішніх шоків дозволяє в подальшому провести ранжування проблемних ситуацій за класами важливості та ризиковості, що є критично важливим для побудови адаптивної системи планування.

Аналіз внутрішньої структури ОПК України дозволяє розкрити складну архітектуру взаємодії між управляючими та керованими підсистемами, специфіку логістичних ланцюгів та особливості збуту в умовах воєнного стану. Для систематизації цих зв'язків доцільно розглянути укрупнену структуру оборонно-промислового сектору (табл. 3).

Таблиця 3 – Укрупнена структура та функціональні зв'язки в ОПК України

Рівень структури	Суб'єкти та об'єкти	Ключові характеристики взаємодії
Управляючий контур	Кабінет Міністрів, Мінстратегпром, Міноборони, РНБО.	Формування державних цільових програм, нормативне регулювання цін та прибутковості.
Продуктовий вертикальний контур	Державні холдинги (напр. АТ "Українська оборонна промисловість"), великі приватні концерни.	Виконання функцій головного виконавця, координація кооперації другого та третього рівнів.

Виробничий контур	Серійні заводи, ремонтні підприємства, науково-дослідні інститути.	Пряма реалізація виробничих циклів, залежність від поставок ЕКБ та енергоресурсів.
Інноваційний контур	Кластери (Brave1), конструкторські бюро, DefenseTech стартапи.	Розробка асиметричних рішень, швидке прототипування та тестування в бойових умовах.

Джерело: сформовано автором на основі [2]

Слід підкреслити, що на відміну від цивільних галузей економіки, підприємства ОПК функціонують в умовах директивно регульованого ринку. Це створює низку специфічних обмежень: жорстка політика стримування цін з боку замовника часто перешкоджає своєчасному оновленню основних фондів. Дрібносерійність продукції та обмежене коло сертифікованих постачальників не дозволяють повною мірою оптимізувати бізнес-процеси для суттєвого зниження собівартості.

Водночас український ОПК має суттєві конкурентні переваги: наявність висококваліфікованої інженерної школи та здатність створювати наукомістку продукцію, що пройшла перевірку в умовах реальних бойових дій (combat proven). Хоча обмеження міжнародної кооперації в окремих секторах забезпечує автономність, воно водночас може стримувати технологічний прогрес, що робить актуальним впровадження механізмів трансферу технологій та спільних підприємств із західними партнерами [3].

Для завершення стратегічного аналізу підрозділу 2.1 скористаємося методом SWOT-аналізу для визначення перспективних можливостей ОПК України (табл. 4).

Таблиця 4 – SWOT-аналіз можливостей розвитку ОПК України

Фактор можливостей	Зміст та стратегічне значення	Очікуваний ефект
Експортний потенціал	Високе визнання якості української зброї на міжнародному ринку після 2022 року.	Надходження валютної виручки та розширення серійності.
Доступ до унікальних ресурсів	Пріоритетне забезпечення сировиною, енергією та фінансуванням.	Стабільність виробничих циклів у кризові періоди.
Стратегічний статус	Визнання ОПК пріоритетом національної безпеки (принцип «безпека через розвиток»).	Державні гарантії та пільгове кредитування.
Технологічний прорив	Можливість першочергового використання досягнень НТР (AI, БПЛА, РЕБ).	Створення асиметричних переваг на полі бою.
Диверсифікація (конверсія)	Реалізація оборонних розробок у цивільних галузях (медицина, зв'язок).	Підвищення загальної стійкості економіки.
Цифрова трансформація	Впровадження передових ІКТ та систем ERP в управління ОПК.	Оптимізація витрат та прозорість планування.

Джерело: розроблено автором на основі [5]

Застосування алгоритму зворотного логічного виводу в процесі стратегічного планування, який розглядається автором як ключовий інструмент [6], дозволяє ефективно використовувати ці можливості для формування «моделі майбутнього» ОПК. Це забезпечує високу пропускну здатність інформаційних потоків усередині продуктових вертикалей та дозволяє гнучко адаптувати плани до динамічних змін воєнно-політичної обстановки.

Розглядаючи перспективи розвитку ОПК України, слід звернути увагу на актуальні законодавчі ініціативи та цифрові трансформації, спрямовані на підвищення ефективності планування:

1. Стимулювання зниження собівартості: обговорюється впровадження механізму фіксації економічних показників на визначений період, що дозволило б підприємствам зберігати частину економії як додатковий прибуток для подальшого інвестування в модернізацію.

2. Цифровізація взаємодії із замовником: впровадження платформ для електронної подачі розрахунково-калькуляційних матеріалів (РКМ), що дозволить суттєво скоротити терміни їх розгляду та забезпечити прозорість ціноутворення [7].

Поряд із можливостями, перед підприємствами ОПК постають серйозні загрози, що вимагають системної антиципації. Причинно-наслідковий аналіз дозволяє систематизувати ці виклики для розробки превентивних заходів (табл. 5).

Таблиця 5 – Систематизація загроз функціонуванню підприємств ОПК України

Джерело загрози	Зміст загрози	Наслідки для системи планування
Ринок та попит	Коливання обсягів державних закупівель після завершення активних фаз конфлікту.	Утворення надлишкових потужностей та дефіцит обігових коштів.
Замовник	Висока залежність від єдиного державного замовника та зміна пріоритетів ВВТ.	Необхідність швидкої перебудови виробничих ліній.
Міжнародне середовище	Технологічні обмеження, складність імпортозаміщення критичних компонентів.	Порушення логістичних ланцюгів та затримки у виконанні контрактів.
Науково-технічний прогрес	Поява зразків озброєння на нових фізичних принципах (товари-субститути).	Ризик морального застарівання продукції до моменту серійного випуску.
Регуляторне середовище	Посилення вимог до постачальників, зростання витрат на адміністрування контрактів.	Зниження чистої рентабельності оборонних проектів.

Джерело: розроблено автором на основі [7]

На основі проведеного SWOT-аналізу було виокремлено ключові напрями стратегічного розвитку ОПК, що можуть бути покладені в основу формування державної політики:

- Впровадження стандартів якості, гармонізованих зі стандартами НАТО (AQAP 2000).
- Реалізація цільових програм підготовки інженерних кадрів та цифрових навичок.
- Удосконалення механізмів військового приймання та контролю якості.
- Активне впровадження результатів НДДКР у серійне виробництво.
- Цифрова трансформація та розробка систем адаптивного стратегічного планування на рівні підприємств.

- Диверсифікація діяльності та збільшення частки продукції подвійного призначення.

Наукова новизна в частині аналізу тенденцій розвитку ОПК полягає в авторській систематизації атрибутивних і реляційних параметрів мікросередовища та структури галузі, що визначають умови формування планових рішень в умовах воєнних загроз.

Особливий інтерес становить динаміка трансформації стратегій ОПК України. Якщо у 1990-х та 2000-х роках переважали стратегії стабілізації та виживання в умовах демілітаризації, то з 2014 року фокус змістився на стратегії прискореного зростання та імпортозаміщення. Початок 2020-х років та повномасштабне вторгнення вивели на перший план стратегію гнучкої адаптивності та інтеграції у глобальні оборонні ланцюги.

Вимоги щодо диверсифікації діяльності підприємств ОПК сьогодні обумовлені не лише економічними чинниками, а й необхідністю забезпечення стійкості (resilience) держави.

Забезпечення завантаженості потужностей за рахунок продукції подвійного призначення дозволяє зберігати унікальні компетенції навіть при коливаннях прямого оборонного замовлення.

Питання аналізу факторів та умов, що враховують особливості ОПК при побудові концептуального каркаса стратегічного управління, детально розглянуті автором у спільних дослідженнях із провідними фахівцями галузі [5].

Дослідивши структуру ОПК України, реляційні та атрибутивні параметри мікросередовища, а також історичні аспекти трансформації галузі, необхідно перейти до аналізу сучасних підходів до планування діяльності підприємства як промислової системи. Це дозволить інтегрувати класичні методи управління у сучасну цифрову архітектуру стратегічного планування.

Аналіз сучасних обставин та підходів до планування діяльності підприємства ОПК як промислової системи

Існує безліч факторів, що вплинули на розвиток планування та контролю операцій. За останні пів століття було впроваджено кілька поколінь систем, проте вони не змогли повністю виключити з процесу управління людину. Мисленнєва діяльність особи, що приймає рішення (ОПР), є надзвичайно складним процесом, формалізація якого лежить на стику логіки, психології, лінгвістики та математики.

Стратегічне планування нерозривно пов'язане з процесами мовленнєвої та інтелектуальної діяльності, які важко піддаються формалізації. Для автоматизації підтримки управлінських рішень лише математичного апарату часто недостатньо. Розвиток ІКТ сприяв появі інтелектуальних або експертних систем, що стали попередниками штучного інтелекту (ШІ), оскільки в їхню основу закладено технології накопичення та вилучення знань.

Сучасні ERP-системи ґрунтуються на принципах процесного підходу (згідно зі стандартами ISO 9001:2015) та інтегрують цифрові рішення Індустрії 4.0:

- HCM (Human Capital Management) — управління інтелектуальним потенціалом;
- MES (Manufacturing Execution System) — оперативне управління виробництвом на рівні цеху;
- CRM (Customer Relationship Management) — управління взаємодією із замовником (Міноборони, іноземні партнери).

Аналіз інтелектуальних рішень на основі когнітивного підходу та можливостей штучного інтелекту в прийнятті рішень

Когнітивний підхід в управлінні складними системами базується на когнітивній лінгвістиці та психології. У когнітивному підході ключову роль відіграє ментальна діяльність суб'єкта розробки стратегії.

Завдання перетворення інформації в управляючий вплив включає:

1. Формування концептосфери та онтології знань (терміносистеми галузі).
2. Фреймове представлення знань про явища (структуровані сценарії подій).
3. Використання прямого та зворотного логічного виводу для опису мисленнєвої діяльності при формуванні рішень.

Когнітивне моделювання стратегії та аналіз метаданих проблемних ситуацій набули широкого вжитку. Теорія когнітивного моделювання представлена не лише когнітивними картами (які фіксують лише факт наявності зв'язку між елементами), а й логіко-лінгвістичним моделюванням — системою формалізації саме процесів мислення ОПР.

В Україні когнітивне управління знайшло відображення в теорії адаптивного управління, зокрема при побудові концептуального каркаса суб'єкта та об'єкта, а також у формуванні логіко-лінгвістичних моделей дискретно-ситуаційних мереж проблемних ситуацій. Такі моделі виступають інтелектуальними засобами підтримки рішень, дозволяючи ОПР діяти ефективно в умовах зовнішніх шоків.

Розвиваючи загальну параметричну теорію управління [2], доцільно використовувати “партикузальну” систему, яка не має жорсткого формалізованого (математичного чи семантичного) представлення про свою поведінку, стійкі характеристики зв’язків чи методи мотивації. Саме для таких систем когнітивний підхід стає незамінним інструментом аналізу, оцінки та прогнозування.

У системі об’єкта управління вивчаються характеристики, що відповідають його функціям (виробництву), утворюючи “атрибутивний концепт” — відому властивість із незрозумілим або мінливим типом відношення в об’єкті. Для ОПК такими концептами є спеціальні характеристики надійності та функціональності, що забезпечуються електронною компонентною базою, унікальними технологіями та конструкторськими рішеннями.

Проблема полягає в тому, що технічні вимоги замовника часто не збігаються з реальними можливостями виробництва, що веде до дрібносерійності. Вивчаючи потреби через модель цифрового двійника за характеристиками потоків ресурсів (матеріальних, інформаційних, фінансових), можна виявити проблемні ситуації першого класу — розрив між потребами та можливостями на вході та виході елементарного об’єкта.

Розглядаючи суб’єкт управління, слід виокремити роль людини (ОПР). Її діяльність має суб’єктивний характер і часто проявляється через індивідуальні мовленнєві акти, дилеми та предикати. Когнітивний аналіз у межах теорії адаптивного управління розглядає дилеми рівноваги, співпраці, довіри, загрози та реалізму між ОПР. Ці когнітивні дефініції служать для розв’язання проблемних ситуацій другого та третього класів, які виникають через конфлікти інтересів усередині управляючої структури або між суб’єктом та об’єктом.

Відповідно до параметричної теорії, визначені відношення з невизначеними властивостями формують «реляційний концепт» — цифровий двійник у свідомості ОПР. Після формалізації такої системи можна виміряти відносини подібності:

- Ізоморфізм (повна відповідність) притаманний серійному виробництву та дотриманню жорстких законодавчих норм.
- Гомоморфізм (часткова подібність) характерний для створення унікальної продукції та техпроцесів, що лише наближаються до ідеальної моделі.

Специфіка ОПК України з його багаторівневою структурою замовників, виконавців та контролюючих органів (Міноборони, Мінстратегпром, казначейство тощо) значно ускладнює пряму формалізацію процесів. Когнітивний підхід у цьому разі виправданий складністю об’єкта дослідження. Можливість реалізації такого підходу прямо залежить від рівня цифрової зрілості підприємства, що передбачає впровадження систем класів ERP, CAD, PDM, ECM та BI (Business intelligence).

Найбільш перспективним інструментарієм для реалізації сучасного стратегічного планування є системи підтримки прийняття рішень — DSS (Decision Support System). Вони базуються на наскрізних технологіях, які аналітична компанія Gartner виділяє як ключові тренди цифрової трансформації:

1. Технології адаптивності: системи, що дозволяють підприємству миттєво реагувати на зміни в зовнішньому середовищі та воєнно-політичні шоки.
2. Мобільність та децентралізація: інструменти для підвищення мобільності персоналу та забезпечення віддаленого доступу до управлінських функцій.
3. Кібербезпека: технології захисту критичних даних та каналів зв’язку в умовах гібридних загроз.
4. Кооперативна інтелектуалізація: технології спільного накопичення та використання досвіду (Knowledge Management) у межах вертикально-інтегрованих структур та оборонних кластерів.

Штучний інтелект: використання алгоритмів машинного навчання та когнітивного аналізу для автоматизації рутинних та прогнозних завдань.

Висновки

Прикладом систем класу DSS для підтримки планування, організації, синхронізації та контролю при прийнятті стратегічних рішень в оборонній сфері можуть слугувати такі рішення, як інтелектуальна платформа Miracle та експертні системи ситуаційного управління (на кшталт комплексу “Керівник”), що адаптовані під специфіку ієрархічних структур.

Зазначені інтелектуальні системи та цифрові технології можуть бути використані як програмна основа для впровадження пропонованої автором системи стратегічного планування підприємства ОПК України.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Porter M. E. Competitive Strategy: Techniques for Analyzing Industries and Competitors. New York: Free Press, 1980. 396 p.
2. Горбулін В. П. Як перемогти Росію у війні майбутнього. Київ: Брайт Букс, 2020. 256 с.
3. Стратегія розвитку оборонно-промислового комплексу України на період до 2030 року: Розпорядження Кабінету Міністрів України від 14.05.2021 № 470-р. URL: <https://zakon.rada.gov.ua/laws/show/470-2021-%D1%80>.
4. Мельник Т. Г. Цифрова трансформація оборонно-промислового комплексу України: виклики та можливості. Економіка та держава. 2023. № 5. С. 14–21.
5. Савченко О. Ф. Адаптивне управління складними системами в умовах невизначеності. Київ: Наукова думка, 2019. 312 с.
6. Gartner Top 10 Strategic Technology Trends for 2024. Stamford: Gartner Inc., 2023. URL: <https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2024>.
7. Про оборонні закупівлі: Закон України від 17.07.2020 № 808-IX. URL: <https://zakon.rada.gov.ua/laws/show/808-20>.

References

1. Porter, M. E. (1980). Competitive Strategy: Techniques for Analyzing Industries and Competitors. Free Press.
2. Horbulin, V. P. (2020). Yak peremohty Rosiiu u viini maibutnoho [How to defeat Russia in the war of the future]. Bright Books.
3. Cabinet of Ministers of Ukraine. (2021). Stratehiia rozvytku oboronno-promyslovoho kompleksu Ukrainy na period do 2030 roku [Strategy for the development of the defense-industrial complex of Ukraine for the period up to 2030]. <https://zakon.rada.gov.ua/laws/show/470-2021-%D1%80>
4. Melnyk, T. H. (2023). Tsyfrova transformatsiia oboronno-promyslovoho kompleksu Ukrainy: vyklyky ta mozhlyvosti [Digital transformation of the defense-industrial complex of Ukraine: challenges and opportunities]. Economy and State, (5), 14–21.
5. Savchenko, O. F. (2019). Adaptivne upravlinnia skladnyimi systemamy v umovakh nevypravdanosti [Adaptive management of complex systems under uncertainty]. Naukova Dumka.
6. Gartner Inc. (2023). Gartner Top 10 Strategic Technology Trends for 2024. <https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2024>
7. Verkhovna Rada of Ukraine. (2020). Zakon Ukrainy “Pro oboronni zakupivli” [Law of Ukraine “On Defense Procurement”]. <https://zakon.rada.gov.ua/laws/show/808-20>